

# SecureLinx SLK Remote KVM User Guide

- SecureLinx SLK1
- SecureLinx SLK8
- SecureLinx SLK16



Part Number: 900–336 Revision B March 2005

#### Copyright and Trademark

© 2005, Lantronix. 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. Printed in the United States of America.

SecureLinx and Remote KVM are trademarks of Lantronix. Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows NT, Windows ME, Windows 2000, and Windows XP are trademarks of Microsoft Corp. Netscape is a trademark of Netscape Communications Corporation.

#### Contacts

#### Lantronix Corporate Headquarters

15353 Barranca Parkway Irvine, CA 92618, USA Phone: 949–453–3990 Fax: 949–453–3995

#### **Technical Support**

Phone: 800–422–4074 or 949–453–7198 Fax: 949–450–7226 Online: <u>www.lantronix.com/support</u>

#### Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix Web site at <u>www.lantronix.com/about/contact/index.html</u>.

#### Disclaimer

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.

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

**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.

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

#### Revisions

Rev.	Date	Comments
А	2/04	
В	3/05	Updated firmware; added new Java viewer applet; added secondary administrator account, integrated remote power control support of SLP series.

# **Contents**

| Contents       |    | <br> |       |       | <br>    |       | .1-i  |
|----------------|----|------|------|------|------|------|------|------|------|------|------|-------|-------|---------|-------|-------|
| List of Figure | es | <br> |       |       | <br>    |       | 1-v   |
| List of Table  | s  | <br> | <br>• | <br>• | <br>• • | <br>1 | l-vii |

## 1: Quick Start

Getting Started	. 1-1
Making the Physical Connections	. 1-2
Powering On and Initial Configuration	. 1-4
Validating Servers	. 1-5
Where to Go from Here	. 1-6

## **2: Introduction**

Overview
SecureLinx SLK Models
SLK1
SLK8
SLK16
Features and Benefits
Features at a Glance
Feature Descriptions 2-3
SLK Configurations
Connecting to the Same Network and Switch as the Server
Connecting to Different Switches 2-5
Multiple Server Configurations 2-5

## 3: Installing the SLK

Unpacking Your Components
Items Supplied by the User
Hardware Description
SLK1 Front and Back Panels 3-3
SLK8 Front and Back Panels 3-5
SLK16 Front and Back Panels 3-7
Installing the SLK
Rack-Mounting the SLK 3-10
Preparing the Target Servers 3-10
Connecting Devices to the SLK 3-13
Connecting to the Network 3-16
Connecting Serial Devices 3-16
Connecting to a Power Source
Validating Target Servers
Where to Go from Here

# 4: Using the Web Control Interface to Configure the SLK

Overview	4-1
Starting a Session	4-2
Understanding the Web Control Interface	4-4

## 5: Using the OSD Interface to Configure the SLK

Overview	5-1
Logging into the OSD	5-2
Navigating through the OSD	5-3
Channel Switch Menu	5-4
Setup Menu	5-5
Network Configuration Menu.	5-5
PPP Options (SLC16 only)	5-7
Monitoring Settings Menu	5-8
First Monitoring Settings Screen	5-8
Second Monitoring Settings Screen	5-9
Third Monitor Settings Screen (SLK16 only)	5-10
Network Management Settings Menu	5-11
SNMP Configuration	5-11
Syslog Configuration	5-12
Security Settings	5-13
Initial Security Screen	5-13
Second Security Screen	5-13
User Administration	5-15
User Name Fields	5-15
Serial Port Configuration	5-16
Local User Control	5-18
Virtual Network Computing 5	5-20
Channel Configuration	5-20
Power Outlet Administration	5-20
Debug – (Factory Only)	5-20

## 6: Using a VNC Viewer to Access the SLK

Overview	յ-1
Using a VNC Viewer to Access Target Servers	<u>5-1</u>

### 7: Troubleshooting

General Troubleshooting	7-2
Keyboard Troubleshooting	7-4
Mouse Troubleshooting	7-5
Video Troubleshooting	. 7-8

## 8: Uploading Flash Files and Certificates

Uploading Firmware	-1
Checking the Current SLK Firmware Version 8-	-1
Downloading Firmware from the Lantronix Web Site	-2
Uploading Firmware to Flash	-2
Using Security and Encryption8-	.3
Using SSL with a Browser	-3
Using SSL without a Browser	-3
Locating Internet Resources	-3
Uploading Certificates	-3

## 9: Defining Custom Send Keys

Custom Key Creation	<del>)</del> -1
Custom Key Guidelines	<b>)-2</b>
Definitions	9-2
Requirements	9-2
Examples	<b>)-</b> 2
Potential Send Keys	<b>)-</b> 3

## **A: Specifications**

Hardware Specifications	A-1
Software Specifications	A-5
Agency Statements	A-6

### **B: Binary to Hexadecimals**

**C: Glossary** 

#### Warranty

## Index

# **List of Figures**

Figure 1-1.	SLK1 Back Panel	1-3
Figure 1-2.	SLK8 Back Panel	1-3
Figure 1-3.	SLK16 Back Panel	1-4
Figure 2-1.	Connecting to the Same Network and Switch as the Server	2-4
Figure 2-2.	Connecting to Different Switches	2-5
Figure 2-3.	Multiple Server Configuration without Firewall	2-5
Figure 2-4.	Multiple Server Configuration with Firewall	2-6
Figure 3-1.	SLK1 Front Panel	3-3
Figure 3-2.	SLK1 Back Panel	3-4
Figure 3-3.	SLK8 Front Panel.	3-5
Figure 3-4.	SLK8 Back Panel	3-6
Figure 3-5.	SLK16 Front Panel.	3-7
Figure 3-6.	SLK16 Back Panel	3-8
Figure 3-7.	Recommended Mouse Settings for Target Servers	3-12
Figure 3-8.	SLK1 Connections	3-14
Figure 3-9.	SLK8 Connections	3-15
Figure 3-10.	SLK16 Connections	3-15
Figure 3-11.	Connecting a Notebook PC to the SLK	3-18
Figure 3-12.	SLK Home Page	3-19
Figure 3-13.	Example of Viewing Video from a Remote Server	3-20
Figure 3-14.	Example of No Incoming Video Message	3-20
Figure 4-1.	Login Wi	ndow4-2
Figure 4-2.	SLK Home Page	4-3
Figure 4-3.	Web Control Interface Page Components	4-5
Figure 4-4.	Example of Controlling a Host	4-9
Figure 4-5.	Viewing Hosts	4-12
Figure 4-6.	Power Control with an Optional SLP Remote Power Manager	4-13
Figure 4-7.	User Activity Page	4-15
Figure 4-8.	Event Log.	4-16
Figure 4-9.	Flash File System.	4-17
Figure 4-10.	Debug Menu Page	4-18
Figure 4-11.	Network Configuration Page	4-20
Figure 4-12.	PPP Configuration Page	4-22
Figure 4-13.	User Accounts Page	4-23
Figure 4-14.	Entering a Master Account Password	4-24
Figure 4-15.	Page for Changing a User ID.	4-25
Figure 4-16.	Page for Changing a User Password.	4-26
Figure 4-17.	Page for Changing User Channel Privileges	4-27
Figure 4-18.	Page for Changing Your Own Password	4-28
Figure 4-19.	Security Policy Configuration Page (Security Profiles and Policy)	4-29
Figure 4-20.	Security Policy Configuration Page (bottom)	4-30
Figure 4-21.	Monitoring Configuration Page (Alert Action)	4-35
Figure 4-22.	Monitoring Configuration Page (Error Conditions to Monitor))	4-36
Figure 4-23.	Serial Port Configuration Page	4-37
Figure 4-24.	Local User/VNC Configuration Page	4-39
Figure 4-25.	Date and Time Page	4-41
-	-	

SNMP Configuration Page4-	43
OSD Menu Page	45
OSD Menu Page	46
Viewing Connection Information4-	47
Version Information Page4-	48
Capture Settings Page4-	49
Copyright Page	50
OSD Menu 5	<u>;</u> -2
Channel Switch Menu	5-4
OSD Setup Menu Screen (1 of 2) 5	<u>;</u> -5
Network Configuration Menu5	5-5
PPP Options	<u>j</u> -7
Monitoring Settings Screen (1 of 3)	j-8
Monitoring Settings Screen (2 of 3)5	<u>;</u> -9
Monitor Settings Screen – SLK16 Only (3 of 3)5-	10
Network Management Settings 5-	11
SNMP Configuration Menu	11
Syslog Configuration	12
User Administration	15
User Name Fields	15
Serial Port Configuration (Screen 1 of 2)5-	16
Serial Port 1 — Baud Rate Settings 5-	16
Serial Port 2 — Baud Rate Settings5-	17
Serial Port Configuration (Screen 2 of 2)5-	17
Serial Port 3— Baud Rate Settings5-	18
Local User Control Screen (1 of 2)5-	18
Local User Control Screen (2 of 2)5-	19
Local Console VNC Configuration Screen	<u>;</u> -2
Connection Details6	ò-2
OSD/VNC Menu with Corner Icon6	5-3
Example of a Version Number 8	3-2
Controls for Locating and Uploading Firmware	3-2
Controls for Locating and Uploading Firmware	3-4
Scientific Calculator with Binary Values E	3-2
Scientific Calculator with Hex Value E	3-2
	SNMP Configuration Page       4-         OSD Menu Page       4-         OSD Menu Page       4-         Viewing Connection Information       4-         Version Information Page       4-         Capture Settings Page       4-         Copyright Page       4-         OSD Menu       5         Channel Switch Menu       5         OSD Setup Menu Screen (1 of 2)       5         Network Configuration Menu       5         PPP Options       5         Monitoring Settings Screen (1 of 3)       5         Monitoring Settings Screen (2 of 3)       5         Monitor Settings Screen (2 of 3)       5         Monitor Settings Screen - SLK16 Only (3 of 3)       5         Network Management Settings       5         Syslog Configuration Menu       5         Syslog Configuration (Screen 1 of 2)       5         Serial Port Co

# **List of Tables**

SLK Feature Comparison2-3
Components Shipped with the SecureLinx SLK Remote KVMs 3-2
SLK1 Front Panel Description 3-3
SLK1 Back Panel Description 3-4
SLK8 Front Panel Description 3-5
SLK8 Back Panel Description 3-6
SLK16 Front Panel Description 3-7
SLK16 Back Panel Description 3-8
Web Control Interface Menus 4-6
SLK Operation Activities 4-8
Menus, Icons, and Buttons 4-10
SLK Configuration Activities
SLK Information Activities 4-44
Navigating through the OSD5-3
Values for Selecting Channels
Binary to Hex ConversionsDecimal Binary Hex

# 1: Quick Start

This Quick Start chapter describes how to get your SecureLinx<sup>™</sup> SLK Remote KVM<sup>™</sup> up and running in the shortest possible time. For detailed installation instructions, see Chapter 5, Installing the SLK. Topics in this chapter include:

Торіс	Page Number
"Getting Started"	1-1
"Making the Physical Connections"	1-2
"Powering On and Initial Configuration"	1-4
"Validating Servers"	1-5
"Where to Go from Here"	1-6

# **Getting Started**

- 1 Verify and inspect the contents of the SLK package using the enclosed packing slip or Table 3-1 on page 3-2. If any item is missing or damaged, contact your place of purchase immediately.
- 2 Rack-mount the SLK, if desired. For more information, see "Rack-Mounting the SLK" on page 3-10.
- 3 For optimum operation during remote sessions, prepare the target servers as described under "Preparing the Target Servers" on page 3-10.
- 4 To use your SLK with other KVM switches, see "Connecting KVM Switches" on page 3-16.

# **Making the Physical Connections**

The following procedure describes how to perform SLK connections. Refer to Figure 1-1 on page 1-3, Figure 1-2 on page 1-3, and Figure 1-3 on page 1-4 for visual reference.

- 1 Disconnect the monitor, keyboard and mouse from the servers or KVM-switch that your SLK is to control.
- 2 Connect the local video, keyboard, and mouse to allow local console access to the SLK and the servers or KVM-switch attached to it:
  - Connect the monitor plug to the blue 15-pin HDDB15 female port labeled Monitor.
  - Connect the keyboard plug to the round PS/2 mini-DIN female port labeled K.
  - Connect the mouse plug to the round PS/2 mini-DIN female port labeled **M**.
- 3 Connect the server monitor, keyboard, and mouse cables (removed in step 1) from the appropriate ports on the server to the appropriate channel ports on the SLK back panel:
  - Connect the monitor plug to the black 15-pin HDDB15 male port labeled Video.
  - Connect the keyboard plug to the round PS/2 mini-DIN female port labeled K.
  - Connect the mouse plug to the round PS/2 mini-DIN female port labeled **M**.

The SLK1 has one channel providing individual ports for a monitor, keyboard, and mouse. The SLK8 and SLK16 have 8 and 16 channels, respectively, with monitor, keyboard, and mouse ports for each channel. For these models, start your connections at CH-1, then CH-2, and so on.

# *Note:* SLK1 and SLK8 only support 2-button mice. The SLK16 is compatible with 2-button wheel mice.

- 4 Connect the SLK KVM to the network using the 10/100Base-T Ethernet port (RJ45) labeled **Network**.
- 5 To remotely control serial devices, configure the serial port(s) to suit your needs. All SLK models provide two serial ports for power control, Telnet, and logging functions. The SLK16 has a third serial port that can connect to an external modem for out-of-band access.

*Note:* The second serial port on the SLK1 and SLK8 is an 8-pin mini-DIN connector that requires the supplied 8-pin–to–DB9 adapter.

6 Connect the supplied power cord to the SLK's AC receptacle and to a power source.

#### Figure 1-1. SLK1 Back Panel



#### Figure 1-2. SLK8 Back Panel



**RJ45 Network Connector** 

#### Figure 1-3. SLK16 Back Panel



# **Powering On and Initial Configuration**

1 Power on the equipment in the following sequence: start with any KVM switches cascaded in front of your SLK, followed by your SLK, and then by attached servers and any converters or extenders.

Scroll

- 2 At the local keyboard, press the key twice.
- 3 When the On Screen Display opens, scroll down to Setup Menus and press Enter.
- 4 Select Network Configuration and press Enter.
- 5 From the Network Configuration page, assign an IP address to your SLK. Write down this number, as you will need to use it in step 1 under "Validating Servers."
- 6 If you want your SLK to communicate outside the Local Area Network (LAN), set the default gateway.
- 7 Select **Commit IP config changes** and press **Enter** to commit your changes.

# **Validating Servers**

After you configure your SLK, connect a PC to it via a TCP/IP connection:



Verify each server's remote performance:

- 1 Start your web browser and enter the SLK's IP address in the address bar. User name and password prompts display.
- 2 Type the default user name **root** in lower-case characters and type the default password **PASS** in upper-case characters; then click **OK**. The SLK home page opens.
- 3 Under **Channel (click to view**), click the first channel (the channel in the top row).
- 4 Verify that you can view the video. If you see **NO INCOMING VIDEO**, see "Video Troubleshooting" on page 7-8.
- 5 Move the mouse and verify that the on-screen pointer moves as you move the mouse. If it does not, see "Mouse Troubleshooting" on page 7-5.
- 6 Click the **Back** button in your browser to return to the SLK home page.
- 7 Click the channel on the next row and repeat steps 4 through 6. Repeat this step for all the remaining channels that are being used.

# Where to Go from Here

Following the initial configuration and verification, set up users and security parameters.

There are two ways to configure your SLK:

- Using its embedded web control interface
- Using the local console's On Screen Display (OSD) interface

The web control interface provides a graphical interface that lets you configure your SLK and control the target servers and other connected devices using a standard web browser. For more information, see Chapter 4, "Using the Web Control Interface to Configure the SLK."

The OSD configuration method provides a text-based interface with minimal prompting and guidance. For more information, see "Using the OSD Interface to Configure the SLK."

After you configure your SLK, you can:

- Change the master account password. See "Changing the Master Account Password" on page 4-23.
- Check for updated firmware. See "Uploading Firmware" on page 8-1.
- Upload the proper encryption certificate and key into the SLK Flash File if you want to use encryption. See "Using Security and Encryption" on page 8-3.

*Note:* For answers to frequently asked questions about the SecureLinx SLK Remote KVMs, please visit <u>www.lantronix.com/support</u>.

# 2: Introduction

This chapter provides introductory information about your SecureLinx SLK Remote KVM. Topics in this chapter include:

Торіс	Page Number
"Overview"	2-1
"SecureLinx SLK Models"	2-2
"Features and Benefits"	2-3
"SLK Configurations"	2-4

## **Overview**

SecureLinx is a family of remote server-management solutions that enable remote clients to efficiently control their target servers and serial devices over a Local Area Network (LAN) or the Internet using the standard Transmission Control Protocol/Internet Protocol (TCP/IP). Secure remote access is provided through any web browser by entering the SLK's IP address. Once access is granted, remote clients can perform activities such as resetting the target hardware, accessing the Basic Input Output System (BIOS), gaining keyboard and mouse control, and cycling power — as if they were accessing the server locally.

*Note:* VNC can also be used for remote access. However, because VNC does not support encryption, it does not provide a secure connection unless used with a Virtual Private Network (VPN) or Secure Shell (SSH).

SecureLinx SLK Remote KVMs also provide automatic monitoring and notification capabilities that notify you of problematic symptoms in your network environment before they become critical. This break-through technology makes the SLK an essential component of your server crisis-management infrastructure by giving you the power to quickly recover from mission-critical server failures anywhere in the world.

SecureLinx SLK Remote KVMs also save you money by eliminating redundant peripherals (such as keyboards, monitors, and mice) and providing centralized control of multiple servers. Best of all, SecureLinx SLK Remote KVMs are plug-and-play solutions that require no additional hardware or software, making initial setup quick and simple. This non-intrusive approach means the SLK does not consume valuable server resources while, at the same time, minimizes potential points of failure.

With a small investment, SecureLinx SLK Remote KVMs can preserve precious office space, centralize the management of your servers and serial devices, slash redundant peripheral costs, and increase uptime and productivity.

# SecureLinx SLK Models

SecureLinx SLK Remote KVMs come in three models:

- SLK1 lets local and remote users control 1 server.
- SLK8 lets local and remote users control up to 8 servers.
- SLK16 lets local and remote users control up to 16 servers.

## SLK1

The SLK1 provides one local user and multiple remote users with "shared" access to one server. All users have simultaneous access to the single server. Because this access is shared, only one user should control the server at a time. The SLK1 has two serial ports.

## SLK8

The SLK8 provides one local user and multiple remote users with access to up to eight servers. The SLK8 supports independent operation between the local user and remote users. This allows the local user to perform tasks independently of remote users. For example, the local user might access the server on channel 1, while remote users access the server on channel 2 at the same time.

By contrast, all remote users are dependent on each other. If a remote user changes the view from the server on channel 2 to the server on channel 3, for example, all other remote users view the channel 3 server.

The SLK8 has two serial ports.

## SLK16

The SLK16 provides one local user and multiple remote users with access to up to 16 servers. The SLK16 supports up to 6 independent remote sessions. This allows the local user and up to six remote users to perform simultaneous tasks independently of each other. They can all access the same server or servers on different channels.

The SLK16 also allows a remote user to "lock down" his server channel for his use only. Locking down a channel privatizes the session, preventing the channel from being accessed by other users. When a channel is locked, only the user who locked it and the SLK administrator can unlock the channel.

The SLK16 has three serial ports.

## **Features and Benefits**

#### Features at a Glance

Table 2-1 summarizes the features of the three SLK models.

#### Table 2-1. SLK Feature Comparison

Feature Description		SLK8	SLK16
Number of server ports	1	8	16
Number of independent remote clients	1	1	6
Number of multipurpose serial ports	2	2	3
Number of user profiles	32	32	32
Monitors video output of all servers simultaneously	No	Yes	Yes
Ability to assign server access for each individual user	No	Yes	Yes
Dial-up access via third serial port	No	No	Yes
Rack size	1U	1U	2U

#### **Feature Descriptions**

#### Anytime, Anywhere Access

SecureLinx SLK Remote KVMs provide centralized control for managing multipleserver environments. Depending on the model, the SLKs can provide remote KVM access to 1, 8, or 16 servers via the Internet or Local Area Network. SLK units can also be daisy-chained with KVM switches to control more servers.

Access is provided through a standard web browser or free VNC software. The SLK16 also provides dial-up modem access.

#### **Complete Control**

SecureLinx SLK Remote KVMs provide simultaneous server access to a local user and multiple remote users. They deliver full BIOS-level control, with remote power cycling and power on/off. They also provide 2 or 3 programmable serial ports, depending on the model. For convenience, the SLKs support user-configurable hotkeys for providing instant access to the On Screen Display (OSD).

#### Advanced Security for Total Control Over System Access

SecureLinx SLK Remote KVMs offer a compete solution. They require no additional software or hardware, and are completely non-intrusive, with minimal impact on servers.

All keyboard and mouse data is fully encrypted with 128-bit Secure Sockets Layer (SSL) encryption. In addition, SecureLinx SLK Remote KVMs support multi-layer

users/passwords and upgradeable public-key certificates. VPN and SSH environments can be used to provide external encryption to support existing security policies. In addition, the SLK provides "Turtle Mode" and "Stealth Mode." These automated security features serve to hide the SLK on a network and provide the ability to shut down the SLK if it is attacked by hackers.

#### **Superior Performance**

SecureLinx SLK Remote KVMs deliver unparalleled performance through state-of-theart compression algorithms, low bandwidth consumption, and high-performance mouse tracking and synchronization. They also monitor servers and notify users if a connected server encounters problems.

#### Easy Setup

SecureLinx SLK Remote KVMs offer true plug-and-play simplicity. They are compatible with most KVM switches and operating systems.

Configuration is performed through an intuitive web interface, with point-and-click access to all servers through a web browser.

## **SLK Configurations**

The following sections illustrate the various network configurations in which the SLKs can be used.

## Connecting to the Same Network and Switch as the Server

Figure 2-1 shows an SLK connected to the same Ethernet and Switch as the server.

Figure 2-1. Connecting to the Same Network and Switch as the Server



## **Connecting to Different Switches**

In Figure 2-2, the SLK and server are connected to different switches.





## **Multiple Server Configurations**

SecureLinx SLK Remote KVMs can connect to an existing KVM switch, as shown in Figure 2-3. During the initial setup, you connect a keyboard, monitor, and mouse to the SLK local port. After the initial setup is complete, you can leave the keyboard, monitor, and mouse connected to the local port for local monitoring.



Figure 2-3. Multiple Server Configuration without Firewall

Figure 2-4 shows another multiple-server configuration. This example includes a firewall. In this example, the SLK continues to monitor the servers, even if the firewall fails or the connection to the firewall goes down.



Figure 2-4. Multiple Server Configuration with Firewall

*Note:* If the KVM switch requires a USB connection to the SLK, you need an appropriate USB-to-PS/2 adapter.

# 3: Installing the SLK

This chapter describes how to install SecureLinx SLK Remote KVMs. Topics in this chapter include:

Торіс	Page Number
"Unpacking Your Components"	3-1
"Items Supplied by the User"	3-2
"Hardware Description"	3-3
"Installing the SLK"	3-10
"Validating Target Servers"	3-18
"Where to Go from Here"	3-21

# **Unpacking Your Components**

Verify and inspect the contents of the SLK package using the enclosed packing slip or Table 3-1. If any item is missing or damaged, contact your place of purchase immediately.

SLK Model	Package Components
SLK1	SecureLinx SLK1 1-port Remote KVM
	<ul> <li>U.S. power cord (500-041)</li> </ul>
	Serial "Y" mini-DIN8–to–RJ12/DB9F cable (SLKCHY001-01)
	Six-foot, 3-in-1 KVM, PS/2 cable (SLKCHS006-01)
	SecureLinx SLK Remote KVM User Guide
SLK8	SecureLinx SLK8 8-port Remote KVM
	<ul> <li>U.S. power cord (500-041)</li> </ul>
	Rack-mount brackets (SLKB08000-01)
	Serial "Y" mini-DIN8–to–RJ12/DB9F cable (SLKCHY001-01)
	SecureLinx SLK Remote KVM User Guide
SLK16	SecureLinx SLK16 16-port Remote KVM
	<ul> <li>U.S. power cord (500-041)</li> </ul>
	Rack-mount brackets (SLKB16000-01)
	SecureLinx SLK Remote KVM User Guide

Table 3-1. Components Shipped with the SecureLinx SLK Remote KVMs

# Items Supplied by the User

In addition to the items in your package, you need the following items to install your SLK:

A keyboard, monitor, and mouse for local console access:

- The keyboard and mouse should have PS/2 cables or equivalent adapters.
- The monitor should have a standard 15-pin VGA male-to-female cable.
- A standard Cat 5 network patch cable for connecting the SLK to your network.

**Note:** The SLK8 and SLK16 models also require the user to provide the appropriate keyboard, mouse, and video cables (such as part number SLKCHS006-01) to attach the target servers.

The following items are optional:

- Serial devices and cables, if you want to control serial devices with the SLK.
- A KVM switch.
- A 19-inch rack and mounting hardware, if you want to rack-mount the SLK. For more information, see "Rack-Mounting the SLK" on page 3-10.

## **Hardware Description**

The following sections describe the front and back panels of the SLK1, SLK8, and SLK16.

## **SLK1 Front and Back Panels**

Figure 3-1 shows the front panel of the SLK1, and Table 3-2 describes the front panel components.



#### Figure 3-1. SLK1 Front Panel

#### Table 3-2. SLK1 Front Panel Description

1	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection
2	Link/Activity LED: ON = good connection OFF = no connection Blinking = network activity

Figure 3-2 shows the back panel of the SLK1, and Table 3-2 describes the back panel components.

Figure 3-2. SLK1 Back Panel



Table 3-3. SLK1 Back Panel Description

1	SLK power connector
2	Serial port 1 (DB9 female, DCE)
3	Recessed reset button. Use a paper clip (or equivalent) to reset the SLK. Does not affect attached server. This unit only controls one device.
4	One group of Local connectors for connecting a local console. Each connector is labeled and color coded. M/green PS/2 mouse connector (6-pin mini-DIN female) K/purple PS/2 keyboard connector (6-pin mini-DIN female) Monitor/blue VGA monitor connector (HDDB15 female)
5	One group of <b>Server</b> connectors for managing the target server or attached KLM. Each connector is labeled and color coded: <b>M/green</b> PS/2 mouse connector (6-pin mini-DIN female) <b>K/purple</b> PS/2 keyboard connector (6-pin mini-DIN female) <b>Video/black</b> VGA monitor connector (HDDB15 male)
6	Serial port 2 (8-pin mini-DIN, DCE)
7	Red and green indicator lights that alternate during normal operation
8	Link/Activity LED: ON = good link connection OFF = no link Blinking = network activity
9	RJ45 network connector.
10	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection

## **SLK8 Front and Back Panels**

Figure 3-3 shows the front panel of the SLK8 and Table 3-4 describes the front panel components.







1	Eight remote channel LEDs show which remote channel is active.
2	Eight local LEDs show which local channel is selected for local moni- toriing.
3	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection
4	Link/Activity LED: ON = good connection OFF = no connection Blinking = network activity
5	Eight push-buttons for selecting the local channel.To select a chan- nel, a local user can use the On Screen Display (OSD) or press the front panel push-button under the desired channel.

Figure 3-4 shows the back panel of the SLK8, and Table 3-5 describes the back panel components.

Figure 3-4. SLK8 Back Panel



Table 3-5. SLK8 Back Panel Description

1	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection			
2	Serial port 1 (DB9 female, DCE).			
3	Recessed reset button. Use a paper clip (or equivalent) to reset the SLK. Does not affect attached server. This unit only controls one device.			
4	Eight groups of <b>Server</b> connectors, labeled <b>CH-1</b> through <b>CH-8</b> , for managing up to eight target servers. Each connector is labeled and color coded:			
	M/green PS/2 mouse connector (6-pin mini-DIN female)			
	K/purple PS/2 keyboard connector (6-pin mini-DIN female)			
	Video/black VGA monitor connector (HDDB15 male)			
5	One group of <b>Local</b> connectors for connecting a local console. Each connector is labeled and color coded.			
	M/green PS/2 mouse connector (6-pin mini-DIN female)			
	K/purple PS/2 keyboard connector (6-pin mini-DIN female)			
	Monitor/blue VGA monitor connector (HDDB15 female)			
6	Serial port 2 (8-pin mini-DIN, DCE)			
7	Red and green indicator lights that alternate during normal operation			
8	Link/Activity LED: ON = good link connection OFF = no connection Blinking = network activity			
9	RJ45 network connector			
10	SLK power connector			

# **SLK16 Front and Back Panels**

Figure 3-5 shows the front panel of the SLK16, and Table 3-6 describes the front panel components.





#### Table 3-6. SLK16 Front Panel Description

1	Link/Activity LED: ON = good connection OFF = no connection Blinking = network activity
2	Sixteen remote channel LEDs show which remote channels are active. Up to six LEDs (six users) can be active at one time.
3	Sixteen local LEDs show which local channel is selected for local monitoring. To select a channel, a local user can use the OSD or the press the front panel push-buttons.
4	Front panel push-buttons lets you connect to one of 16 local channels. Press the left button to move down and the right button to move up.
5	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection

Figure 3-6 shows the back panel of the SLK16 and Table 3-7 describes the back panel components.



Table 3-7. SLK16 Back Panel Description

1	Serial port 2 (DB9 female, DCE)		
2	Serial port 1 (DB9 female, DCE)		
3	Recessed reset button. Use a paper clip (or equivalent) to reset the SLK. Does not affect attached servers		
4	10/100 Speed LED: <b>Green</b> = 100 Base-T connection <b>Orange</b> = 10 Base-T connection		
5	RJ45 network connector.		
6	Link/Activity LED: ON = good link connection OFF = no link Blinking = network activity		
7	Sixteen groups of <b>Server</b> connectors, labeled <b>CH-1</b> through <b>CH-16</b> , for managing up to 16 target servers. Each connector is labeled and color coded:		
	M/green PS/2 mouse connector (6-pin mini-DIN)		
	K/purple PS/2 keyboard connector (6-pin mini-DIN female)		
	Video/black VGA monitor connector (HDDB15 male)		

8	One group of <b>Local</b> connectors for connecting a local console. Each connector is labeled and color coded.	
	M/green PS/2 mouse connector (6-pin mini-DIN female)	
	K/purple PS/2 keyboard connector (6-pin mini-DIN female)	
	Monitor/blue VGA monitor connector (HDDB15 female in blue)	
9	Serial port 3 (DB9 male, DTE)	
10	SLK power connector	

# **Installing the SLK**

Installing the SLK consists of the following steps:

- 1 Install the SLK in a rack to use it in a rack-mount configuration. See "Rack-Mounting the SLK" below.
- 2 Prepare the target servers. See "Preparing the Target Servers" below.
- 3 Connect the local keyboard, monitor, and mouse and cables for the target servers that are to be remotely controlled. See "Connecting Devices to the SLK" on page 3-13.
- 4 Connect the SLK to your network. See "Connecting to the Network" on page 3-16.
- 5 Optional: connect serial devices to the SLK. See "Connecting Serial Devices" on page 3-16.
- 6 Connect the SLK to a power source. See "Connecting to a Power Source" on page 3-17.

## **Rack-Mounting the SLK**

To rack-mount the SLK, place it in a suitable 19-inch rack (the SLK1 and SLK8 are 1U in size, while the SLK16 is 2U). The SLK8 and SLK16 come with their own mounting hardware. Mounting hardware for the SLK1 can be ordered from Lantronix.

When rack-mounting the SLK units, place the rack in a dry, well-ventilated location, with a minimum of dust and vibration. Leave at least 1 inch of clearance on each side of the unit for air to circulate. (Units run hotter when in a rack than when operating as standalone devices.)

## **Preparing the Target Servers**

For optimum operation and performance, use the following guidelines to configure the target servers as recommended in the following sections.

## **Optimizing the System**

To optimize the attached servers, use the following guidelines:

- Remote access can introduce a measure of latency, and a user is likely to see a delayed response to mouse or keyboard input. Enabling features that slow the boot process (such as seek floppy, enhanced startup testing, and enhanced memory testing) increase the opportunity to send a keybound signal to enter the BIOS mode of an attached server.
- If you are using an optional third-party power control unit, access the system's Basic Input/Output System (BIOS) and enable Power on state upon power recovery.

#### **Optimizing Video**

For optimum viewing during remote sessions, use the following guidelines to configure the video resolution settings on the servers that the SLK will control:

- Make sure all monitors and adapters are VESA-compliant.
- Select a video resolution of 1280 x 1024 or less.
- Select a refresh rate of 75 Hz or below.
- Install the latest video drivers from the original manufacturer.
- Disable energy savings, suspend, and hibernation modes.
- Turn off screen savers.
- Unclutter the desktop by choosing a solid-color background with minimal icons.
- Disable animations and video effects such as fade out and show content when dragging.

#### **Adjusting Your Mouse**

For optimum mouse control during remote sessions, use the following guidelines to configure the mouse settings on the servers that the SLK will control:

- Use generic mouse drivers only. Avoid elaborate "ergonomic" drivers.
- Recommended mouse pointer speed: depends on the server operating system (see Figure 3-7).

Windows 98	Windows 2000
Set pointer speed to slowest, and leave trails on.	Set motion to Slow, acceleration to none.
Duttons   Pointers   Motion	Speed
Pointer speed	Adjust how fast your pointer moves
Slow Fast	Slow Fast
Pointer trail	Acceleration
SSS: Show pointer trails	Adjust how much your pointer accelerates as
Short Long	
	• None C Low C Medium C High
Windows NT	Windows ME
Set motion to Slow.	Adjust pointer to midrange speed. Turn off Accelerator
Mouse Properties	Mouse Properties
Ruttered Baisters Motion Consert	Buttons Pointers Pointer Options
	Pointer speed
Pointer speed	Adjust how fast your pointer moves: Accelerate.
Slow	
S	SpapTo-
Windows XP	Silicon Graphics Inc IR IX
Set pointer speed to medium. Unlock Enhance.	Adjust acceleration below midrange. Set threshold low.
Mouse Properties	
Buttons Pointers Pointer Options Wheel Hardware	Mouse Acceleration:
Motion	Slow - Fast Finer Control
Select a pointer speed:	Acceleration
Slow Fast	Acceleration
Enhance pointer precision	
Linux	
Set acceleration to medium, set threshold to medium.	
C Left handed Acceleration	
Right handed     Slow     Fast	
Threshold	
Sman Large	
Or, on the command line, set acceleration and threshold	
Dy xset mouse 11 .	

Figure 3-7. Recommended Mouse Settings for Target Servers

*Note:* SLK1 and SLK8 only support 2-button mice. The SLK16 is compatible with 2-button wheel mice.
## **Connecting Devices to the SLK**

The following sections describe how to connect devices to the SLK. Refer to Figure 3-8, Figure 3-9, and Figure 3-10 for visual reference.

#### **Preparing the Servers**

Use the following procedure to prepare the target servers that the SLK is to manage.

- 1 Optimize the servers according to the recommendations under "Preparing the Target Servers" on page 3-10.
- 2 Power-down all equipment that will be connected to the SLK.
- 3 Disconnect the monitors, keyboards, and mice from the servers that the SLK will manage.

#### Connecting a Local Keyboard, Video, and Mouse

Before you perform the target server connections, connect the video, keyboard, and mouse to the local ports on the SLK back panel. These connections let you perform administrative tasks. They also let you control the attached servers using a single monitor, keyboard, and mouse on the local console.

- 1 Connect the monitor plug to the blue HDDB15 female port labeled **Monitor**.
- 2 Connect the keyboard plug to the purple PS/2 port labeled K.
- 3 Connect the mouse plug to the green PS/2 port labeled **M**.

#### **Connecting Target Servers to SLK**

Use the following procedure to connect servers to the SLK back panel.

*Note:* For low noise and reduced wiring clutter, use Lantronix-suggested KVM cables to connect target servers to the SLK.

#### Installing the SLK

- SLK1 1 Connect the mouse to the green PS/2 mini-DIN female connector labeled M.
  - 2 Connect the keyboard to the purple PS/2 mini-DIN female connector labeled K.
  - 3 Connect the monitor plug to the black HDDB15 male connector labeled Video.

The SLK1 manages one server. Server connections are made using the mouse, keyboard, and video connectors under **Server** (see Figure 3-7).

# SLK8 and SLK16

The SLK8 and SLK16 use 8 and 16 channels to manage 8 and 16 servers, respectively. The channels are labeled **CH-1** through **CH-8** on the SLK8 (see Figure 3-10) and **CH-1** through **CH-16** on the SLK16 (see Figure 3-11). Each channel has a set of mouse, keyboard, and video connectors. When you connect target servers, start with **CH-1**, then **CH-2**, and so on.

#### Figure 3-8. SLK1 Connections



#### Figure 3-9. SLK8 Connections



#### **Connecting KVM Switches**

You can connect KVM switches to the SLK to increase the number of target servers that can be controlled. To connect a KVM switch, attach the mouse, keyboard, and monitor connector from a server port on the SLK to the appropriate uplink connectors on the KVM switch (the manual that came with the KVM switch should describe this procedure). For a list of compatible KVM switches, please visit our Web site at www.lantronix.com.

To optimize the use of KVM switches:

- Disable or time-out any permanent video overlays showing KVM switch status
- Coordinate the defined hotkeys on the SLK or the KVM switch to avoid any conflicts between them. See Chapter 9, "Defining Custom Send Keys".

#### **Connecting to the Network**

After connecting a local console, connect the SLK to your network.

- 1 Plug one end of an RJ45 cable into the SLK 10/100 BaseT Ethernet port labeled **Network**.
- 2 Connect the other end of the cable to your network.

#### **Connecting Serial Devices**

The SLK back panel provides serial connectors for serial devices to be remotely controlled. All SLK models have two serial ports, labeled **Serial 1** and **Serial 2**.

- Serial 1 is a DB9 female connector configured as Data Communications Equipment (DCE).
- Serial 2 (SLK1 and SLK8) is an 8-pin, mini-DIN, female connector configured as DCE. To use this serial port, attach the supplied 8-pin-to-DB9 adapter. On the SLK16, it is a DB9 (just like serial 1).
- Serial 3 (SLK16) has a third serial port, labeled Serial Port 3 Modem. It is a DB9 male connector configured as Data Terminal Equipment (DTE). This serial port supports the Point-to-Point Protocol (PPP). Connecting an external modem to this port allows a remote dial-up client to access the SLK.

Serial port 1 and serial port 2 support the following activities:

- SLK log relays system log events to a serial device.
- Telnet lets remote users establish a Telnet session with a serial device through the SLK.

- Watchdog monitors the status of a server. A server data stream into the serial port is examined for a match with a string pattern that must occur within a set time interval or an alert will be issued. The pattern, interval, and alert are all user-configurable.
- Power Control connects to an optional Lantronix SLP Remote Power Manager to turn power off or on at the controlled device.

# **Connecting to a Power Source**

To connect the SLK to a power source:

- 1 Connect the supplied power cord to the SLK AC receptacle.
- 2 Power-on any KVM switches cascaded in front of the SLK.
- 3 Power on the SLK followed by attached servers and any converters or extenders.

# **Validating Target Servers**

After you make your SLK connections, use the following procedure to configure the network settings and to validate the performance of the target servers.

- 1 At the local keyboard, press the key twice.
- 2 When the On Screen Display opens, scroll down to Setup Menus and press Enter.
- 3 Select Network Configuration and press Enter.
- 4 From the Network Configuration page, assign an IP address to the SLK. Write down this number. You will need to use it in step 7.
- 5 If you want the SLK to communicate outside the Local Area Network (LAN), you must set the default gateway.
- 6 Select **Commit IP config changes** and press **Enter** to commit your changes.
- 7 Use a PC connected to the network (not the Local Console) to connect to the SLK (see Figure 3-11). Start your web browser and enter the SLK's IP address in the address bar. A screen prompts you for a user name and password.



Figure 3-11. Connecting a Notebook PC to the SLK

8 Type the default user name **root** in lower-case characters and the default password **PASS** in upper-case characters; then click **OK**. The SLK home page opens (see Figure 3-12).

control Hosts	SLK16 web control in	terface		
iew Hasts	Channel (click to view)	Configuration	Power	
ower Control	11 SupportPDC	Configure	On	
vent Log	21.RHURUN	Configure	On	
ash File System	3: Win2003Server	Configure	On	
ebug	4: DanKPC	Configure	On	
nfiguration	5: Noname	Configure	off	
etwork:	6: Noneme	Configure	Off	
np Inc Accounts	7: NT4Server	Configure	On	
hange Password	8: SupportBDC	Configure	On	
ecurity	9: Solaris9 Vitras	Configure	On	
onitoring	10: Noname	Configure	Off	
erial Ports	11: NetwareS	Configure	On	
ate & Time	12: Noname	Configure	Off	
slog	12: Noname	Configure	off	
IMP	14: Noname	Configure	Off	
ormation	15: Noname	Configure	Off	
ull Menu Tree	16: Noname	Configure	Off	
rowse Menu Tree onnection ersion	Start a new browser window to control a H	ost.		
opyright	Start a new fullscreen browser window to c	control a Host. You may ne	ed to use Alt-F4 to get ou	t of this special windo
	If the VNC (Virtual Network Computer) clier	it software is installed on y	our machine, you can also	connect using:
	172.19.0.216:5900			

Figure 3-12. SLK Home Page

- 9 Under Channel (click to view), click the first channel (the channel in the top row). In Figure 3-12, the first channel is Support PDC (for demonstration purpose only).
- 10 Verify that you can view the video (see Figure 3-13). If you can, proceed to the next step. Otherwise, perform the following steps:
  - If the video is noisy, click Blank Screen in the left pane (under the Misc menu) to assess the video noise buildup.
  - If the video is not properly detected or is noisy, click Optimize Video in the left pane (under the Advanced menu) to adjust to the appropriate resolution.
  - If none of these suggestions helps, see "Video Troubleshooting" on page 7-8.



Figure 3-13. Example of Viewing Video from a Remote Server

Figure 3-14. Example of No Incoming Video Message



11 Test the mouse and keyboard functionality. If the on-screen pointer moves satisfactorily as you move the mouse, proceed to the next step. Otherwise, click **Resync Mouse** in the left pane (the upper left-most button). Then move the mouse again to see whether the pointer movement has improved. If it has, proceed to the next step. If this does not help, see "Mouse Troubleshooting" on page 7-5. Open a

text-editing application and perform a keyboard functionality test to confirm operation.

- 12 Click the **Back** button in your browser to return to the SLK home page.
- 13 Click the channel on the next row and repeat steps 10 through 12. Continue this process for all the remaining channels that are being used.
- 14 In the left pane, under **Configuration**, click **User Accounts**. The User Accounts screen opens.
- 15 Enter a new master account password in the first text box. Then enter the same password in the second text box next to it. For security reasons, each typed character appears as a dot.

*Note:* Store the new master account password in a safe place. If you lose or forget it, contact Lantronix Technical Support.

- 16 Click Change.
- 17 Follow the instructions on the SLK home page to view the current screen contents and take control of the host's keyboard and mouse. You can open a new window to view the screen contents or start a new full screen browser

window. You may need to use the



keys to exit the window.

*Note: For future troubleshooting, see Chapter 7, "Troubleshooting" on page 7-1.* 

# Where to Go from Here

Following the initial configuration and verification, set up users and security parameters.

There are two ways to configure your SLK:

- Using its embedded web control interface.
- Using the local console's On Screen Display (OSD) interface.

The web control interface provides a graphical interface that lets you configure your SLK and control the target servers and other connected devices using a standard web browser. For more information, see Chapter 4, "Using the Web Control Interface to Configure the SLK."

The OSD configuration method provides a text-based interface with minimal prompting and guidance. For more information, see Chapter 5, "Using the OSD Interface to Configure the SLK".

After you configure your SLK, you can:

- Check for updated firmware. See Chapter 8, "Uploading Flash Files and Certificates".
- Upload the proper encryption certificate and key into the SLK Flash File if you want to use encryption. See "Using Security and Encryption" on page 8-3.

*Note:* For answers to frequently asked questions about the SecureLinx SLK Remote KVMs, please visit www.lantronix.com/support.

# 4: Using the Web Control Interface to Configure the SLK

This chapter describes how to use the web control interface to configure SecureLinx SLK Remote KVMs and control the attached servers. Topics in this chapter include:

Торіс	Page Number
"Overview"	4-1
"Starting a Session"	4-2
"Understanding the Web Control Interface"	4-4
"Performing Operation Activities"	4-8
"Performing Configuration Activities"	4-19
"Performing Information Activities"	4-44

# **Overview**

SecureLinx SLK Remote KVMs provide a graphical, web-based control interface that lets you control servers and other connected devices. This interface is compatible with most standard browsers.

To access the web control interface, your browser must support cookies. The SLK will not start a session until you configure your browser to accept cookies.

*Note:* The web pages shown in this chapter are for the SLK16. If significant differences exist between these pages and those of other SLK models, they are identified.

# **Starting a Session**

To access the web control interface, use the following procedure:

- 1 Start a web browser from a computer that is on the same subnet as the SLK.
- 2 Enter the SLK's IP address into the address bar of your web browser. A login window similar to the one in Figure 4-1 opens. The proper syntax is http://111.222.333.444 (substitute your SLK's IP address for the numeric portion).

*Note:* If this procedure fails, ensure that the computer is on the same LAN segment as the SLK and that the SLK does not have an IP address that is already in use by another device on the subnet.

Connect to 216.254	.154.11 ? 🗙
	GP
216.254.154.11	
User name:	🔮 root 💌
Password:	
	Remember my password
	OK Cancel

Figure 4-1. Login Window

- 3 For **User Name**, type the default user name **root** in lower-case characters.
- 4 For **Password**, type the default password **PASS** in upper-case characters.
- 5 Click the **OK** button. The SLK home page displays (see Figure 4-2).

*Note:* The following figure is accurate for the SLK16, but not for the SLK8 or SLK1.

Configuration Configure Configure Configure Configure Configure Configure Configure Configure Configure Configure	Power On On On Off Off On On
Configure Configure Configure Configure Configure Configure Configure Configure Configure	On On On Off Off On On
Configure Configure Configure Configure Configure Configure Configure Configure	On On Off Off On On
Configure Configure Configure Configure Configure Configure Sonfigure	On On Off Off On On
Configure Configure Configure Configure Configure Configure	On Off On On
Configure Configure Configure Configure Configure	Off Off On On
Configure Configure Configure Configure	Off On On
Configure Configure Configure	On On
Configure	On
Configure	
	Ón
Configure	Off
Configure	On
Configure	Off
may need to use Alt-F4 to g led on your machine, you car	et out of this specia n also connect using
	may need to use Alt-F4 to g led on your machine, you car <u>Home 1 Back 1 Logo</u> ht © Lantronis, Inc. 2004. All J

Figure 4-2. SLK Home Page

The home page is your starting location for configuring the SLK and the attached servers. It displays all the channels supported by your SLK and the power status of each. The **Configuration** column provides a **Configure** link that lets you apply configuration parameters you select during your session on a per-channel basis.

At the bottom of the home page are links for starting a new browser window to control a host and starting a new full-screen window to control a host.

You can return to the home page by double-clicking the house icon ( ) above the left menu pane. The next section describes this icon as well as the other components in the web control interface.

# **Understanding the Web Control Interface**

The web control interface consists of a menu pane and a main viewing area. The menu pane is along the left side of the page. It organizes activities into three categories:

- **Operation** lets you perform various tasks such as controlling and viewing hosts.
- Configuration lets you set up the SLK to suit your requirements. To get the SLK up and running, you must perform two configuration tasks: specify the SLK network settings and set up users.
- Information lets you view information such as menu trees or a connection.

Each category contains links to HTML pages in the SLK's web control interface. These pages cover all aspects of configuration and operation of the target servers and attached devices. For a description of these pages, see Table 4-1 on page 4-6.

Above the menu pane is a home page icon. You can click this icon to return to the SLK home page. To the right of this icon is the **Logout** button. Click this button to log out of the current web control interface session.

At the bottom of each page are a **Home** link for returning to the SLK home page, a **Back** link for returning to the previous page displayed, and a **Logout** link for logging out of the current session. There is also a link to the Lantronix web site.

**Note:** In addition to the controls in the web control interface, you can also use the **Back** and **Forward** buttons in your browser to move backward and forward.

	Operation	SLK16 web control in	terface		
gout	View Hosts	Channel (click to view)	Configuration	Power	
tton	Power Control	1: SupportPDC	Configure	Ori	
	User Activity	2: RHLINUX	Configure	On	
	Flach File System	3: Win2003Server	Configure	On	
	Debug	4: Dankec	Configure	On	
	Configuration	S: Noname	Configure	Off	
	Network	6: Noname	Configure	Off	
nu	PPP	7: NT4Server	Configure	On	
ne	Obende Password	8: Support6DC	Configure	On	
	Security	9: Solaris9 Ultras	Configure	On	
	Monitoring	10: Noname	Configure	Off	
	Senal Ports	11: Netware5	Configure	On	
	Date & Time	12: Noname	Configure	off	
	Syslog	13: Noname	Configure	Off	
	SNMP	14: Noname	Configure	Off	
	Information	15: Noname	Configure	Off	
	Full Menu Tree	16: Noname	Configure	Off	
L	Connection Version Capture Settings Copyright	Start a new browser window to control a H Start a new fullscreen browser window to c If the VNC (Virtual Network Computer) clien 172 <mark>19,0:216:5900 Copyrig</mark>	ast. sontrol a Host. You may ne it software is installed on y Home I Back I Lo Home I Back I Lo Diantomix. Ind. 2004. A	ed to use Alt-F4 to get rour machine, you can i pout Biohts Reserved.	t out of this special wind also connect using:
	SLK Home P	age Link htronix Web Sit <del>e</del>	nt to <u>Lantroniz</u> , Inc. 2004. A	n rugnits Keserved.	

# Figure 4-3. Web Control Interface Page Components

Menu	Description	See Page			
Operation					
Control Hosts	Initiates a JavaView session without an active channel being selected.	4-9			
View Hosts (SLK16 only)	Displays server desktops in one of the four preset views for monitoring.	4-12			
Power Control	Displays channel power outlet names and lets you power-off, power-on, and reset individual outlets, if an optional SLP Remote Power Manager is installed and configured on a serial port.	4-13			
Jser ActivityDisplays the user activity history (for example, user name, session type, login and idle times, and IP information).					
Event Log	Displays the event log history.	4-16			
Flash File System	Displays a list of internal SLK system files and applets used to upgrade these files. Provides access to keyboard/mouse emula- tion firmware and tools to save or reload system configuration.	4-17			
Debug	Helps you to reset, maintain, and to calibrate video and key- boards, and load configuration files. This option is for Technical Support use only.	4-18			
Configuration					
Network	Helps you to understand and configure the network connection.	4-19			
PPP	Lets you set up a dial-up modem as a backup strategy.	4-21			
User Accounts	Displays user names, passwords, and account information and lets the Administrator set user-access privileges for each chan- nel.	4-23			
Change Password	Enables users to change their own passwords.	4-28			
Security	Sets profiles and policies for logout time, Turtle, Stealth, and other functions.	4-29			
Monitoring	Sets error conditions and responses.	4-35			
Serial Ports	Sets operating mode, baud rate, power, and other serial port functions.	4-37			
Local User/VNC	Sets VNC port, mouse threshold, and exit key for OSD as well as VNC.	4-39			
Date and Time	Sets the SLK internal clock and time zones to the remote values.	4-41			
Syslog	Lets you set the configuration of basic Syslog parameters.	4-41			
SNMP	Lets you to control the SNMP agent running in the SLK.	4-43			
Information					
Main Menu Tree (SLK1 and SLK8 only)	Displays a representation of the OSD menu.	—			
Full Menu Tree (SLK16 only)	Displays an expanded menu of SLK functions and current settings.	4-45			

#### Table 4-1. Web Control Interface Menus

Menu	Description	See Page
Browse Menu Tree (SLK16 only)	Displays a representation of the OSD menu.	4-46
Connection	Displays miscellaneous installation and SSL information.	4-47
Version	Displays serial numbers and versions for your installation.	4-48
Capture Settings	Shows a snapshot of the system log and settings in text format.	4-49
Copyright	Shows the Open SSL encryption copyright requirements.	4-50

#### Table 4-1. Web Control Interface Menus

# **Performing Operation Activities**

SLK operation activities can be performed using the links under **Operation** in the menu pane of the web control interface. Table 4-2 lists the SLK operation activities.

Menu	Description	See Page
Control Hosts	Initiates a JavaView session without an active channel being selected.	4-9
View Hosts (SLK16 and SLK8 only)	Displays server desktops in one of the four preset views for monitoring.	4-12
Power Control	Displays channel power outlet names and lets you power-off, power-on, and reset individual outlets, if an optional third-party power control unit is installed and configured on a serial port.	4-12
User Activity	Displays the user activity history (for example, user name, session type, login and idle times, and IP information).	4-13
Event Log	Displays the event log history.	4-14
Flash File System	Displays a list of internal SLK files.	4-16
Debug (SLK16 only)	Helps you to reset, maintain, and to calibrate video and keyboards, and load configuration files.	4-17

Table 4-2. SLK Operation Activities

# **Controlling Hosts**

The **Control Hosts** link lets you view and control a server desktop. **Control Hosts** is functionally equivalent to clicking a server in the **Channel** column on the SLK home page.

Note: If NO INCOMING VIDEO appears, see "Video Troubleshooting" on page 7-8.

You perform tasks on this page using the menus, icons, and buttons at the top of the page. The REMOTE FOCUS indicator normally is red; however, it turns gray if the remote cursor is moved off the server desktop.

For a description of the menus, icons, and buttons, see Table 4-3 on page 4-10.



Figure 4-4. Example of Controlling a Host

Menu Item	Description
REMOTE FOCUS	Status indicator; turns gray when the mouse leaves the active server desktop
Session>	Provides session management options.
Connect	Restores the connection if the connection was disconnected.
<b>Burne</b>	
Disconnect	Disconnects from the server you were viewing.
SSL	Lets you encrypt SLK transmissions (with certificate and access key installed). Encryption levels vary depending on the Security settings selected.
Channel	(Does not apply to SLK1.) Lets you choose a channel (server) from the drop-down list. Names represent servers and KVM switches.
4 - Win 2003 💌	
Send>Send Keys	Send Keys are a set of pre-defined keystroke combinations to perform specific functions.
Send>Custom Keys	Allows redefinition of Send Keys if attached devices require key combina- tions not included in the default Send Keys definition. See Chapter 9, "Defining Custom Send Keys".
Power> Cycle power Power off Power on	Shows choices on an optional power control unit. Power control requires installation of an optional SLP Remote Power Manager.
Misc	
Resynchronize Mouse	Lets you reset the local mouse cursor to more closely follow crosshairs of remote mouse.
Refresh Entire Screen	Refreshes the screen.
<b>Q</b>	
Blank Screen	Clears the screen so you can better detect whether you are receiving system noise.
Release the CTRL, ALT, and SHIFT keys	Releases you from the states in which <b>Ctrl, Shift</b> , or <b>Alt</b> are always on.

## Table 4-3. Menus, Icons, and Buttons

Advanced	
Color Depth	Allows the user to select either 8-bit or 16-bit color mode.
Position Calibration	Allows remote users to choose between manual and automatic position- ing of the server screen. (This feature may not function properly with a black desktop background.)
	The icon automatically calibrates the screen position.
Redetect Video	Prompts the SLK to redetect the video signal.
Optimize Video	Applies an algorithm to sharpen the image or correct for noisy images.
View Current User	(SLK16 only) Shows which users are logged into which channel.
Lock this channel	Locks the channel, preventing access by other users, including local users. Administrator can override by closing this session and user activity, (SLK16 only.)
Auto-Scaling	Dynamically resizes the viewing area so that remote users can see the entire desktop of the server being accessed.
Performance monitor	Provides real-time bandwidth usage measurement.
Help	Provides software version information.
Scale	Resizes the active server window.
NUM	When bold, indicates that <b>Num Lock</b> is on.
CAPS	When bold, indicates that <b>Caps Lock</b> is on.
SCROLL	When bold, indicates that <b>Scroll Lock</b> is on.

# Table 4-3. Menus, Icons, and Buttons

# **Viewing Hosts**

The **View Hosts** link lets SLK16 users view the maximum number of channels supported by the SLK16. (This feature is not available with the SLK1 and SLK8.)

- SLK1 users can store the desktop view for one channel.
- SLK8 users can view all channels from one screen.
- SLK16 users can store up to four sets of channels, each of which can contain 1 to 16 desktop views.

You can right-click any channel to see video data such as 1024x768@60Hz and double-click any channel to control it.



Figure 4-5. Viewing Hosts

**Note:** The SLK1 and SLK8 View Host function pauses when a remote session is in progress. Several such sessions can be created from different locations. The SLK16 View Host function is independent of a remote session in process because of the dedicated hardware for this functionality. Also, multiple View Host sessions at different locations and six remote sessions can be supported simultaneously.

The SLK16 View Host function remains interactive regardless of remote sessions in process. Multiple View Host sessions do not interfere with the SLK's ability to support six concurrent remote sessions.

# **Using Power Control**

The **Power Control** link provides on/off/reboot control of attached systems when an SLP Remote Power Manger is attached to the SLK. You must attach a serial cable (Appendix A:, Specifications) between a serial port on the SLK and the serial (serial, RS-232) port of the SLP, and configure the SLK serial port for "Power Module," before you can control power to the attached systems.



LANTRO	SLK16				Í
Control Hosts View Hosts View Hosts Power Control User Activity Event Log Flach File System Debug	Power Control This page allows you to control th devices plugged into the power co You may rename any of the outlet channel names.	e power module ; introf module. Is by clicking on f	attached to the name it:	) SLK16. You can power off, on, or reset any of the attache self. You may also <u>synchronize all putiet names</u> to the	ed
Ceofiguration Network	Click corresponding link below to p	ower reset, powe	Power Off	wer off appropriate machine.	
User Accounts	1: Support PDC	Power Ruser	Off	DD	
Change Password	21 Linux - Red Hat	Decet	off	00	
Security	31 Nordanie	Reput	off	On	
Serial Ports	4: Win 2003	Depet	Off	On	
Local User/VNC	5 Noname	Repet	off	<u>00</u>	
Date 6, Time	5. Noriame	Repet	off	201	
SNMP	7) Win NT 4 Server	Repet	Off	00	
Information	8: Support BOC	Deast	Off	On	
Full Menu Tree Browse Menu Tree Connection	1000100.003	Comments of Land	me i bac	t I Logout	

This page gives you control over the power status of all IT equipment connected to the SLK. In particular:

- Power Reset (power cycling) lets you remotely force a reboot on a server.
- Synchronize all outlet names lets you name the outlet names identical to the channel names.

*Note:* If you assign the same name to two devices, Power Control turns them on and off at the same time.

# **Performing User Activity Functions**

The **User Activity** link lets you view which users are currently logged into the SLK. When the User Activity page appears (see Figure 4-7), you can click a slot number link to terminate the corresponding session. (System administrator only.)

The maximum number of users that can be logged in varies by model.

The maximum number of sockets is limited to 32 slots for remote activity (web, telnet, VNC, Java). When filled, the one with the longest timeout is terminated and recycled. Sessions are also terminated when logout is done properly or timeout is reached.

- SLK1 and SLK8: Up to 10 remote users can start a session to use the web control interface pages without viewing video. These users are "active" or logged on, but not considered when counting the single user viewing or controlling servers.
- SLK16: Up to 32 remote users can start a session to use the web control interface pages without viewing video. These users are "active" or logged on, but not considered when counting the number of users (up to 6) viewing or controlling servers.

**Note:** Users can log in multiple times (up to 32 logins). When a user logs out of a session, only that session closes, not all sessions associated with that user. Therefore, check for a duplicate **Name** or **Remote IP** on this page. Logging in multiple times reduces the number of available sessions. Setting the idle time-out to a low value such as 10 minutes reduces exposure to this situation. (This can be done on the Security page.)

Lington		and the second						
an I Horts Hosts Control Log	ser Act are are 1 act date the dsp	<b>Livity</b> ive users to lay by rela	ygged-in ( ading (ref	or trying to logir teshing) this pay	n) at the pr ge.	resent momenit.		
de System	Slot	Name	Туре	Login Time	Idle Time	Remote IP	Remote	Channel
ration rk	1	root	Web (HTTP)	Thu, 11 Nov 2004 20:26:39 -400	0:00	172.19.100.199	1267	none
coounts	2	(unused)						none
e Password	3	(unused)						none
rina -	4	(unused)						none
Ports	5	(unused)						nome
Jaan/AMC	15	(unused)						none
Time	7	(unused)						none
	6	(unused)						none
1000	9	(unused)						nome
nu Tree	10	(unused)						none
Mercia Tress	11	(unused)						none
tion	12	(unused)						none
- Andrews	13	(unused)						none
ht	14	(unused)						none
	15	(unused)						none
	16	(unused)						none
	17	(unused)						none
	10	(unused)						none
	19	(unused)						none
	20	(unused)						none
	21	(unused)						none
	22	(unused)						none
	23	(unused)						none
	24	(unused)						none
	25	(unused)						none
	26	(unused)						none
	27	(unused)						none
	20	(unused)						none
	29	(unused)						none
	30	(unused)						none
	31	(unused)						none
	32	(unuted)						none

Figure 4-7. User Activity Page

*Note:* For the SLK1 and SLK8, the title of this page is "Who's logged in," and it does not have a Channel column.

# Viewing the Event Log

The **Event Log** link lets you view system messages. Figure 4-8 shows an example of the event log. To clear the events in the log, click the **Clear log contents** button.

Event logs are stored in volatile memory and are cleared when the SLK is reset. Use syslog to capture and store event logs. (See "Configuring Syslog Parameters" on page 4-41.)

Note: For the SLK1 and SLK8, the title of this page is "System Log History."

E	vent Log		
ul Hasts T	we are 29 messages in the l	og hutory.	This display is in reverse-chronological order, meaning t
Control Activity	cent events are at the top of	c the list.	
The Dystere	ou can update the display of	over log must	on by record (rememory) the page.
aration .	ou may clear the buffer by cit	cking the b	utton below,
eccounts pe Password	Claim log contents		
unig	Three	Lovel	Mossage
HORTS MARK	Thu, 11 May 2004 20:27:01 -400	PIFO.	httpd-Lugm: root has logged in from 172.19.100.199-1205.
h Terra	Thu, 11 Nov 2004	DIFO	Junew: User 'roof' from 172.19.100.199 1231 is being
1.000	Thu, 11 Nov 2004	DEO	Auto logout: Session # 1, 'root' via http from
etice ency Thee	19:43:12 -400 Thu, 11 Nov 2004		172.20.197.56:3000 has timed out. Juans: User 'root' connected from
e Marua Tree	19:32:33 -400	200	172.19.100.199:1231 using control port # 0.
n re Settings	19/28:33 -400	340	172.19.100.199.1224
ant of the second	Thu, 11 Nov 2004 19:12:42 -400	700	httpd-Logn: root has logged in from 172.20.197.56:2992
	Thu, 11 Nov 2004	780	Julew: User Yoo? from 172.19.100.199:1160 = being
	Thu, 11 Nov 2004	-	Auto logout: Session # 1, '(urknown)' via http: from
	18:52:51 -400 Thu: 11 Nov 2004		128.170.44.228:7 has timed out. Julew: User 'rost' connected from
	18:23:28 -400	INP Q	172.19.100.199-1160 using control part # 0.
	18:20 48 -400	INFO .	172.19.100.199 1148.
	Thu, 11 Nov 2004 18:09:14 -400	INFO	Auto logout: Session # 1, 'root' via http from 172.20.197.56:2782 has timed out.
	THM, 11 NOV 2004	INFO	Iview: User Yoo? from 172-20 197.56 2782 is being
	Thu, 11 Nov 2004	alara -	Sview: User 'root' connected from 172.20.197.56:2782
	17:37:41-400 Thu: 11 May 2004		using control port # 0. Introductions must have been at in from
	17:37:31 -400	INFO	172.20.197.56:2770
	16:08:44 -400	INFO	Auto logout: Session # 1, Yoot' via http://rom 172.20.197.55/2502 has timed out.
	TRu, 11 Nov 2004 15:38:33 -400	INFO	httpd-Lager: root has logged in from 172 20, 197 56-2469
	Thu, 11 Nov 2004	EPPOR	Unable to load server certificate: Cannot find, crt file!
	Thu, 11 Nov 2004	-	Reserved and an Addition ( Arms ) and ( a sure fragment
	15:37:09 -400 Thu 11 New 2004		subultification for Carrot ford any authoritation
	18:37:05 -400	DEBUG	config file.
	18:37:04 -400	WARNENG	#M ferrievane on channel 11 (version 1.31) does not match the one in the file (1.36).
	Thu, 11 Nov 2004 15:37-04 -400	WARNENG	KM Remware on channel 9 (version 1.31) does not match the one in the Re (1.36).
	Thu, 11 Nov 2004	WARNING	KM fereware on channel 8 (version 1.31) does not
	15:37/04 -400 Thu, 11 Nov 2004	1800-040-0	match the one in the file (1.36), KM fermware on channel 7 (version 1.31) does not
	15:37:04 -400 Thu: 11 Mars 2004	-convertes	match the one in the file (1.36).
	15:37/04 -400	WARNING	match the one in the file (1.36).
	Thu, 11 Nov 2004 15/37/04 -400	WARNING	KM firmware on chaosel 3 (version 1.31) does not match the one in the file (1.36).
	7%s, 11 Nov 2004	WARNENG	KM firmware on channel 2 (version 1.31) does not match the one in the file (1.54)
	Thu, 11 Nov 2004	WARRANT	KM firmware on channel 1 (version 1.31) does not
	15:37:04 -400 Thu, 11 Nov 2004	-	match the one in the file (1.36). Found 7 sets of video hardware including the
	15:37:02 -400	RF0	monitoring hardware
	15:36:57 -400	WARHING	Changing lognask from Ddff to Ddff.

Figure 4-8. Event Log

### Flash File System

The **Flash File System** link displays the Flash File System page (see Figure 4-9). From this page, you can open or delete files critical to the operation of the SLK. These files are stored in the SLK on-board Flash memory.

Because most of these files are critical for correct operation, do not perform modifications on this page unless instructed to do so by Lantronix Technical Support.

The Flash File System page also lets you upload new firmware and certificates. For more information, see Chapter 8, "Uploading Flash Files and Certificates'.

Note: For the SLK1 and SLK8, the title of this page is "Internal Flash File System."

		1000				
ration .	Flash Fi	le System	1			
er Pitate	Current File	5				
et achivity ent Log	These files are Please do not p	stored in the on-to enform modification	and Flaim mer	nory of the unit. Euriess mitracte	Most files are d to dn so by	onhow for correct operatio Lantronic technical support
est File System Ibles	Personation	Neme	Size (bytes)	CRC32 (hes) A	an C + la serve	ar) Culatu?
Algoration Freidig		-	3099	#0100041	38	Delate
er koosinty langa Passwind kointy		panel are obj	1040	07364:10	45	Defete
enal Durts and Clary/Mac		comthe atop	9927	muestast	88	Datate
eter Ar Terrer : Luting gran		scenation	143440	40410244		Detete
armation at Marus Time Unite Marus Time		kei.otisa	80995	(5:71:0)	17	Carete
eriectum elan acture Settings		active toppe	149430	8027546	10	Colore
THE REAL PROPERTY AND INCOME.		thakhn	2012	-month	10	(Dates)
		lactions.html	\$24380	+05(65)	00	(Databas)
		Sectorical de la	1205630	what2wfil	#1	( Contraction of the second se
	<ul> <li>The factor</li> </ul>	of new the possible	H 4.6728.0v	tes in size becau	to the setting t	Securitary can only alterate
	<ul> <li>Of total - <ul> <li>The large flass state solution of the solution of the solution of the currently Uploadd File The file 1 supplies typicading</li> </ul> </li> </ul>	at new the possible configurus regions and space wither a costly and cannot b ). to Flash o be traded must h i mealed in corrupt 1	In 4,6728 by brok summary c cleared the eve a builtable fies may rend	tes in star becau ( is either in train to overlap with p ( extension, Firms er plur scht nope	on our proje t pton Chaing w ther Nes (94	Recention can only allocate others to right new) an was is in this "dicty" state have the "dicty" scatescon, it income, remember that the
	<ul> <li>Of the large flass into;</li> <li>Wancour use previous previous previous currently;</li> <li>Upload File</li> <li>The file 1 example;</li> <li>Uploading boot tool</li> </ul>	et new the people combiguous regions that epice in the a ously and cannot b b to Flosh o be trailed much h provide an corrupt 1 t can be used to re- tican be used to re-	in 4,672k by brow summary a cleared due even a butable files may rend cover via 171 to upload	tes in star becau (a either in trans to overlap with o exclusion, Firms ar pour unit inspe if	or our ungle t stors chaing a ther films (9k one reads to rable, of the r	Securities can only allocate entran to right new) or was is in this "dety" state have the "dety" state have the "dety state that the
	<ul> <li>Or out- The large Rise and veracoun- ve</li></ul>	of new file possible combourse regions and space in the a costly and cannot b b to Flash o be trailed must h prevail or corrupt t can be used to re- File.	in 4,672k by boux summary e cleared due even a turtable files may rend cover we tri to upload	tes yn star becau ia either yn trans te overlap with o eichensun, Firms er plur unit mege fl. SherLiptonst	or our employ the out of the outo	Seyritem can only allocate entran to room new or was in in this . don's state have the ".fm" extension, fi nours, remember that the
	Of the large files and the large files and the large file of the large back for the large	at new Kie possible combours response that space in the a courty and cannot b b to Flash o be tradient much th provide or compil can be used to re- Plia	in 4,672k by bowk summary e closenid due ave a buitable files may rend cover we 171 to upload	tes in size becau in either in trans to overlap with p exclusion. Firms ar pour sold inope if. [Derruption]	in our engle t attor their (He ore reads to ratio, of the (Bowes)	Reportenci can only allocate entran to optimize an was in in the optimized an was have the ", the extension, it inclust, remember that the Debust o

Figure 4-9. Flash File System

The **Keyboard and Mouse Emulators** link (SLK16 only) enables you to control keyboard and mouse timing. This function is useful for fine tuning compatibility, resetting the emulation, and upgrading the emulation software.

Keyboard and mouse emulation firmware can be upgraded on a "per-port" basis.

*Warning:* When upgrading a port's keyboard and mouse emulation, all keyboard and mouse signaling is lost, and the attached server sees this as a disconnect. It is preferable for the attached server to be shut down during this process. Otherwise, a server reset may be required.

The Save/Load Configuration File link allows you to save and load configurations into a file in Flash. The file can be downloaded, uploaded, and edited for configuring multiple units with same or similar settings.

# Debug (SLC16 only)

The **Debug** link (on the SLC16 only) lets you perform maintenance and calibration activities.

# Do not perform modifications on this page unless instructed to do so by Lantronix Technical Support.



Figure 4-10. Debug Menu Page

# **Performing Configuration Activities**

SLK configuration activities can be performed using the links under **Configuration** in the menu pane of the web control interface. Table 4-4 lists the SLK operation activities.

Menu	Description	See Page
Network	Helps you to understand and configure the network connection.	4-19
PPP (SLK16 only)	Lets you set up a dial-up modem as a backup strategy.	4-21
User Accounts	Displays user names, passwords, and account information and lets the Administrator set user-access privileges for each channel.	4-24
Change Password	Enables users to edit their own passwords.	4-28
Security	Sets profiles and policies for logout time, Turtle, Stealth, and other functions.	4-29
Monitoring	Sets error conditions and responses.	4-35
Serial Ports	Sets operating mode, baud rate, power, and other serial port func- tions.	4-37
Local User/VNC	Sets VNC port, mouse threshold, and exit key for OSD as well as VNC.	4-39
Date & Time	Sets the SLK internal clock and time zones to the remote values.	4-41
Syslog	Lets you set the configuration of basic Syslog parameters.	4-41
SNMP	Lets you control the SNMP agent running in the SLK.	4-43

Table	4-4.	SLK	Configuration	Activities
TUDIC		OLIV.	Configuration	Activities

# Specifying the SLK Network Configuration

The **Network** link lets you specify SLK network configuration information (see Figure 4-11). Network configuration information consists of the SLK's IP address, subnet mask, default gateway, and machine name.

Before you can access the SLK through the web control interface, you must specify the SLK's IP address, subnet mask, and default gateway using the local console. This task should have been completed during the initial configuration of the SLK. Thereafter, you should only need to modify this information if these settings conflict with another device on the network or if you move the SLK to a different network.

co Lapos	Network Confi	aurat	ion							
Operation Control Hosts View Hosts Power Control User Activity Event Log Flash File System Dates	Addresses and Routing On this screen, you can confinetwork (you are), then these	gurat gure the r e values a	vetwork details for re probably prett	r the SUK16. y close to wh	If you are readir nat you want.	ng this over the				
Contraction of the	1P Addres	5	Subnet r	nask	Default G	ateway				
Change Password Security Monitoring	When you make changes to any of the above, your changes will take effect after the next reset or power- cycle. If you want the new values to be in effect immediately, click on the button below. Since the web page you are currently reading was at the old network address, you may get an error after pressing this button and your browser will probably take a long time to timenut. This is to be expected if you are changing the IP address or other details to new values. Commit P config changes									
Senal Ports Local User/VNC Date & Time Syslog SNMP	page you are currently readin button and your browser will changing the IP address or of Commit IP config changes	ig was at t probably t ther detail	e in effect immed the old network a ake a long time t s to new values.	lately, click o ddress, you o timeout. Th	in the button be may get an error is is to be expec	low. Since the web r after pressing this cted if you are				

#### Figure 4-11. Network Configuration Page

To change the network information, use the following procedure:

- 1 Close all remote user sessions. Otherwise, the sessions lock up and become unavailable to remote users. If this happens, perform a warm reset of the SLK from the Debug menu of the OSD. (Debug is available from the OSD on all models. Only the SLK16 has it as a web choice as well.)
- 2 In the menu pane, click **Network** under **Configuration**. The Network Configuration page appears.
- 3 To change the IP address, enter the appropriate new address in the **IP Address** field and click the **Apply** button next to this field. This is the address you enter in your web browser to access the web control interface. To enable DHCP, type **DHCP** or **0.0.0.0** in the IP address section.

*Note:* The IP address must uniquely identify the SLK. Be sure no other device on the subnet has this IP address.

- 4 To change the subnet mask, enter the appropriate new one in the **Subnet mask** field and click the **Apply** button next to this field. This value must match the subnet mask used on the LAN.
- 5 To change the default gateway, enter the appropriate new address in the **Default Gateway** field and click the **Apply** button next to this field.

- 6 To change the machine name, enter a name that will uniquely identify this device on the network and click the **Apply** button next to this field. The machine name can be an alphanumeric string up to 15 characters long.
- 7 Once changes to all individual fields have been made, click **Commit IP Config Changes** to have the changes take effect. If you omit this step, the new settings take effect the next time the unit reboots.

**Note:** If the configured gateway is not on the same LAN segment as the IP address and subnet mask specified, the SLK calculates an appropriate gateway using standard network numbering conventions.

# **Configuring PPP Settings**

The Point-to-Point Protocol (PPP) is an out-of-band communication channel that allows dial-in access to the SLK16. If you have an SLK16 with a modem connected to serial port 3, you can use the **PPP** link to configure the following PPP options. After you select your options, click the **Apply** button to initialize them. Once PPP is established, to access the SLK, use a browser, Java, VNC, or Telnet as usual.

Note: The PPP link does not apply to the SLK1 and SLK8.

#### **IP Addressing**

- PPP Local IP address the IP address that is assigned to the PPP interface of the SLK16.
- PPP Remote IP Address the IP address assigned to the dial-up client once attached and authenticated.

#### **Authentication**

- User Name the user name (or peer name) used for authentication when a client dials in.
- Password the password (or secret) used for authentication.
- PPP Authentication Protocol the authentication protocol used for PPP. You can select CHAP (Challenge Handshake Authentication Protocol), PAP (Password Authentication Protocol), or None.

#### **Compression**

- PPP Van Jacobson lets you enable or disable Van Jacobson TCP/IP header compression.
- PPP Protocol Compression lets you enable or disable Protocol Field Compression (uses single octet Protocol fields).
- PPP Address Compression lets you enable or disable Address and Control Field Compression.

#### Modem

- Modem Init String an initialization string specific to the modem attached to the SLK16. We recommend you set this string to factory defaults and set the modem speaker volume to level 2.
- ACCM Asynchronous-Control-Character-Map. Provides a way to negotiate the use of control character transparency on asynchronous links.

Figure 4-12. PPP Configuration Page

LANTRO	SLK16
Co. Ligent Control Hosts Control Hosts Power Control User Activity Event Log Flash File System Debug Configuration Network PDP User Accounts Change Password	PPP Configuration         On this screen you can configure the PPP options for the SUK16. These settings will only be used if PPP is enabled on Serial Port 3 in the Serial Ports page.         IP Addressing         • PPP Local IP Address: This is the IP address that is assigned to the PPP interface of the SUK16.         172:18:18:18         • PPP Remote IP Address: This is the IP address assigned to the dial-up client once attached and proteinstance
Security Monitoring Serial Ports Local User/VNC Date & Time Syslog SNMP	172.18.18.19 Authentication
Information Full Monu Tree Browse Menu Tree Connection Version Capture Settings Copyright	User Name: This is the user name (or peer name) used for authentication when a client dials in.     Password: This is the password (or secret) used for authentication.
	PPP Authentication Protocol: Specify the authentication protocol used for PPP.     CHAP      Compression
	PPP Van Jacobson: Enable Van Jacobson TCP/IP header compression.     T: Enabled      PPP Protocol Compression: Enable Protocol Field Compression (uses single octet Protocol fields).
	Enabled      PPP Address Compression: Enable Address and Control Field Compression.      Enabled      I:Enabled      I:Enabled II:Enabled      I:Enabled II:Enabled      I:Enabled II:Enabled II:
	Modern     Modern Init String: This is specific to the modern attached to the SLK16     (suggestion: set to factory defaults and speaker volume level 2).
	AT &FL2  ACCM: Asynchronous-Control-Character-Map This Configuration Option provides a method to negotiate the use of control character transparency on asynchronous links.
	Bestart PPP Server
	Copyright © Lantroniz, Inc. 2004. All Rights Reserved.

# **Setting Up User Accounts**

The User Account link allows the administrator to specify users, assign permissions, and allocate access (see Figure 4-13). User accounts must be defined before remote (web) sessions are available.

Figure	4-13.	User	Accounts	Page
--------	-------	------	----------	------

LANTRO		КВ																		
Control Hosts Control Hosts View Hosts Power Control User Activity Event Log Flash File System	Us Ma: The will a	ster Aco master (or accept eith	ount Pass r root) passw her `root' or	S word ord can be `administrat	changed he or' as the r	ire. 1am	The e of	usi thi	er n s ac	ame	e foi unt.	r th	e m	aster aci	cour	nt can	not	be c	hanged: The system	
Configuration Network User Accounts Security Monitoring Benial Ports Local User/VNC Channel Names Date & Time Syslog SNMP	Acc Here login Follo	ount Pro you may ( is, w the links	ofiles define user n s in the table	ames and p to change	Apply asswords fo the values.	e uj	p to	10	reg	ular	use Se	ervi	You	i must ei	nabl	e the i	ecci	ount	in order to permit	
Information	#	Name	Password	Account	Privilege	1	2	3	4	s	6	7	8	(	Com	mands				
Connection	1	dmonson	*****	Normal	Control+	7	R	P	P	4	9	7	P	Submit	C	None	C	All		
Version Capture Settings	2	btutor		Normal	Control+	R	R	R	R	R	R	R	R	Submit	С	None	c	All		
Copyright	з	jblyther	<u></u>	Normal	Control+	P	R	P	<b>V</b>	P	R	R	P	Submit	C	None	c	All		
	4	gfisher	**	Normal	Control+	R	R	5	9	9	P	5	5	Submit	C	None	c	All		

The User Accounts page lets you:

- Change the master account password.
- Define user accounts (normal or administrator).
- Set user names, passwords, and flags.
- Select the servers that users can access and not access (available on SLK 8 and SLK16).

#### **Changing the Master Account Password**

The master account password is the password you enter to perform Administrator activities using the web control interface. The default password is **PASS**. For security purposes, we recommend you change it. This step should have been completed during the initial configuration of the SLK. If not, or if you want to change it again, perform the following procedure.

- 1 In the menu pane, click **User Accounts** under **Configuration**. The User Accounts page appears.
- 2 Under **Master Account Password**, type the new master account password in the left field; then retype it in the right field (see Figure 4-14).

**Note:** The master account password is case-sensitive. For security purposes, each typed character appears as a dot (•).

Mast	Master Account Password						
The m or `ad	aster (or root)   ministrator' as t	bassword can be c he name of this ac	hanged here. The user name for the master account cannot be changed: The system will accept either count.	`root'			
		•••••	Apply				
Ente mas	r the new ter accour	tt	nen retype it again here.				

## password here...

- 3 Click the **Apply** button next to the right field.
- 4 Record the new master account password for future use.

*Warning:* The master account password can be changed on the local console if access is left shared. If the local console is locked and the password is lost, the only method to reset the password is by sending the unit back for factory reset. An invoice will be required and a surcharge will apply. Please do not lose the password, or leave the local console unlocked (unless keeping it locked is critical.)

#### Setting Up User Accounts

Before users can access the target servers, you must set up an account for them. When you set up a user account, you:

- Specify the user name and password the user must enter before accessing a server.
- Enable the user account.
- Specify the channel privileges, if any, for a user.
- Select which target servers, if any, the user can access.

To define user accounts, use the following procedure:

- 1 If the User Accounts page is not displayed, click **User Accounts** under **Configuration** in the menu pane.
- 2 Each row under **Account Profile** belongs to a different user. Find the row that corresponds to the user you want to configure. If you are setting up users for the first time, start with the user on the top row.
- 3 To change the user ID, click the link under **User Name**. A page similar to the one in Figure 4-15 appears. Enter a user ID for the user and click the **Apply** button. When the User Accounts page returns, the updated value displays.

LANTRO	SLK16
Loost     Loost     Control Hosts     View Hosts     Power Control     User Activity     Event Log     Flash File System     Debug     Configuration     Network     PPP     User Accounts     change Password     Security     Monitoring     Serial Ports     Local User/VNC     Date & Time     Syslog     SNMP	Changing: User6 Name User6 Apply • User6 Name is currently set to "User6". • This value is a text string up to 19 characters long. • The default value is "User6". Set to default Return to previous page. Home   Back   Logout Copyright © Lantronix, Inc. 2004. All Rights Reserved.

Figure 4-15. Page for Changing a User ID

4 To assign a password to the user, click the link under **Password**. A page similar to the one in Figure 4-16 appears. Enter a password for the user in the left field, type it again in the right field, and click the **Apply** button. When the User Accounts page returns, the updated value displays.

**Note:** For security purposes, each typed password character appears as a dot (•) in the page where you enter the password and as an asterisk in the User Accounts page. **User passwords are case-sensitive; user names are not.** 

LANTRO	SLK16
Control Hosts     View Hosts     Downer Control	Changing: User6 Password
User Activity Event Log Flash File System Debug	User6 Password is currently set to **.     This value is a secret password up to 19 characters long. Enter twice to confirm value.     The default value is "forces/montyl".
Configuration Natwork PSP User Accounts Change Password Security Monitoring Senal Ports Local User/VNC Date III Time Sysleg	Eetum to previous page. Home 1 Back 1 Logout Copyright © Lantronic, Inc. 2004, All Rights Reserved.
Information Full Menu Tree Brawse Menu Tree Connection Version Capture Settings Copyright	

Figure 4-16. Page for Changing a User Password

5 To change the user account status, click the link under **User Account**. A page similar to the one in Figure 4-17 appears. Click the appropriate user account type and click **Apply**. When the User Accounts page returns, the updated value displays.

The types of user accounts are:

- ♦ 0: Disabled user account is disabled.
- 1: Normal view and control access to target server(s).
- Administrator view and control access to target server(s) and all configuration parameters.


6 To change the user's channel privileges, click the link under **Channel Privilege**. A page similar to the one in Figure 4-17 opens. Select the appropriate privilege and click **Apply**. When the User Accounts page returns, the updated value displays.

The types of user channel privileges are:

- **0: Disabled** user's channel privileges are disabled.
- View user can only view channel information.
- Control user can view and change channel information.
- Control+ use can view and change channel information and has additional privileges, such as viewing and changing power switching. Changing power switching is performed using an optional Lantronix SLP Remote Power Manager.

*Note:* This numbering is correct for the SLK16, but is different on the SLK1 and SLK8.

7 SLK8 and SLK16 users: To select the servers that the user can access, check the servers under **Server Access**. If you change your mind about granting the user access to a server, uncheck the server.

*Note: None* and *All* under *Commands* can be used as shortcuts for selecting the servers that a user can access.

- 8 After making your selections, click the **Submit** link under **Commands** to submit your selections for this user.
- 9 Repeat steps 3 through 8 for each additional user account.

Version Capture Settings Copyright

# **Changing Your Own Password**

The Change Password link lets users change their own passwords. This password is specific to the user and affects only their access to the SLK.

1 Click **Change Password** in the menu pane. The Change My Password page displays.

LANTRO	SLK16
Control Hosts Opention Control Hosts Yow Hosts Power Control User Activity Event Log Flash File System Debug	Change My Password Changing Password (UID: 0) New Password:
Configuration Network PPP User Accounts Change Password Security Monitoring Serial Ports Local User/VNC Date & Time Syslog SNMP	Change Home   Back   Logout Copyright © Lantronia, Inc. 2004. All Rights Reserved.
Information Full Menu Tree Browse Menu Tree	

Figure 4-18. Page for Changing Your Own Password

- 2 In the **New Password** field, type a new password.
- 3 In the **Confirm Password** field, type the same new password.
- 4 Click the **Change** button.

# **Configuring a Security Policy**

The **Security** link lets you define a security policy for the SLK. Clicking this link displays a page with a summary of preset security profiles, buttons for selecting a security policy, and controls for customizing security parameters (see Figure 4-19). Using this page, you can set optional security parameters, configure ports, and set local security controls.

Figure 4-19. Security Policy Configuration Page (Security Profiles and Policy)

A 1000	with Policy Configu	un film in		
ration strol Hosts W Hosts Secur	ity Profiles	ration		
Activity The fol 14 Log parame 16 Eystem	lowing table provides the default setting ter to your own needs in the Security P	gs for three predefine arameters section.	ed security profiles. Yo	u are able to customiz
Investion	Security settings	security	snoopers	Por use on the public Internet
rt	Turtle mode:	Disabled	Disabled	Sensitive (S attacks)
A CONTRACT OF	Turtle reset timeout:	24 hours	24 hours	24 hours
counts	Stealth mode:	Disabled	Disabled	Enabled
Password	Permise exception (HTTPG):	Onticnal	Required	Required
00	HTTD port number	0A	äň	0000
orts	HTTP: part number:	440	440	4444
er/VNC	Idla Isaacit tima (minitar)	20	10	4444
Time	Talpat canar part number	00	10	0
	Terrier server port number:	10000	10000	10000
1000	Java viewer port number (clear);	19900	19900	19900
• ( ד י • ( • (	Default releved security his is the factory default and provides to have passwords to be transmitted "in th asswords needed to access the SLK16- ou might need to use this mode if your Internet LAN with snoopers his preset provides security but uses st fice networks. It requires all connections preset provides not try to conceal its prese	the best performance is clear" over the net This is the only mod browser does not su landard ports for trans to use encryption ence on the network	e level. It requires pass work. This means net e that leaves the telm pport encryption. Isomissions and is the n (*). Passwords are no	swords (where defined work sniffers can see t et server enabled. ecommended setting fi it visible to network sr
• (	Foruse on the public Internet his is the recommended setting if the u nforcing encryption (*), non-standard TTPS), but you should change them fro he SUX10: Turtle mode and Sleath mode	nit is outside of a firr values are used for w m these default valu r. See below.	ewall and is visible to t eb server TCP/IP port es. This mode also en.	he public Internet. Bes s (8888 for HTTP, 444 ables two proprietary f

Turtle mode     Ot Disabled     Turtle reset timeout     24 hours	
D: Disabled     Turtle reset timeout     24 hours	
Turtle reset timeout     24 hours	
24 hours	
Stealth mode	
0: Disabled 🛩	
Require encryption (HTTPS) (This takes effect immediately.)	
0: Optional 💌	
Idle logout time (minutes)	
30	
HTTP port number	
80	
HTTPS port number	
443	
Teinet server port number	
23	
Viewer port number (clear)	
19900	
Viewer nort number (SSI )	
1001	
• viewer Encryption Policy	
Charles and a set of the set	
Channel locking policy (Jview)	
Apply	
To make your changes to any of the above effective immediately (rather than the next reset), click on this butto to reset the web server.	
Reset web server	
User Accounts	
See this page to change user names and passwords.	
Local Console Security	
There are a number of controls provided for the local console as well. The master password may always be used t change any settings of the system from the local console. You may restrict regular users as follows:	
Local console	
0: No passwords 🛛 👻	
Local user exclude	
0: Shere access 💌	
Apply	
Home I Back I Lopout Copyright © Lantroniz, Inc. 2004. All Rights Reserved.	

Figure 4-20. Security Policy Configuration Page (bottom)

### **Security Profiles**

This area shows security settings for three pre-defined profiles. You use the buttons in the **Security Policy** area to select the profile you want to use.

### Security Policy

The **Security Policy** area allows an Administrator to select from the three predefined levels of security shown in the **Security Policy** area. The Administrator can customize these profiles to suit the security needs of the network. Click the **Reset Web Server** button only after all fine-tuning is done.

Default Relaxed Security

This is the factory default. It requires passwords (where defined) but allows those passwords to be transmitted "in the clear" over the network. This means network sniffers can see the passwords needed to access the SLK unit. This is the only mode that leaves the Telnet server enabled. You will need to use this mode if your browser does not support encryption.

#### Internal LAN with Snoopers

This is the recommended setting for most office networks. It requires all connections to use encryption. Passwords are not visible to network sniffers, but the unit will respond to Ping and does not try to conceal its presence on the network.

For use on the Public Internet

This is the recommended setting if the unit is outside of a firewall and is visible to the public Internet. Non-standard values are used for web server TCP/IP ports (8888 for HTTP, 4444 for HTTPS), but you should change them from these default values. This mode also enables two proprietary features of the SLK: Turtle mode and Stealth mode.

#### Security Parameters

The **Security Parameters** area lets you fine-tune the parameters in your profile to suit the requirements of the network.

#### **Turtle Mode**

Turtle mode enables the SLK unit to shut down network access when it senses that it is under attack and security may be compromised. For example, if more than five password failures are detected before a successful login, the SLK unit disconnects itself from the network. In this state, remote access to the SLK unit is completely locked out. However, the operation of the attached server(s) is not affected. To regain network access, the turtle mode timeout period must be fulfilled, or an administrator must log in from the local port and issue a reset command via the OSD.

Turtle mode provides a rapid security barrier, but it can make the SLK susceptible to denial-of-service attacks. Consequently, this mode is not enabled by default. When Turtle mode is enabled, a default timeout value of one hour is set. This value can be configured to suit administrative needs.

#### **Stealth Mode**

In Stealth mode, the SLK unit deliberately disables certain TCP/IP protocol functions to conceal its presence on a network. This mode attempts to make the SLK invisible to a "port scan" attack. When Stealth mode is enabled, the SLK will not respond to ICMP PING requests, and Broadcast TCP/IP connection requests to any/all unused ports will go unanswered and will not elicit the expected "connection refused" response. For optimum security, the administrator should change the web server port number from the default setting.

Stealth mode ensures that operation of the SLK unit by legitimate users who can correctly specify both the IP address and web server port number will be normal. At the same time, it prevents intruders who cannot accurately guess both the IP address and port number from gaining access.

#### Encryption Required

This option takes effect immediately. For this feature to work, install a valid server certificate and key provided by a trusted source into the device. The certificate and key must be of the PEM format and the name of the files should be "server-cert.crt" and "server-cert.key."

To install the certificate and key, you must access the "manage flash file system" through the device's web browser and upload the certificate and key through the browser. A reset through the reset link on the Flash File System page has to be performed to allow the device to load the new certificate and key and delete any old ones in the system. For more information, see Chapter 8, "Uploading Flash Files and Certificates".

If you are using a browser, you must have the Sun Java Plug-in 1.4.0 or higher installed. SSL is not available through VNC.

#### Idle Logout Time

The default Idle Logout Time is 30 minutes. To change, enter a new number of minutes.

#### HTTP Port Number

The default HTTP Port Number is 80. To change, enter a new HTTP port number.

HTTPS Port Number	The default HTTPS Port Number is 443. To change, enter a new HTTPS port number.
Telnet Server Port Number	The default Telnet Server Port Number is 23. To change, enter a new Telnet server port number. To disable, set the Port Number to zero.
Viewer Port Number (Clear)	The default Java Viewer Port Number is 19900. To change, enter a new Java Viewer port number.
Viewer Port Number (SSL)	The default Java Viewer Port Number for secure connections is 19901. To change, enter a new Java Viewer port number.
Applying Changes	If you change any security parameter settings except <b>Require encryption</b> , click the <b>Apply</b> button to apply them. This area also provides a <b>Reset web server</b> button you can click to put your changes into effect immediately, rather than after the next reset.
	User Accounts The User Accounts area provides a link that lets you configure user accounts. For more information, see "Setting Up User Accounts" on page 4-24.
Local Console	

### Local Console Security

The **Local Console** area lets you change the local console security level. Requiring a password restricts all but the root used account from the local console. This does not affect the passwords used for remote access.

#### Local User Exclude

This option lets you select the following parameters:

- O: Share access: Local user can type when the remote user is connected and also controlling the same machine.
- 1: No keyboard: Local keyboard is locked out when remote user connects
- 2: Blank screen+keyboard: Local keyboard is locked out and the screen is blacked out, so a local user cannot see the screen when a remote user is connected.
- **3: Local off**: Local access is disabled.

# **Monitoring Your Configuration**

To reduce server downtime, use the **Monitoring** link to have the SLK alert you by email to user-defined error conditions. To receive email alerts, enter your email address, the numeric IP address of the SMTP server used to send the email, and the message format (long or short).

*Note:* If you will be receiving email messages on a cellular phone or page, select short messages.

After you specify this information, you can use the **Error Conditions to Monitor** (**Host**) area to specify which errors you want to be alerted about and even select the channels that are to be monitored.

#### Figure 4-21. Monitoring Configuration Page (Alert Action)

LANTRO	SLK16
Logout     Control Hosts     View Hosts     Power Control     User Activity     Event Log     Flash File System     Debug	Monitoring Configuration Background The SLK16 may be configured here to detect certain common failure modes. Once enabled, the SLK16 will continuously monitor for a failure and if it occurs will log the event. It can also be configured to send out an email to alert you of the problem. For completely autonomous monitoring, it is also possible to reset the power to the controlled computer.
Configuration Network PPP User Accounts Change Password Security Monitoring Serial Ports Local User/VNC Date & Time Syslog SNMP	Alert Action Configure what you would like the unit to do when an error condition occurs. All error conditions are added to the log when they happen (with a time stamp) regardless of whether email is enabled.   • Send email for alerts: This control must be enabled before any email will be sent. You can use this to turn off email, without losing your other settings above.   1:Yes   • Alert email addresses: This is the email address used in outgoing email.
Information Full Menu Tree Browse Menu Tree Connection Version Capture Settings Copyright	<ul> <li>SMTP relay/destination (IP address): This is the IP address (numeric) for the SMTP server to use to send the mail. This server must be willing to relay to the above email address, or else be the mail server for that domain. You may disable email by setting this to 0.0.0.0, or use the control below.</li> <li>(disabled)</li> <li>Message format: Type of email message to send. The short format is appropriate for cell-phones and pagers that have a limited display.</li> <li>Image: Normal Y</li> </ul>

Error Conditions to Monitor (Host)
Here is a list of all host error conditions we can detect. Each one can either be monitored or ignored.
<u>Configure Which Channels to Monitor</u>
<ul> <li>Alert if host power lost: Power from the controlled computer is present at the keyboard/mouse connectors. If the power supply fails to the controlled computer, this condition is considered active.</li> </ul>
0:No 💌
<ul> <li>Alert if no NumLock toggle: If this is enabled, then the SLK16 will simulate the NumLock key being pressed regularly (every few seconds). If at any time, the NumLock light does not toggle in response to a NumLock key press, then the software on the controlled computer is assumed to have crashed and this error condition will be active. (Please ensure the above option is enabled first).</li> </ul>
0:No 🛩
<ul> <li>Alert if no video: No graphics or text video signal coming from controlled computer. Please note that power saving screen-savers (DPMS) may trigger this falsely.</li> </ul>
0:No 💌
<ul> <li>Alert if text (blue screen): This occurs when the machine is rebooting (BIOS screen) or displays the 'blue screen of death'. Can be useful for detecting self-initiated reboots. (Please ensure the above option is enabled first).</li> </ul>
0:No 🛩
<ul> <li>Power-cycle host if alert happens: Do you want the controlled computer to be automatically reset (via power cycle) when an error condition occurs? This option carries a certain risk to it, since there is a possibility of false positives with all the above tests.</li> </ul>
0:No 💌
Apply
Error Conditions to Monitor (System)
Here is a list of all system error conditions we can detect. Each one can either be monitored or ignored.
<ul> <li>Alert if my power reset: If the SLK16 is reset or powered-off for any reason, then this condition is activated when power is restored. This might be used in combination with other controls above.</li> </ul>
0:No 🛩
<ul> <li>Alert if my Ethernet link down: Ethernet link signal to SLK16 is lost. There can be some difficulty sending email if this condition occurs, since the SLK16 is off the net in this situation. The event is still logged, however.</li> </ul>
0:No 💌
<ul> <li>Alert if turtle mode active: Occurs if turtle mode (see security page) is activated by too many bad login attempts over a certain period.</li> </ul>
0:No 💌
<ul> <li>ICMP Ping this address: This should be an IP address (or use 0.0.0.0 to disable) that will be pinged continuously. If more than half of the packets are lost during a short interval, then the error condition is triggered. This IP address does not need have to be the controlled computer, but might be a border router or other important component of your network.</li> </ul>
(disabled)
<ul> <li>HTTP Poll this address: This should be an IP address (or use 0.0.0.0 to disable) of a web (HTTP) server. The server will be asked to GET the root page (/). If nothing is returned (zero length) or the connection fails, then this error condition is considered active. The URL that is fetched is effectively: <a href="http://disabled1:00/">http://disabled1:00/</a> WTTP IP address</li> </ul>
(disabled)
HTTP Bort Number
00
Apply
Home   Back   Lopout Copyright © Lantroriz, Inc. 2004, All Rights Reserved.

Figure 4-22. Monitoring Configuration Page (Error Conditions to Monitor))

# **Configuring Serial Ports**

The **Serial Ports** link lets you configure the SLK serial ports. Serial ports 1 and 2 provide similar functionality. Serial port 3 on the SLK16 supports modem (PPP) connections (see "Configuring PPP Settings" on page 4-21).

#### Figure 4-23. Serial Port Configuration Page

LANTRO	
Configuration Network Power Control User Activity Event Log Flash File System Debug Configuration Network ppp User Accounts Charige Password Security	Serial Port Configuration Background The SLK16 has three serial ports. Port 1 and 2 can be used for the following modes (except PPP). Port 3 can only be used for PPP mode. 1. SLK16 Log - Output log from SLK16 to serial port. 2. Telmet - Allow remote telnet user to connect to serial device. 3. Workholog - Dotect and log the presence of string (or absence). 4. Power Control - Connect to a serial device to turn off power to the controlled device. 5. PPP - Dial-up connection (part 3 only). Allow a remote dial-up client to access the SLK16 for configuration and control.
Monitoring Serial Ports Local User/VNC Date & Time Syslog SNMP	Port 1 (DB-9 female)  • Seriel port mode: This is the operating mode for this port. See above for description.
Information Full Menu Tree Browse Menu Tree Connection Version Capture Settings Copyright	Log     Watchdog pattern (string): Each line of input (to the SL:16) will be matched against this simple string. Only lines that contain this string will be logged in Watchdog mode. If this field is empty, then all lines will be logged.
	<ul> <li>Watchdog mode: Choose what to do with lines that match the pattern. See the monitoring page to configure what happens with the alert.</li> <li>D Log lines </li> <li>Watchdog timeout: Period of time during which a matching string must be seen, before an error</li> </ul>
	condition is considered to have occurred. Used only with Watchdog mode "Alert if missing".           1 minutes         .           Boud rate, Data bits, Parity and Stop bits         .
	1:8 bits ×
	1: 2 stop bits 💌 • Hardware flow control (0: None 👻
	(APPY)

## Port 1, Port 2, Port 3

These areas let you individually configure the serial ports. (Port 3 only appears for the SLK16.) Selectable parameters are:

Mode — lets you configure the serial port for log, Telnet, watchdog, or an SLP Remote Power Manager (Serial port 3 also supports PPP mode.) Before you choose a mode, specify the port parameters such as Watchdog pattern, mode, timeout, and baud rate.

**Note:** If you configure serial port 3 to accept a modem, the SLK persistently searches for the modem. With this configuration, performance will be reduced until a modem is connected and identified by the SLK.

- Watchdog pattern (string) each line of input to the SLK is matched against this simple string. Only lines that contain this string are logged in Watchdog mode. If this field is empty, all lines are logged.
- Watchdog mode lets you choose what to do with lines that match the pattern. A link is provided for the Monitoring Configuration page, so you can configure the action that occurs with the alert.
- Watchdog timeout the period of time during which a matching string must be seen, before an error condition is considered to have occurred. Used only when Watchdog mode is set to Alert if missing.
- **Baud rate, Data bits, and Stop bits** lets you specify these character formats.
- Flow control lets you select Clear To Send/Request To Send (CTS/RTS) or no flow control.

Once you have completed the serial port settings for a port, click **Apply** for that port.

# **Configuring Local User/VNC Settings**

The **Local User/VNC** link lets you configure Virtual Network Computing (VNC) and adjust mouse and keyboard settings for local users. The mouse adjustments do not affect remote operations.

LVNLSO	SLK18
Control Hosts Control Hosts View Hosts Power Control User Activity Event Log Flash Pile System Debug	Local User / VNC Configuration VNC Server Configuration • VNC server port number [5500 Apply]
Configuration Network ppp User Accounts Change Password Security Monitoring Sorial Ports Local User/VNC Date & Time Sysiog Sysiog Sysiog	Normally this is 5900, which is the default port for the first VNC display on a VNC server. It is easy to specify a different port number from the VNC client: just append it after the host name with a colon (target:123 for example).  VNC Bandwidth goal           1:Medium Y         Apply           This influences the trade-off between speed and compression. On the 'min' setting, the maximum amount of video compression is performed but that consumes some time, in the 'max' mode, the video is not compressed at all: it's just set as quickly as possible. 'Max' mode is useful on a local area networks. Of course 'medium' is a compromise that does some compression.
Information Full Manu Tree Browse Manu Tree Connection Version Capture Settings Copyright	<ul> <li>In this year cooperation.</li> <li>We recommend, 'ma' for local area networks (10 megabits and above), and 'min' for links with less than 256%bits/s</li> <li>Max resolution (expected)</li> <li>I and I area</li> <li>I area</li> <li< td=""></li<></ul>

### **VNC Server Configuration**

The VNC Server Configuration area lets you select the following parameters:

- VNC server port number the default port for the first VNC display on a VNC server (normally 5900). To specify a different port number from the VNC client, append it after the host name with a colon (for example, target:123).
- Max resolution (expected) lets you select the resolution for your subsequent VNC sessions. Most users should select the highest resolution from within VNC.

*Note:* See Chapter 6, "Using a VNC Viewer to Access the SLK' for a description of VNC.

### Local User Setup

The **Local User Setup** area lets you select the mouse threshold and mouse acceleration for local users. These two values determine the speed of the local mouse. When the mouse is moved faster than the threshold value, its movement is accelerated by the acceleration value.

### Keyboard Exit Key

The **Keyboard Exit Key** area lets you select the key used to escape normal operation and enter the SLK OSD menu system. On the local port, pressing this key twice quickly starts the menu system that lets you configure the SLK. Over a VNC connection, the same key pressed twice quickly displays a menu of useful functions while online.

### Setting the Date and Time

The **Date & Time** page lets you synchronize the SLK (local) time setting to match the remote time on your browser. The SLK reports the remote time rather than the local time zone setting for the controlled servers.

#### Figure 4-25. Date and Time Page

LANTRO	SLK16					
Control Hosts     Control Hosts     Yiew Hosts     Power Control     User Activity     Event Log     Plash Pile System     Debug	Date and tim shown in log Daylight save	nd nd s ar ave ngs tim	Time red internally in UTC (Ci r the web, a timezone o e.)	oordinated Universal Tim Iffset is applied to conv	e, sometimes call GMT or Zulu time). When times a ert that time into local time, (No provision is made l	re for
Configuration Network ppp User Accounts Change Password Security Monitoring Senal Ports Local User/VNC Date & Time Systog StMp	Change ti If the compu- zone of the 1 Set dat Current ti Thu, 11 Nov	me/d iter you SLK16 h e. time a me 2004 2	ate are using to view this p o the same time as your nd time zone	age knows the correct browser.	time, just press the button below to set the time a	nd
Information Full Menu: Trop Browse Menu: Trop Connection Version Capture Sattings Copyright	(When this p Timezone This is a nun time in Green	ege wa coffse	s sent.) <b>:t (from UTC)</b> minutes offset from UTC ic) and add this (signed <u>Apply</u> )	. Most timezones are or ) value to it, you should	n one-hour boundaries. If you take the UTC time (t) I get your current local time,	10
		Code	Timezone name	Hours from UTC	Timezone Offset in minutes	
		EST	Eastern standard	-4 hours	-240	
		PST	Pacific standard	-7 hours	-420	

### Background

Provides an overview of the date and time information.

#### Change time/date

This area provides a **Set date, time and time zone** button. Selecting this button sets the SLK time and zone settings to those of your browser.

#### Timezone offset (from UTC)

This area lets you specify the number of minutes offset from Universal (UTC) time. Most time zones are on 1-hour boundaries. If you take the UTC time (the time in Greenwich Mean Time) and add this signed value to it, you should get your current local time.

### **Configuring Syslog Parameters**

The **Syslog** link lets you configure system messages to view in the Event Log. This page provides links for changing the Syslog collector IP address and Syslog facility.

This page also provides checkboxes for selecting severity levels that are to be enabled (the severity level that has been enabled/disabled also affects the log messages on the serial port, as it uses the same mask). You can use the **Default**, **Clear all**, and **Select all** links to select or clear these checkboxes. Once you make your selections, click the **Submit** link to apply them.

A list of Syslog facility codes appears at the bottom of the Syslog Configuration page.

Image: Section of the section of th	-	Syslog Configuratio	n						
The parameter part to compare the registing parameters in tabula. If the parameter parameter is the parameters in tabula. If the parameter parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameter is the parameters in tabula. If the parameter is the parameters is the parameters in tabula. If the parameter is the parameters is the parameters in tabula. If the parameter is the parameters is the parameters in tabula. If the parameter is the parameters is the parameters in tabula. If the parameter is the parameters is the parameters is the parameters in tabula. If the parameter is the parameters is the parameters is the parameters in tabula. If the parameters is the parameters is the parameters is the parameters in tabula. If the parameters is the parameters is the parameters is the parameters in tabula. If the parameters is the p	and of Houstal								
<ul> <li>Antivity of a standard set of the system is a standard bars will also up to your log.</li> <li>Single confliction must be taken immediately in the set of the system is a standard bars will also up to your log.</li> <li>Single confliction must be taken immediately in the set of the system is a standard bars will also up to your log.</li> <li>Antive attain must be taken immediately in the set of the system is a standard bars will also up to your log.</li> <li>Antive attain must be taken immediately in the set of the system is a standard bars will also up to your log.</li> <li>Antive attain must be taken immediately in the set of the</li></ul>	Control	this page allows you to configure basic	Systog parameters in SLX16						
<ul> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages selected hare will show up in your ligit.</li> <li>• Spring the - Orly messages generated in the rule of the spring the spring of the Spring the - Orly messages in the spring the spring of the spring of the Spring the spring of the Spring the spring of the Sprin</li></ul>	antiwity .	<ul> <li>System Collector IP address = (Nas system)</li> <li>System Facaty = 18</li> </ul>	slog)						
Provide         Provide <t< th=""><th>For Suptain</th><th><ul> <li>Sysing Log Mask Only messages and</li> </ul></th><th>elected here will show up in your li</th><th>rg.</th></t<>	For Suptain	<ul> <li>Sysing Log Mask Only messages and</li> </ul>	elected here will show up in your li	rg.					
# Strengty: pythem is unvalue       0         # Artin action mult be taken immediatory       0         # Artin action       0	ration		evenity level	Check box(es) to select					
a Address action must be taken immediately       immediately         a Address action must be taken immediately       immediately         a Address action must be taken immediately       immediately         a Maning       immediately         b Maning       immediately         c Maning <td< td=""><td>and the second s</td><td>E Emergency: system is</td><td>ununable</td><td>2</td></td<>	and the second s	E Emergency: system is	ununable	2					
get Fastered to the product of the significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if there is normal but significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant condition       get fastered to the significant condition         if the significant conditis significant conditis significant condition       get f	and the second s	1 Alert: action must be	taken immediately	8					
i       immediate indication       immediate indication       immediate indication         i       indication much but significant condition       immediate indication       immediate indication         i       indication much but significant condition       immediate indication       immediate indication         i       bibbling the bubbling the indication       immediate indication       immediate indication         i       bibbling the bubbling the indication       immediate indication       immediate indication         i       bibbling the bubbling the bubbbling the bubbbling the bubbbling the bubbling the bubbl	pe Casewood	2 Official		8					
A Warning       Image: Constraint Condition         A Statistical Condition       Image: Condition         A Statistical Condition       Image: Condition Condition         A Statistical Condit Condition	1112	3 Error		2					
A year of a local condition in missages in the local a loc	Ports	4 Warning		E					
Bit International         District         District <thdistrict< th="">         District         District</thdistrict<>	A Term	8. Notice: normal but sig	inficant condition	8					
Total with restance in the second restance is the second restance in the second restance in the second restance is the second restance in the second restance is the second restance in the restance is the second restance is the restance is the restance is the second restance is the restance is th	12 C	<ol> <li>Informational</li> </ol>		E					
A series of the series of the sourd sourd with the series of the sourd back there is a fact of systel a sourd with the series of the sourd back the sourd	100	7 Debug debug level m	estages	21					
Action         Source           Book is a fixed of systeling facility code values.         We recommend the use of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (code 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (codes 16 to 27).         Image: Code of the focult facilities (codes 16 to 27).           Image: Code of the focult facilities (code 16 to 27).         Image: Code of the foculities 16.           Image: Code of the	and Ires	Defeut	Class.al Select.al	Dutient					
Notes           Below is a flat of syslog facility code values.           We recommend the use of the focal facilities (codes 10 to 23).           Numerical Code         Feldy           1         use-free immessages           2         recurrty/Authonization messages           3         system disensors           4         ascurty/Authonization messages           5         response immessages           6         discurtery/Authonization messages           6         discurtery/Authonization messages           7         response immessages           8         (UCP subsystem           9         citize immessages           10         Hercurty/Authonization messages           11         FTP damin           12         KTP using           13         kip subsystem           14         kip subsystem           15         cick damon           16         kip subsystem           17         kip subsystem           18	e Herse Tree	Notor							
Below is a fist of syslog facility code values.      We recommend the use of time of the focal facilities (codes 16 to 21).      Numerical Code     Facility     0     User-field meesiages     1     user-field meesiages     2     meesiages generated informally by sylogd     5     messages     messag	Contract of Contra	wotes:							
Note reconvenient the same of the flocal flocklikes (codes 16 to 25).           Numerical Code         Facility           0         Seminification           1         user-free/interstages           2         new stages           3         system deemons           4         new stages generated informally be systemed           5         messages generated informally be systemed           6         the printer subsystem           7         relation flock           10         Interview the stages           11         off subsystem           12         relation           13         Note stages           14         rig wint           15         risk deemon           16         risk wint           17         risk deemon           18         risk deemon           19         risk deamon           10         risk deamon           12         risk dia risk 3           13         risk dia risk 3           14         risk dia risk 3 </td <td>en Settings</td> <td>Below is a list of syslog facility o</td> <td>ode values.</td> <td></td>	en Settings	Below is a list of syslog facility o	ode values.						
Numerical Cade         Facility           0         Numerical Cade         Facility           1         user-trevel messages         1           2         near system         1           3         system damons         1           4         ascustry/kuthonization messages         1           5         messages generated informally by system           6         time private subsystem           7         retrock news obsystems           8         AUXP subsystem           9         clock damon           10         security/kuthonization messages           11         FTP damon           12         NTP subsystem           13         tog addition           14         tog addition           15         tog addition           16         tog addition 1           17         tog addition 2           18         tog addition 2           19         tog addition 2           10         tog addition 2           11         tog addition 2           12         tog addition 2           13         tog addition 2           14         tog addition 2           15         <	200	the increase of the line of the line of the	and facilities from the to box						
Numerical Code         Facility           0         Kernel messages           1         use-freel messages           2         mail system           3         system disensors           4         security/kuthonization messages           5         messages generated internally by systepd           6         ternally system           7         network messages generated internally by systepd           6         ternally system           7         network mess adaystem           7         network messages           10         security/kuthonization messages           11         #TP daemon           12         MTP uthystem           13         tog adds           14         tog adds           15         tocal use 0           17         tocal use 1           18         tocal use 1           19         tocal use 2           19         tocal use 3           21         tocal use 3           22         tocal use 4           23         tocal use 4           24         tocal use 3           25         tocal use 4           26         tocal use 4		we recommend the time of the of the	ocial uncludes (contact to to tra).						
0         kernel resistages           1         user-free messages           2         mail system           3         system deamons           3         system deamons           3         system deamons           4         security/athonation messages           5         messages generated informally by systepd           6         like sinter subsystem           7         nativoic mess subsystem           8         0.005 subsystem           9         clock deamon           10         security/athonation messages           11         FTP deamon           12         NTP subsystem           13         log alert           14         log alert           15         clock deamon           16         local use 1           17         local use 1           18         local use 1           19         local use 3           20         local use 3           21         local use 4           22         local use 6           23         local use 7           Below is a first of syslog severity codes.         <		Numerical Code	Facility						
I use-revert message     Viter deemons     Viter deemon     V		0	kemel messages						
A security/Authonation messages     A security/Authonation     A security/Authonationation     A security/Authonationation     A security/Authonationation     A security/Authonationation     A security/Authonationationationationatio		1	user-level messages						
			system daemons						
S         messages generated internative by systed         S         messages generated internative by systed         S         matwork news subsystem         T         matwork news subsystem         S         UVCP subsystem         S         Uvcl subsystem         S         Uvcl subsystem         Uvcl subsyst			accurity/authoritation messag	e1.					
Below is a fist of syslog severity codes.      Below is a fist of s		5	messages generated internally	by syslogd					
f         f             f		6	line printer subsystem						
Cook deemon     Gook deem		1	network news oubsystems						
10         recently/witheritation messages           11         rTr dammin           12         hTr dammin           13         log avoit           13         log avoit           14         log avoit           15         clock dammin           16         log avoit           17         local use 1           18         local use 1           19         local use 1           19         local use 3           20         tocal use 4           21         local use 6           22         local use 7           Eelow is a first of syslog severity codes.           Severity codes are assigned to each message depending on the importance of the event that generated the message           10         local use 7           Vou can choose, however, which message depending on the importance of the event that generated the message           1         cattraction must be taken on endutately           2         critical           3         firmit           4         Warming           5         Defourtery message           6         informational           7         Defourtery message			clock daemon						
11     FTP damon       12     NTP tubsystem       13     tog awit       14     tog awit       15     clock deemon       16     tocal ure 0       17     tocal ure 1       18     tocal ure 2       19     tocal ure 3       20     tocal ure 4       21     tocal ure 6       22     tocal ure 6       23     tocal ure 7       Below is a fist of syslog severity coles.       Severity coles are assigned to each message depending on the importance of the event that generated the message       You can choose, however, which messages you want to see based on their severity (see the Log Maxis settings above)       0     Benergincy, system is unuable       1     Alert: action must be taken immediately       2     critical       3     Brow       3     Brow       4     Warming       5     Motice: normal but significant.condition       6     Informational       7     Debug-freqt messager		10	security/authoridation messag	**					
13     h17 ubsystem       13     big with       14     big with       15     clock deamon       16     bical use 0       17     bical use 0       18     bical use 1       19     bical use 3       20     bical use 3       21     bical use 6       22     bical use 6       23     bical use 6       23     bical use 7   Below is a fist of syslog severity codes.   Severity codes are assigned to each message depending on the importance of the avent that generated the message advent to see based on their severity (see the Log Mask settings above 10       Numerical Code     Beverity       0     Benerity system is sinulable       1     alter: action must be taken messaged advent of the avent that generated the message advent of the avent of the avent the Log Mask settings above 10       0     Benerity system is sinulable       1     alter: action must be taken messaged advent of the avent that generated the message advent of the avent of the avent of the log Mask settings above 10       1     alter: action must be taken sensediately       2     Critical       3     firmit       4     Werning       5     Matter internal tut significant.condition       6     Informational       7     Debug freqt message		11	FTP daemon						
13     50 mixth       14     50 mixth       15     Clock deemon       15     Clock deemon       16     tocal ure 0       17     tocal ure 1       18     tocal ure 3       20     tocal ure 3       20     tocal ure 4       21     tocal ure 5       22     tocal ure 6       23     tocal ure 7       Below is a first of syslog severity codes.       Severity codes are assigned to mach message depending on the importance of the event that generated the message       You can choose, tolwaver, which messages you want to see based on their severity (tee the Log Maill settings above       Numerical Code     Severity       0     Brengmony: system is simulable       1     Alert: action must be taken immediately       2     Critical       3     Brow       4     Weening       5     Notice: nermal but significant condition       6     Informational       7     Debug-trapt messager		10	NTP subsystem						
		13	ion alert						
10     total use 0       17     local use 1       18     total use 2       19     local use 3       20     total use 4       21     total use 6       22     local use 7       Below is a first of syslog severity codes.       Severity codes are assigned to each message depending on the importance of the event that generated the message       You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above       Numerical Code       1     altert action must be talen immodulately       2     official       3     firms       4     Werning       5     Motice: internal tus significant.condition       6     informational       7     Debug-trayet messager		15	clock daemon						
17     local use 1       18     local use 2       19     local use 3       20     local use 3       21     local use 6       22     local use 7   Below is a fist of syslog severity codes.  Severity codes are assigned to such message depending on the importance of the event that generated the message to a concept the severity (see the Log Mail settings above) Vou can choose, nowwer, which messages you want to see based on their severity (see the Log Mail settings above) Numerical Code Severity 0 Emergency: system is unusable 1 Alert action must be taken immediately 2 Critical 3 Emergency: System is unusable 3 Emergency: Sy		10	local use 0						
18     local use 3       19     local use 3       20     local use 3       20     local use 4       21     local use 5       22     local use 7   Below is a fist of syslog severity codes.  Severity codes are assigned to such message depending on the importance of the event that generated the message for a control of the severity (code to a control of the result of the message system is unuable.  Neuroscience Severity 0 Benerginary: system is unuable. 1 Benerginary: Severity 0 Benerginary: system is unuable. 1 Benerginary: Severity 0 Benerginary: system is unuable. 1 Benerginary: Severity 0 Benerginary: Severity 1 Benergin		17	local use 1						
Nome         Security of a loss if and a loss if a loss if a loss if and a loss if		10	excal late 2						
21     tocal use 5       22     local use 6       23     local use 7       Below is a first of syslog severity codes.       Gevently codes.       Gevently codes are arroughed to each message depending on the importance of the event that generated the message you want to see based on their severity (see the Log Mask settings above to use choose, however, which messages you want to see based on their severity (see the Log Mask settings above to a first action must be taken immediately a distribution of the above to be taken immediately a distribution of the above to be taken immediately a distribution of the above to be taken immediately a distribution of the above to be taken immediately a distribution of the above to be taken immediately a distribution of the above terms but significant condition a distribution of the belog term immediately a distribution of the belog term immediately a distribution of the above terms in the significant condition a distribution of the belog term immediately distribution of the belog term immediate		20	tical use 6						
22     local use 6       23     local use 7       Below is a first of sysleg severity codes.       Severity codes are assigned to such message depending on the importance of the event that generated the message you want to see based on their severity (see the Log Masil settings above to use conclusion)       You can choose, towever, which messages you want to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to see based on their severity (see the Log Masil settings above to severity of the severity (see the Log Masil settings above to severity of the severity of the severity (see the Log Masil settings above to severity of the severity (see the Log Masil settings above to severity of the severity of th		21	local use 5						
23 local use 7 Below is a first of syslog severity codes. Severity codes are assigned to each message depending on the importance of the event that generated the message You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above You can choose, however, which messages (see the log Mask settings above I a severity (see the log Mask settings above to severity (see the		22	local une 6						
Below is a fist of syslog severity codes. Severity codes are assigned to each message depending on the importance of the event that generated the message You can choose, however, which messages you want to see based on their severity (see the Log Masil settings above Numerical Code Severity 0 Emergency, system is unusable 1 Alert action must be taken immediately 2 Critical 3 Error 4 Warming 5 Motore i normal but significant condition 6 Informational 7 Debug-teept messager		23	local use 7						
Severity codes are assigned to each message depending on the importance of the event that generated the message You can choose, however, which messages you want to see based on their severity (see the Log Mass settings above Numerical Code Sevenity 0 Emergency: system is unusable 1 Alert: action must be taken immediately 2 Ontical 3 Error 4 Warning 5 Motoe: normal but significant condition 6 Informational 7 Debug-teept messager		Relow is a list of suslog severity	codes.						
Severity codes are assigned to each message depending on the importance of the event that generated the message You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above Numerical Code Severity 0 Emerginary, system is unusable 1 Alert action must be taken mendiately 2 Ontical 3 Error 4 Weening 5 Motion: Internal but significant condition 6 Informational 7 Debug-teept messages		contract of the second second second							
You can choose, however, which messages you want to see based on their sevenity (see the Log Masil settings above Numerical Code Sevenity 0 Emergency: system is unusable 1 alert: action must be taken immediately 2 Critical 3 Enor 4 Warning 5 Notice: normal but significant condition 6 Doformational 7 Debug-texpt messages		Severity codes are assigned to each message depending on the importance of the event that generated the message.							
Numerical Code         Sevenity           D         Emergency: system is unusable           1         alert: action must be taken immediately           2         Critical           3         Broit           4         Warning           5         Nettice: normal but significant condition           6         Doformational           7         Debug-tergit messager		You can choose, however, which messages you want to see based on their severity (see the Log Mask settings above).							
0 Brenzpracy, system is shuadele 1 Alert: action must be taken immediately 2 Critical 3 Bros 4 Werning 5 Notice: normal but significant condition 6 Johanational 7 Crebug-frequimissages		Numerical Code	Severity						
Alert: action must be taken immediately     Ciricul     Revol     Revol     Warning     Notice: inerval but significant condition     Difformational     Cebug-level messages		0	Emergency: system is unusab	in a second s					
a critical 3 Error 4 Warning 5 Notice invest but significant condition 6 Informational 7 Debug-Invest missages		1	Alert: action must be taken a	nneGately					
Warning     Metrice: internal but significant condition     Solution:     Debug-ferent missages		-	Critical Rites						
Notce i normal but significant condition     Cologinational     Debug-terupt messages			Wenning						
6 Informational 7 Debug-level messages		8	Notice: normal but significant	condition					
7 Debug-level messager		D	Informational						

Figure 4-26. Syslog Configuration Page

# **Configuring SNMP**

The Simple Network Management Protocol (SNMP) is the most widely used way to gather information about the status of individual nodes on the network and make changes in the operational parameters of the nodes. The **SNMP** link lets you control the SNMP settings for the SLK.

*Note:* If you are not familiar with using SNMP, do not change the settings on this page.





#### System Variables

This area lets you specify the location where the SLK resides, a system contact, and a system name.

#### **Community Names**

This area lets you define the read and write community name to be used.

#### **Trap Send Enable**

This area lets you enable or disable SNMP notifications and authentication traps.

#### **Trap Destination**

This area lets you specify a target IP trap address and a target IP trap port.

# **Performing Information Activities**

SLK information activities can be performed using the links under **Information** in the menu pane of the web control interface. Table 4-5 lists the SLK operation activities.

Menu	Description	See Page
Full Menu Tree	Displays an expanded menu of SLK functions and current settings.	4-45
Browse Menu Tree	Displays a representation of the OSD menu.	4-46
Connection	Displays miscellaneous installation and SSL information.	4-47
Version	Displays serial numbers and versions for your installation.	4-48
Capture Settings	Shows a snapshot of the system log and settings in text format.	4-49
Copyright	Shows the Open SSL encryption copyright requirements.	4-50

	Table 4	4-5.	SLK	Information	Activities
--	---------	------	-----	-------------	------------

# Viewing the Full Menu Tree

The **Full Menu** link displays an expanded, interactive tree view of all the operation and configuration functions. This is an alternative access method for configuring SLK functions and provides a visual mapping to the OSD selections.

LANTRO	SLK16
A Loose	OSD Menu
Control Hosts	
View Hosts Prevent Constrai	<ul> <li>Channel Evilop John (10 items)</li> <li>Channel #01: Support PDC</li> </ul>
User Activity	<ul> <li>Channel #02: Linux - Red Hat</li> </ul>
Event Log Flash File System	<ul> <li>Channel #04: Win 2003</li> </ul>
Debug	Channel #05: Noname
Configuration	<ul> <li>Chattel #07: We NT + Server</li> </ul>
Network	<ul> <li>Channel #00: Support BDC</li> </ul>
User Accounts	Channel #10: Noname
Change Password flacurity	Channel #11: Noname
Monitoring	• Chamel #13: Noname
Senal Ports Local User/VNC	Channel #14: Noname
Data & Time	• Chattel #10. Noname
Syslog StMD	Satur Manus (11 items)
Information	<ul> <li>IP address = 172.19.0.216</li> </ul>
Full Menu Tree	<ul> <li>Subtet mark = 255 255.0.0</li> <li>Subtet mark = 275 250.0</li> </ul>
Connection	<ul> <li>ETH Speed/Duples = 100 M8PS/FULL DUP</li> </ul>
Version	<ul> <li>Commit IP. config changes</li> </ul>
Capture Settings	<ul> <li>MaC Address = 00:00:43:88:27:4a</li> </ul>
100.00	<ul> <li>Ethernet's current IP = 172.19.0.216</li> </ul>
	Electart PPP Server
	<ul> <li>Local IP address = 172,10,10,10</li> <li>Design 10 address = 172,10,10,10</li> </ul>
	<ul> <li>Yan Jacobion Header Compression = Enabled</li> </ul>
	<ul> <li>Erotocol Field Compression = Enabled</li> <li>Address Field Compression = Enabled</li> </ul>
	Authentication = CHAP
	Econ <sup>4</sup> Annue     Tanton
	ACCHS = FITTERF
	<ul> <li>Modem Initialization = AT GF L2</li> <li>Monitoring testings (22 item)</li> </ul>
	Alert email addresses =
	<ul> <li><u>SMTP relay/destruction (IP address)</u> = (dsabled)</li> <li>Message format = Normal</li> </ul>
	<ul> <li>Send small for alerts = Yes</li> </ul>
	Eover-cycle host if dert happens = No     Alert if no video = No
	<ul> <li>Alart If no NumLock toggle = No</li> </ul>
	Alert if test (blue screen) = No     Alert if turtle mode active = No
	<ul> <li>Alart if host power lost = No</li> </ul>
	Alert if my power must = No     Alert if my Ethernet link down = No
	<ul> <li>ICMI Fing this address = (disabled)</li> </ul>
	HTTP Pint cort number = 80
	Hotspot temperature = 30°C
	Video monitoring View 1 = 107
	<u>Video monitoring View 2 = 9</u>
	Video monitoring View 4 = 0
	Which Channels to Monitor     Automatic Automatics
	State Configuration (9 items)
	Systemation = Server-room 1     Secondariant = Admin
	<ul> <li>Systiame = KVM</li> </ul>
	Eread Community     Write Community
	<ul> <li>Trap Destination IP = 10.0.0.2</li> </ul>
	Trap Destination Port Number = 162     Enable SMMP Auth Tracs = No
	<ul> <li>Enable SMMP Notifications = No</li> </ul>
	Syslog Configuration (3 items)     Syslog Collector ID address = (No syslog)
	<ul> <li>Syslog Facility = 16</li> </ul>
	Log Mask (HER) = ff     Security settings (21 items)
	Change overal security mode (3 items)
	Default related security     Internal LAN with encoders
	<ul> <li>For size on the public Internet</li> </ul>
	<ul> <li>SCA Access Manager Name = KCA</li> </ul>
	<ul> <li>SCA Access Manager Password =</li> </ul>
	<ul> <li>Jurtie mode + Disabled</li> </ul>

Figure 4-28. OSD Menu Page

# Viewing the Browse Menu Tree

The **Browse Menu Tree** link shows the collapsed structure of the Full Menu Tree. If you click a link, the next page provides a high-level, at-a-glance view of the channel or setup menus. (SLK16 only)

LANTRO					
Control Hosts Control Hosts View Hosts Power Control User Activity Event Log Flash File System Debug	OSD Menu • <u>Channel Switch Menu (16 items)</u> • <u>Setup Menus (11 items)</u> Back				
Configuration Network PPP User Accounts Change Password Security Monitoring Serial Ports Local User/VNC Date & Time Syslog SNMP	Home, I Back, I Logout Copyright © Lantronix, Inc. 2004. All Rights Reserved.				
Information Full Menu Tree Browse Menu Tree Connection Version Capture Settings Copyright					

#### Figure 4-29. OSD Menu Page

# **Viewing Connections**

The **Connection** link displays a page containing connection and SSL information related to the SLK. Figure 4-30 shows an example of this page.

#### Figure 4-30. Viewing Connection Information



# **Viewing Version Information**

The **Version** link displays a page containing firmware release version information. The network administrator can view (and record) the MAC address from this page without having to remove the device from its installation. Figure 4-31 shows an example of this page.



#### Figure 4-31. Version Information Page

# **Viewing Capture Settings**

The **Capture Settings** link lets you capture text of log entries and system settings to aid in troubleshooting.

#### Figure 4-32. Capture Settings Page

LANTRO	SLK16
Ligned     Operation     Cantrol Hosts     View Hosts     Power Cantrol     User Activity     Event Log     Flash File System     Debug	Capture Settings Before contacting your customer support organization, click the following links to create text files that capture the settings of your SLK16 unit. It will help our troubleshooting personnel assess the problem that you are having.  • Text copy of system log. Use the File command "Save As" from your browser to collect the information in a text file.  • Text copy of system settings. Use the File command "Save As" from your browser to collect the information in a text file.
Configuration Network PPP User Accounts Change Password Security Monitoring Senial Ports Local User/VNC Date & Time Syslog SNMP	The Vou may save the file as "C:\SLK16_settings.txt". We encourage you to review the text files prior to sending them to your customer support organization. You may wish to edit the files if you feel any information should remain confidential. Home   Back   Logout Copyright © Lantronix, Inc. 2004. All Rights Reserved.
Information Full Menu Tree Browste Menu Tree Connection Version Capture Settings Copyright	

**Note:** The saved settings file allows you to view the configuration for reference. It does not provide a format that can be used to upload a saved configuration for reinstallation. (See "Debug (SLC16 only)" on page 4-18 for this functionary.)

# **Viewing Copyright Information**

The **Copyright** link displays a page that shows the text that users of Open SSL are required to post on their web sites.

#### Figure 4-33. Copyright Page



# 5: Using the OSD Interface to Configure the SLK

This chapter describes how to use the local console's On Screen Display (OSD) interface to configure SecureLinx SLK Remote KVMs. Topics in this chapter include:

Торіс	Page Number
"Overview"	5-1
"Logging into the OSD"	5-2
"Navigating through the OSD"	5-3
"Channel Switch Menu"	5-4
"Setup Menu"	5-5
"Network Configuration Menu"	5-5
"PPP Options (SLC16 only)"	5-7
"Monitoring Settings Menu"	5-8
"Network Management Settings Menu"	5-11
"Security Settings"	5-13
"User Administration"	5-15
"Serial Port Configuration"	5-16
"Local User Control"	5-18
"Virtual Network Computing"	5-20
"Channel Configuration"	5-20
"Power Outlet Administration"	5-20
"Debug – (Factory Only)"	5-20

# **Overview**

In addition to the web control interface, you can use the local OSD interface to configure the SLK. During the SLK installation procedure, you used the OSD interface to perform the initial network configuration required to set up remote access. Generally, users find the graphical web control interface more intuitive and easier to use than the OSD's text-based interface. *Note:* Alpha-numeric naming restrictions within the OSD are strict. You can enter names that contain upper- and lower-cased a-z and 0-9, as well as period and @ sign. If you use other characters, results may be erratic or confusing.

**Note:** All OSD operations are fully described in the web control interface chapter (see Chapter 4, "Using the Web Control Interface to Configure the SLK" on page 4-1). If you are uncertain about an OSD operation, find its explanation in the like-named menu item in the web control interface. For example, **local user control** in the OSD is duplicated by the Home page menu item called **Local User/VNC** in the web control interface.

# Logging into the OSD

Scroll

To log into the OSD, press the key twice. The OSD menu in Figure 5-1 displays.

**Note:** If the local console is attached to the SLK via a KVM switch that uses as a display command, you can redefine the local console key combination to invoke the OSD menu by redefining the VNC/OSD hotkey on the Local User/VNC Configuration page in the web interface (see "Configuring Local User/VNC Settings" on page 4-39).

For example, pressing twice can be defined to invoke OSD instead of pressing

*twice. For a list of available key values, see* Chapter 9, "Defining Custom Send Keys" on page 9-1.

	<b>*</b>		
Docs for Deview op	Registry First		
WORD 2002	Notepad (2)		
P.		OSD N	lenu
WinZip		Channel Switch Menu	
_		Setup Menus	
<b>W</b>			
WORD 2002			
(2)		Keys:	Enter (ESC=quit)

#### Figure 5-1. OSD Menu

Scroll

# Navigating through the OSD

The OSD has no mouse support, only simple keyboard navigation commands shown below the black screen. Table 5-1 lists the keys for navigating through the OSD.

То	Press
Navigate through the menu and highlight line items.	Arrow keys up/down, or page up/down keys
Return to the previous menu branch	Left arrow
Expand a menu item that contains a + sign.	Right arrow or Enter
Change or commit a value.	Enter
Quit OSD and return to the desktop	Esc

Table 5-1.	Navigating	through	the	OSD
------------	------------	---------	-----	-----

*Note:* In the following OSD screens, numbers beside each line refer to the explanations with matching numbers.

# **Channel Switch Menu**

From the OSD menu (Figure 5-2), highlight the first option to choose channels to control at the local console. To select an active channel, use the directional arrows to highlight that channel and press **Enter**. The SLK then switches the Local Console view to that channel. (The SLK8 and SLK1 do not display this item. They display each available channel as a separate item).



#### Figure 5-2. Channel Switch Menu

- 1 Channel #1-8. Use the **down arrow** to navigate to a channel. Press **Enter** to select, view, and control the channel.
- 2 Channel # 9-16. To view these channels, use the **down arrow** to continue past the channel 8 menu item.

# **Setup Menu**

From the OSD menu (Figure 5-1), move the cursor down to the **Setup Menu** and press **Enter.** (For the SLK8, move the cursor up.) The Setup menu opens, with OSD functions arranged in categories (see Figure 5-3). The following sections describe these categories.





# **Network Configuration Menu**

From the Setup menu in Figure 5-3, ensure that **Network Configuration** is highlighted and press **Enter** to open the menu.



#### Figure 5-4. Network Configuration Menu

From the Network Configuration menu (Figure 5-4), use the following procedure to configure the network details for the SLK.

1 **IP address**. Highlight **IP address**, press **Enter**, and type the IP address for the SLK you are configuring.

If you prefer to use Dynamic Host Configuration Protocol (DHCP), type the IP address 0.0.0.0 to configure the SLK to request a dynamic address. When

configured for DHCP, the **IP address** field displays **DHCP**, and the **Ethernet's current IP** field displays the acquired address.

- 2 **Subnet mask**. Highlight **Subnet Mask**, press **Enter**, and type the value for the subnet mask.
- 3 **Default gateway**. Highlight **Default Gateway**, press **Enter**, and type the IP address for the default gateway.
- 4 **Commit IP config changes**. When you select **Commit IP config changes**, the SLK attempts to verify the configuration. If it does not identify a conflict on the network, the OSD is refreshed to display the new values.

Scroll

When you make changes to the **Network Configuration**, you must select **Commit IP Changes** to enable the configuration. Otherwise, the new configuration will take effect after the next reset or power cycle. The OSD screen vanishes after a short

pause, so you have to press

twice to continue with OSD.

**Note:** Before you change an existing dedicated IP address, **close all remote user sessions**. Otherwise, the running sessions may get locked up and become unavailable to remote users (because they no longer have an IP address to which they can respond). If this happens, perform a warm reset of the SLK from the Debug menu.

- 5 **Machine name**. A simple text string that identifies this machine. To change the machine name, enter a new alphanumeric name up to 20 characters long with no special characters.
- 6 **MAC address**. Displays the hardware address of the Ethernet interface on this SLK. It is assigned by the factory to uniquely identify this SLK and cannot be changed.
- 7 Ethernet's current IP. Displays the current IP address of the SLK.
- 8 **PPP options**. SLK16 users can set PPP options by pressing **Enter** to specify a **dialup URL**. You must have serial port 3 set to **Modem** mode and have a modem connected to the serial port. If you set port 3 to **Modem** without connecting a modem, system performance will suffer because the SLK16 will keep looking for a modem attached to serial port 3.

# PPP Options (SLC16 only)

Select the lines you need to change in PPP Options and press **Enter** to change as required.

	Figure	5-5. PPP Options	
	Finance	PPP Options	
•	Restart PPP Server		
9 10	Local IP address:	172.18.18	
11	Remote IP address:	172.18.18.18	
12	Van Jacobon Header Compressio	on: Enabl	
13	Protocol Field Compression:	Enabled	
14	Address Field Compression:	Enabled	
15	Authentication:	CHAP	
16	Peer's Name:		
17	Secret		
18	Modem Init String		
19	ACCM		
	Keys: 📫 🏚 🏫	Enter (ESC=quit)	

- 9 **Restart PPP server**. Reset the server function in the SLK.
- 10 Local IP address. Address of the SLK for dial-up.
- 11 Remote IP address. Address of the client (remote) PC.
- 12 **Van Jacobson Header Compression**. Enable if your traffic is mostly small packets that can benefit from reduced header size; otherwise, ignore.
- 13 **Protocol field compression**. Enable to reduce overhead.
- 14 Address field compression. Enabled by default. Sends compression warning.
- 15 Authentication. Login authentication. Select the level you want to support.
- 16 Peer's name. Enter the peer's user name.
- 17 Secret. Dialup account password paired with peer's name.
- 18 **Modem Init String**. Initialization string specific to the modem attached to the SLK serial port. For more information, see "Configuring PPP Settings" on page 4-21.
- 19 ACCM. Asynchronous Control Character Maps. Provides a way to negotiate the use of asynchronous control characters. For more information, see "Configuring PPP Settings" on page 4-21.

# **Monitoring Settings Menu**

The Monitor Settings menu spans three OSD screens. Use the **up** and **down arrows** to navigate between them. From these menus you can configure the SLK to continuously monitor the attached servers for common failures. If such a failure occurs, the SLK logs the event and can be configured to alert an administrator via email. Alternatively, for more autonomous monitoring, the SLK can be configured to automatically reset power (power-cycle) to an attached server that reports one of the enabled alerts (this feature requires use of a third-party power control unit).

# **First Monitoring Settings Screen**

Highlight and select **Monitoring Settings** from the **Setup Menus** screen (see Figure 5-3). The first of three available menus displays (Figure 5-6).

Specify an address if you need to	♥ more Monitoring setting	
get alerts 1	Alert email addresses: SMTP relay & destination (IP address):	
3	Message format: Send email for alerts:	No
5	Power-cycle host if alert happens:	Yes
6 7	Alert if no NumLock toggle:	Yes
8	Alert if text (blue screen):	Yes
	Kevs: Enter (ESC=quit)	

#### Figure 5-6. Monitoring Settings Screen (1 of 3)

Note: All alert conditions are disabled by default.

- 1 Alert email addresses. Enter the email address of the administrator who should be notified.
- 2 **SMTP relay.** Enter the IP address of the SMTP server to use to send mail. This server should be the mail server for the domain or a server willing to relay to the specified email address. To disable, set the address to 0.0.0.0 (default)
- 3 **Message format.** The email message format can be configured for either normal (default) or short messages.
- 4 **Send email for alerts.** Enabled by default, but this setting will not take effect until an SMTP server address is configured and enabled.
- 5 **Power-cycle the host.** The SLK can be configured to use a third-party power control unit to automatically reset a server after a reported failure.

*Note:* This choice carries risk because the failure tests may sometimes report a fault erroneously.

6 **Alert if no video.** Enabling this alert causes a notification if no video signal comes from one of the controlled servers.

Note: Active screensavers (DPMS) can trigger this notification erroneously.

- 7 Alert if no NumLock toggle. If this is enabled, the SLK simulates the key being pressed every few seconds. If the NumLock light does not toggle in response to pressing the NumLock key, the server is assumed to have crashed and this error condition becomes active. To enable, select Yes. To disable, select No.
- 8 Alert if text (blue screen). If this server enters text mode, (which can occur if the attached server is rebooting and displaying boot information or is displaying the Windows blue screen). To enable, select **Yes**. To disable, select **No**.

### **Second Monitoring Settings Screen**

Figure 5-7. Monitoring Settings Screen (2 of 3)



Keys: main and Enter (ESC=quit)

- 9 Alert if Turtle Mode active. Turtle Mode is activated if too many bad login attempts occur between successful logins (this setting is dependent upon the security level selected). To enable, select Yes. To disable, select No.
- 10 Alert if host power lost. This alert is triggered if an attached server loses power. Power loss of the server is determined by power loss on the PS/2 ports. To enable, select **Yes**. To disable, select **No**.
- 11 Alert if my power is reset. If the SLK is reset or powered off for any reason, this alert is activated when power is restored. This alert might be used in combination with other controls. To enable, select **Yes**. To disable, select **No**.
- 12 Alert if my Ethernet link down. If the Ethernet signal to the SLK is lost, this condition is activated. Since the SLK is off the network in this situation, it is only able to send the alert once connectivity has been restored. However, the event is logged for future troubleshooting. To enable, select **Yes**. To disable, select **No**.
- 13 **ICMP Ping this address.** This address should be an IP address that will be pinged continuously. This error condition is triggered if more than half the

packets are lost during a short interval. This IP address does not need to be that of the controlled server but might be a border router or other "always-on" network component. To enable, enter an IP address to ping. To disable, type 0.0.0.0 (default).

- 14 HTTP Ping this address. The number designated for HTTP pings of addresses/ ports should be an IP address of a web (HTTP) server. The server will be asked to get the root page. If nothing is returned (zero length) or the connection fails, this error condition is considered active. To disable, type 0.0.0.0.
- 15 **HTTP Ping this port number**. The number designated for HTTP pings of addresses/ports should be an IP address of a web (HTTP) server. The server will be asked to get the root page. If nothing is returned (zero length) or the connection fails, this error condition is considered active. To disable, type 0.0.0.0.
- 16 Hotspot temperature. Displays the current internal temperature of the SLK.

# Third Monitor Settings Screen (SLK16 only)

**Note:** SLK8 shows **Current Time** (monitor menu 2) and **Timezone Offset** (monitor menu 3).

Figure 5-8. Mc	nitor Settings Scree	en – SLK16 Only (3 of 3)
----------------	----------------------	--------------------------

	more 👕	Monitoring setting
17	Video monitoring server port:	19902
18	Video monitoring view 1:	1
19	Video monitoring view 2:	2
20	Video monitoring view 3:	3
21	Video monitoring view 4:	4

Keys: Man Hand Keys: Key

- 17 Video monitoring server port. Allows configuring of the Java port used for video monitoring to a custom port number.
- 18 Video monitoring view 1. First of four arrangements of screens that you can store as hexadecimal values.
- 19 Video monitoring view 2. Second of four arrangements of screens that you can store as hexadecimal values.
- 20 Video monitoring view 3. Third of four arrangements of screens that you can store as hexadecimal values.
- 21 Video monitoring view 4. Last of four arrangements of screens that you can store as hexadecimal values.

# **Network Management Settings Menu**

To configure network logging, use the menus in Network Management Settings (see Figure 5-9). Network Management Settings has two sub-menus, SNMP Configuration and Syslog Configuration.



Figure 5-9. Network Management Settings

*Note:* The SLK8 and SLK1 display SNMP and Syslog as unique top-level menu selections.

# **SNMP** Configuration

**SNMP Configuration** lets you configure Simple Network Management Protocol settings for device communication. Highlight **SNMP Configuration** and press **Enter** to open the SNMP menu (Figure 5-10).

#### Figure 5-10. SNMP Configuration Menu



Keys: Man Lenter (ESC=quit)

- 1 SysLocation. The physical location of the SLK.
- 2 SysContact. User ID of the responsible contact.
- 3 SysName. The name of the SLK.
- 4 **Read Community**. Community that can read messages. (These display as asterisks on the SLK8).

- 5 Write Community. Community that can write messages. (These display as asterisks on the SLK8).
- 6 **Trap Destination IP**. IP address of SNMP management station (e.g., HP OpenView).
- 7 **Trap Destination Port Number**. UDP port number of the SNMP management station (default 162).
- 8 **Enable SNMP Auth Traps**. Enabling authentication traps generic to SNMP. Enabled is the default.
- 9 Enable SNMP Notification (SLK8 only). Enabled by default.

# **Syslog Configuration**

**Syslog Configuration** follows the Internet Engineering Task Force standard for handling system events. Highlight **Syslog** to display choices for system logging (Figure 5-11).



- 1 **Syslog Collector IP address**. Type IP address of Syslog collector (daemon). The default is **no syslog**.
- 2 **Syslog facility**. Numeric designation of message facility (default 16).
- 3 Log Mask. Hex code of severity. Pick any of 8 available codes listed (00–FF). For information about converting binary numbers to hex format, see Chapter B, "Binary to Hexadecimals'. For more details about Syslog configuration, see Figure 4-26.
# **Security Settings**

There are two OSD screens for configuring the SLK security.

# **Initial Security Screen**

The first security screen handles functions like Stealth and Turtle as well as general policy.

- Change overall security mode. Press the right arrow key to select between relaxed, snooper, or public options. (See Figure 4-19.)
- Admin password. The password for the master account (for which the user ID can be only root or administrator).
- Turtle mode. Select to disable (default) or set sensitivity to authentication failure.
- Turtle reset timeout. Type the number of hours that the SLK locks out remote access after Turtle mode has been triggered. Local reset is allowed.
- **Reset Turtle protection now**. Manual reset is allowed only at local console.
- Stealth mode. Select Enabled to conceal your presence on the net. Ignores pings.
- Require encryption. The default is Optional. When set to Mandatory (on SLK1 and SLK8, this option is Required), all Web requests are rerouted to HTTPS ports.

The SLK provides SSL encryption. For this feature to work, install in the SLK a valid server certificate and key provided by a trusted source. The certificate and key must be in PEM format and the name of the files should be server-cert.crt and server-cert.key. To install the certificate and key, access the flash file system through the web control interface and upload the certificate and key through the browser (see "Using Security and Encryption" on page 8-3). Perform a hard reset to have the SLK load the new certificate and key and delete any old ones in the system. If you use a browser, you must have the **Sun Java Plug-in 1.4.0** or higher installed. SSL setup is not available through VNC.

**Note:** Be sure an appropriate certificate/key is installed and functional before changing the mode. If the certificate/key is not installed, not loaded, or wrong, mandating HTTPS locks out the SLK to any remote access. For installation information, see Chapter 8.

HTTP port number. You may specify a number other than the HTTP default port number of 80. (HTTP port number is on the second screen in the SLK8.)

# Second Security Screen

The second security screen offers the user additional security by allowing changes to default port numbers, as well as forcing logout of idle terminals.

HTTPS port number. You may specify a value other than the HTTPS default port number of 443.

- Reset web server. Select and press Enter to reset Web server to implement new Web server settings.
- Idle logout. This logs out sessions that are no longer in use and makes these resources available for a new remote connection. The default is 30 minutes. Enter the number of minutes to change idle logout time.
- Telnet server port. Enter the new Telnet port number that you want to use. Type 0 to disable.
- JavaViewer port number (clear). "Clear" means unencrypted. The default value is 19900. To change, enter the new JavaViewer port number that you want to use.
- JavaViewer port number (SSL). The default value is 19901. To change from default, enter the new JavaView port number that you want to use.
- Viewer encryption policy (SLK16 only). KM1 only encrypts keyboard and mouse data. KVM encrypts keyboard, video, and mouse data streams with reduced performance.
- Channel locking policy (JView) (SLK16 only). The default setting, Manual, initiates channel access without locking. Automatic locks down the channel being accessed during initiation of the remote session.

# **User Administration**

If you have the authority to access this screen, you can configure new users and assign their passwords and system privileges. The total number of user accounts you can specify depends on the SLK model you have:

- SLK1 and SLK8: You can specify 10 user accounts.
- SLK16: You can specify 32 user accounts.

#### Figure 5-12. User Administration

Four OSD screens let you set passwords for 32 users	User administration () User #1 () User #32
$\smile$	Keys: 🗰 🏟 🚭 Enter (ESC=quit)

1 **User #**: Highlight the user number for the person whose name and password you want to configure. This opens that user account for editing.

#### **User Name Fields**





- 1 **User 1 Name**: Enter a user name or a user ID for the first user. The name can contain up to 19 contiguous alphanumeric characters. Including non-alphanumeric characters or spaces results in an unusable account.
- 2 **Password**: Enter the password for the account. Confirm the password when prompted.
- 3 Account type: Accounts can be disabled or enabled.
- 4 **Channel Privileges**: Select authorized actions for the channel. For more information, see step 6 on 4-27.

*Note:* You can create user accounts using the OSD, but you must define server access using the web control interface.

# **Serial Port Configuration**

Using the serial port screens, you can configure the SLK serial ports. For the SLK16, you can also configure serial port 3 for a dial-up response.

For each available setting, select the menu item and press **Enter** to advance through the options.



	➡ more	Serial port (RS-232 co	onfig)
1	C Port 1 - Baud r	ate settings	
2	P1 - Serial port 1 n	node:	PowerModule-8
3	P1 - Watchdog mo	vde:	Log lines
4	P1 - Watchdog pat	ttern:	
5	P1 - Watchdog tim	eout:	1 minutes
6	C Port 2 - Baud r	ate settings	
7	P2 - Serial port 2 m	node:	Log
8	P2 - Watchdog mo	ode:	Log lines

Keys: Math Keys: K

1 **Port 1 - Baud rate settings.** The default is 38400/8/N/2/N (see Figure 5-15). Select and press **Enter** to open the option list.

Figure 5-15. Serial Port 1 — Baud Rate Settings

		Port 1 - Baud rate settings	
13	P1 - Baud Rate:		38400
14	P1 - Data bits:		8 bits
15	P1 - Parity:		None
16	P1 - Stop bits:		2 stop bits
17	P1 - Flow Control:		None

Keys: Market & Enter (ESC=quit)

- P1 Baud Rate. Choose a baud rate, in bits per second (bps), for serial port 1.
- P1 Data bits. Choose 7 or 8 bits.
- P1 Parity. Choose Odd, Even, None, Mark, or Space.
- P1 Stop bits. Choose 1 or 2.
- P1 Flow Control. Choose None or CTS/RTS.
- 2 Serial port mode. Select and press Enter to advance through the available modes for serial port 1. You may select from Log, Telnet, Watchdog, and Power Control. For details see "Configuring Serial Ports" on page 4-37.
- 3 **Watchdog mode.** Select and press **Enter** to advance through the available watchdog modes for serial port 1. You may select from Log lines, Alert if found, and Alert if missing. For details see "Configuring Serial Ports" on page 4-37.

- 4 **Watchdog pattern.** Select to enter the watchdog pattern. Each channel is matched against this simple string.
- 5 **Watchdog timeout.** Select and press **Enter** to edit. Enter timeout values in minutes.
- 6 Port 2 Baud rate settings. The default is 38400/8/N/2/N (Figure 5-16). Select and press Enter to open the option list. Select Port 2 settings (Baud Rate, Data bits, Parity, Stop bits, Flow Control) in the same way as for port 1.

	Port 2 - Baud rate setting:	s
P2 - Baud Rate:		38400
P2 - Data bits:		8 bits
P2 - Parity:		None
P2 - Stop bits:		2 stop bits
P2 - Flow Control:		None

Figure 5-16. Serial Port 2 — Baud Rate Settings

Keys: Mar & Enter (ESC=quit)

- 7 Serial port mode. Select and press Enter to advance through the available modes for serial port 2. You may select from Log, Telnet, Watchdog, and Power Control. For details see "Configuring Serial Ports" on page 4-37.
- 8 **Watchdog mode.** Select and press **Enter** to advance through the available watchdog modes for serial port 2. You may select from Log lines, Alert if found, and Alert if missing. For details see "Configuring Serial Ports" on page 4-37.





- 9 **Watchdog pattern.** Select to enter the watchdog pattern. Each channel is matched against this simple string.
- 10 **Watchdog timeout.** Select this menu item and press **Enter** to edit. Enter timeout values in minutes.
- 11 **Port 3- Baud rate settings**. The default is 38400/8/N/2/N (see Figure 5-18). Select and press **Enter** to open the option list.

Port 3 - Ba	ud rate settings
P3 - Baud Rate:	115.2k
P3 - Data bits:	8 bits
P3 - Parity:	None
P3 - Stop bits:	1 stop bits
P3 - Flow Control:	CTS & RST

Figure 5-18	. Serial Por	t 3— Baud	Rate Settings
-------------	--------------	-----------	---------------

Keys: 10-48 Enter (ESC=quit)

Port 3 settings (Baud rate, data bits, parity, stop bits, and flow control) are selected the same way as for port 1.

12 **P3 serial port 3 mode**. PPP (dial-up through modem). Select and press **Enter** to select other modes on port 3. This option is valid for the SLK16 only.

# **Local User Control**

This screen allows administrators to configure local usage of the targeted server.

#### more... Local user control Reset local keyboard+mouse 1 Resync mouse position 2 3 Mouse threshold: 4 Mouse acceleration: 5 Local console: No passwords 6 Local User exclude: Share access Current time (approx): 7 Fri, 6 Jun 2003 Time zone offset (from UTC): 8 -240 minute

#### Figure 5-19. Local User Control Screen (1 of 2)

Keys: math Enter (ESC=quit)

- 1 Reset local keyboard and mouse. Resets these devices connected to the SLK local port. This is a good way to remove control-key locks and other undesirable states from the keyboard. You can also try resetting the mouse locally by unplugging and replugging the mouse cable.
- 2 **Resync mouse position**. Resynchronizes the mouse of the remote client and that of the server by forcing the server mouse to the top-left corner for renewed tracking.
- 3 **Mouse threshold**. Determines the starting threshold (mouse speed) for mouse acceleration. These are SLK-specific modifiers to counter disabled acceleration on target servers and rarely need to be modified.
- 4 **Mouse acceleration**. The factor by which to modify the mouse speed. See comments above for **Mouse threshold**.

5 **Local console**. The available options are No password, Require Password, and Disable access.

#### *Note:* Disable access renders the SLK inaccessible if remote access fails.

- 6 **Local User exclude**. Options are to share access with remote, have no keyboard for the local user, or have a blank screen + keyboard (no local access except for mouse).
- 7 **Current time (approx)**. Displays current time and date set on the SLK. Changes can only be applied through the web control interface. (This setting is on the Monitor Settings menu on the SLK8 and SLK 1.)
- 8 **Time zone offset (from UTC)**. Sets the time offset, in minutes, from Greenwich Mean Time (GMT). A minus sign indicates you are east of the Greenwich Observatory. (This setting is on the Monitor Settings menu on the SLK8 and SLK 1.)



Figure 5-20. Local User Control Screen (2 of 2)

- 9 Clear memory log buffer. Clears the event log in memory.
- 10 **Power Control menu**. Opens the Power Control menu when you want to change the state of a port on an optional third-party power control unit.

*Note:* This requires configuring a serial port for power control.

- 11 Rotate: Delay after last K/M (SLK16 only). Idle time (keyboard and mouse) in seconds before rotation starts. Default = 0 (disabled).
- 12 **Rotate: Time showing channel** (SLK16 only). Duration, in seconds, that each channel is displayed. Default = **0** (disabled).
- 13 **Reset the power to outlet** *n*. Turns the power state **off** and then back **on** for outlets 1 through 16, regardless of the current power state (same as Cycle Power).
- 14 **Turn off power to outlet** *n*. Turns the power state **off** for the selected outlet (1-16). Requires use of third-party power control.
- 15 **Turn on power to outlet** *n*. Turns the power state **on** for the selected outlet (1-16). Requires use of third -party power control.

# **Virtual Network Computing**

If you can access the web control interface but cannot use the Java Viewer to remotely control the attached servers, you can choose Virtual Network Computing (VNC). This OSD screen allows configuration of the VNC server port number, bandwidth goal, and display resolution. It also displays the current OSD/VNC hotkey setting (this value must be changed through the web control interface).

- **VNC server port number**: Specify a server port number or leave the default.
- Bandwidth goal, network bandwidth, and resolution can be set or optimized for those who use VNC frequently. Others may choose to keep the defaults.

# **Channel Configuration**

This screen allows administrators to alter generic names (for example, Channel 1) to custom names that more accurately identify the attached server. Options include:

- Channel Name
- Emergency Contact Name
- Emergency Contact Number
- Operating System
- Mouse Acceleration Type (choose None, Microsoft Win, Sun Solaris)

**Note:** Operating systems use different mouse acceleration algorithms. Proper identification of the attached operating system allows the SLK to adjust mouse synchronization accordingly.

# **Power Outlet Administration**

This screen allows administrators to alter generic names (for example, Outlet 1) on an attached power control unit to custom names that more accurately identify the attached server. Options include:

Synchronize Outlet Names to Channel Names

# **Debug – (Factory Only)**

This screen provides OSD map and maintenance options (including a warm reset feature). Do not change settings in this submenu unless authorized by Lantronix Technical Support.

# 6: Using a VNC Viewer to Access the SLK

This chapter describes how to use a Virtual Network Computing (VNC) viewer to access target servers attached to SecureLinx SLK Remote KVMs. Topics in this chapter include:

Торіс	Page Number
"Overview"	6-1
"Using a VNC Viewer to Access Target Servers"	6-1

## **Overview**

You can use a VNC viewer to access target servers. To download a free VNC viewer, visit http://www.realvnc.com/download.html or search the Web for the keywords "vnc" and "research vnc". The VNC site also offers examples and instructions, which are not repeated here.

Note that:

- VNC is a thin client (consumes only 228 K) and is command-line oriented.
- VNC can be configured locally in the SLK.
- VNC supports most basic features of the SLK.
- VNC cannot access the web control interface.

*Note:* VNC does not support encryption natively. However, it can be streamed over Virtual Private Network (VPN) or Secure Socket Handling (SSH) tunnels.

# **Using a VNC Viewer to Access Target Servers**

After you install the VNC viewer on your remote PC, follow these steps to remotely access and control the target server through the SLK.

- 1 At the local console, access the On Screen Display (OSD) Setup menu.
- 2 Select the **VNC** menu (see Figure 6-1 on page 6-2).
- 3 Enter the VNC server port number. You can also optimize the bandwidth and resolution, or leave them at the default values.



#### Figure 6-1. Local Console VNC Configuration Screen

- 4 At your remote PC, click the **VNC.exe** file to open the VNC Viewer.
- 5 Enter the SLK's IP address in the Connection details dialog box (see Figure 6-2). Then type a colon and the VNC port number.

*Note:* If no port number is specified (as shown in Figure 6-2), the default port 5900 is assumed and used.

Connecti	on details		×
V2	VNC server:	192.168.1.73	OK
		Use host:display	Cancel
		e.g. snoopy:2 (Display defaults to 0 if not given)	Options

#### Figure 6-2. Connection Details

- 6 Click **OK**.
- 7 Enter the SLK password in the VNC Authentication dialog box. (This is the same password you use to access the web control interface.) After a few seconds, the VNC menu appears (see Figure 6-3).

*Note:* SLK1 and SLK8 automatically show channel 1 and the last remote channel accessed, respectively.



Figure 6-3. OSD/VNC Menu with Corner Icon

- 8 Although the menu contains the word **OSD** and looks like the SLK's local OSD, it is only for remote access to the SLK.
- 9 To navigate between channels in the OSD via VNC menu, enter a value from 1-9 or A to G to select one of the 16 possible channels. The selected channel displays in the VNC window. You can also control that channel using VNC commands.

Channel	Value	Channel	Value
Channel 1	1	Channel 9	9
Channel 2	2	Channel 10	Α
Channel 3	3	Channel 11	В
Channel 4	4	Channel 12	С
Channel 5	5	Channel 13	D
Channel 6	6	Channel 14	Е
Channel 7	7	Channel 15	F
Channel 8	8	Channel 16	G

Гаble 6-2. V	/alues for	Selecting	Channels
--------------	------------	-----------	----------

Using a VNC Viewer to Access the SLK

# 7: Troubleshooting

This chapter provides troubleshooting suggestions you can follow in the unlikely event that you encounter a problem using SecureLinx SLK Remote KVMs. In addition to this chapter, you can find answers to frequently asked questions at www.lantronix.com/support.

Topics in this chapter include:

Торіс	Page Number
"General Troubleshooting"	7-2
"Keyboard Troubleshooting"	7-4
"Mouse Troubleshooting"	7-5
"Video Troubleshooting"	7-8

# **General Troubleshooting**

Problem	Suggestion
You forgot your password.	Please contact Lantronix Technical Support.
You cannot log into the SLK Web page or ping its IP	There is a problem with the assigned IP address.
	From the Local Console OSD:
	1. Go to Network Settings.
	2. Verify the IP address.
	<ol> <li>Re-enter the IP address if necessary and recommit the change.</li> </ol>
	<ol> <li>Confirm the validity of the IP addresses with your IT department.</li> </ol>
	5. Verify that the default HTTP port number is 80; otherwise you must include the port number in the URL.
	<ol> <li>When troubleshooting, disable stealth mode (otherwise there will be no ping response).</li> </ol>
When you use VNC, it only shows a portion of the remote screen. If the video resolution on the attached server is higher than that of the VNC viewer, you will not be able to see the entire remote screen	If you are looking at servers with different resolu- tions, when you switch to a higher resolution server via a KVM switch, you will not be able to see the entire remote. There are two solutions to fix this problem:
	<ol> <li>Change VNC server configuration - Max resolu- tion (expected) from Auto to Max (permanent, but uses more bandwidth).</li> </ol>
	2. Reload VNC when changing to higher resolu- tion image (not permanent).
The VNC does not work under Linux or FreeBSD.	Use "vncviewer -bgr233" to initiate the VNC viewer with the proper flag to get it to work with your SLK unit.
You want to reduce the steady-state network traffic generated by VNC.	<ol> <li>Improve video quality first. Any video noise is sent over the network, so you can reduce the resolution or refresh rate to reduce the noise.</li> </ol>
	2, Reduce the resolution to 1024x768 or lower.

## Troubleshooting

Problem	Suggestion	
You want to reduce the overall network traffic gener- ated by VNC.	<ol> <li>Use a flat-color desktop background, rather than a personal picture (e.g., your family). This data must be sent every time the window is moved, so it is best if it is a single color that requires little compression.</li> <li>Improve video quality, so no analog noise is sent.</li> </ol>	
You tried to upload firmware, but received a mes- sage that the file was not found.	Some versions of Internet Explorer cannot upload the firmware image (or any other file) if part of the file path contains a space. This is a problem, for example, if the file Image.frm is stored as C:\My Document\Image.frm. The solution is to use Netscape, or move the file to be uploaded into another directory that does not contain spaces in its file path.	



# Keyboard Troubleshooting

Problem	Suggestion	
There is no keyboard signal.	Disconnect and reconnect keyboard cable between the server and the SLK, or reset the server.	
	If you are using extended length cables, try using shorter ones.	
The local keyboard does not respond or the key- board mapping is wrong.	Locally re-seat the keyboard.	
	Make sure the SLK responds when you press the hotkey ( <b>Scroll Lock</b> ) to access the local OSD.	
	If yes, reset the keyboard and mouse using <b>OSD-&gt;Local Settings</b> .	
	If no, try a different keyboard.	
The remote keyboard does not respond or the keyboard mapping is wrong.	Remotely reset the keyboard through the web control interface or the VNC menu.	
The hotkey combination for web control interface	Reset the keyboard or change the hotkey.	
or vive viewer does not work.	<ol> <li>Remotely reset the keyboard and mouse either through web control interface or VNC menu.</li> </ol>	
	2. Change the hotkey combination in the SLK web control interface. You can access the hotkey combination under the Local/VNC configuration menu below the Keyboard Exit Key area (see "Keyboard Exit Key" on page 4-40).	

# **Mouse Troubleshooting**



**Note:** This guide refers to the mouse indicator on the attached server as the "local" mouse. We refer to the mouse on the PC accessing the KVM remotely as the "remote" mouse. (In the browser interface, the remote mouse usually displays as a crosshair icon. In the VNC interface, the remote mouse usually displays as a small black square.

Problem	Suggestion
There is no mouse signal.	Disconnect and reconnect mouse cable between the server and the SLK, or reset the server.
	If using extended length cables, try using shorter ones.
The remote and local mice work poorly or are out of synchronization.	Reset the mouse synchronization or shift the screen.
	<ol> <li>Using the web control interface, click the Resync Mouse button to resynchronize the mouse.</li> </ol>
	<ol> <li>Verify that acceleration has been disabled on the server according to Figure 3-7 on page 3- 12.</li> </ol>
	The mouse may be sluggish due to video noise. See "Video Troubleshooting" on page 7-8.
The mouse is always in the wrong position by a small, fixed amount. This persists even after a "mouse resync" operation.	There is a screen position error, so the SLK's idea of the mouse position is offset by the width of the black bars/or missing area.
	Realign the screen from either the web control interface or VNC viewer:
	From the web control interface, toggle the Shift Screen to "On". Use the arrow keys to change the position of the screen until the mouse is aligned.
	From the VNC viewer, use the phase shift command.
The remote (console) mouse does not respond.	Locally re-seat the mouse.
	Reset the keyboard and mouse using <b>OSD&gt;</b> Local Settings.
	Try a different mouse.

## Troubleshooting

Problem	Suggestion
The local mouse (on the attached server) does	Perform the following steps:
	1. Disconnect and reconnect connections.
	<ol> <li>Select "Reset local keyboard+mouse" from Local user control in the OSD (see "Local User Control" on page 5-18).</li> </ol>
	<ol> <li>Reset target server to re-initialize the PS/2 ports. Not all computers respond well to hot- swapping mouse connections and can dis- rupt the port in the process.</li> </ol>
	4. Verify the mouse type and driver on the target server.
	<ol> <li>Try using another mouse to see if you achieve better results.</li> </ol>
The local (attached server) mouse does not respond, or the mouse mapping is wrong.	Remotely reset the mouse through the web con- trol interface or the VNC menu.
The remote (console) mouse moves but the local (attached server) mouse does not.	Be sure the web control interface window is the active window. When you move the mouse, the REMOTE focus on the top-left corner of the web control interface should be highlighted in red.
The remote and local mice move in a non-linear	Perform the following steps:
	<ol> <li>Verify that the refresh rate or the mouse setup are configured properly. See '.</li> </ol>
	<ol> <li>Check the resolution and refresh rate in use. Reduce vertical refresh rate to no higher than 75 Hz and resolution to no higher than 1280 x 1024.</li> </ol>
	<ol> <li>On the target server, turn off or set to normal, all operating system-specific adjustments to mouse speed and acceleration. See Figure 3-7 on page 3-12.</li> </ol>
	<ol> <li>Verify that the mouse driver on the target server is up-to-date and operating system- generic.</li> </ol>

Problem	Suggestion
The remote and local mice are tracking slowly.	Perform the following steps:
	1. The cause could be noisy video. Using the web control interface, log into the SLK and the target server, and observe the bandwidth meter on the web control interface window. On a static screen, the indicator should show negligible traffic (less than 20 Kbps). If the indicator is fluctuating or constantly at a higher throughput level, the video source could be noisy, generating unwanted network traffic. This would cause the video feed to appear slow and cause an apparently slow mouse.
	2. This may be an indication and the result of network latency. Mouse performance is measured by how quickly the local cursor arrow follows the remote crosshairs.

# Video Troubleshooting



Problem	Suggestion	
You see <b>NO INCOMING VIDEO</b> when trying to view a remote server.	Perform the following steps:	
	<ol> <li>Disable or time-out any video overlays, such as KVM switch status, as overlays often gen- erate noise.</li> </ol>	
	<ol> <li>Select different resolutions and refresh rates within the supported maximum of 1280 x 1024 and 75 Hz. A refresh rate of 60 Hz is highly recommended. Excessive resolution increases network activity as more data is passed from the server to remote.</li> </ol>	
	<ol> <li>Use minimum acceptable color depth set- tings. Eight bits are suitable for remote sessions.</li> </ol>	
	4. Try a different video cable. Poor quality cable can contribute to degradation and loss of signal.	
	5. If none of these suggestions improves the video, use the local console to select the appropriate video settings.	
	If you are using KVM switches in your configuration:	
	<ol> <li>Disable or time-out any permanent video overlays showing KVM switch status.</li> </ol>	
	<ol> <li>Rename the hotkeys on the SLK or the KVM switch if there are conflicts between basic VNC/OSD hotkeys and any "switch" VNC/ OSD Hotkeys. See Chapter 9, "Defining Cus- tom Send Keys" on page 9-1.</li> </ol>	

## Troubleshooting

Problem	Suggestion
You cannot see any local video.	Perform the following steps:
	<ol> <li>Check physical connections between the SLK and the local monitor.</li> </ol>
	2. Reduce the vertical refresh rate to 75 Hz and resolution to no higher than 1024x768.
	<ol> <li>Disable all energy-saving modes and screen savers.</li> </ol>
	<ol> <li>Update the driver of your video card. It may be introducing spurious noise.</li> </ol>
The remote video is scrambled.	Perform the following steps:
	1. Check your firmware version and try using different video settings. You can obtain the latest firmware updates at www.lantronix.com.
	2. Try different resolutions/refresh rates on the target servers.
Video colors are off.	Contact Lantronix Technical Support.
Video is sluggish.	Perform the following steps:
	1. Check your firmware version and try using different video settings. To update to the newest firmware, go to www.lantronix.com.
	2. Try different resolutions and refresh rates on the target servers.
Video is not updating.	Perform the following steps:
	<ol> <li>Open and close the connection to see whether the problem gets resolved.</li> </ol>
	2. From the web control interface, click the <b>Disconnect</b> button; then click the <b>Connect</b> button.
	<ol> <li>From the VNC viewer, close and reopen the VNC session.</li> </ol>

## Troubleshooting

Problem	Suggestion
You see black video when opening a browser session.	If the connect/disconnect options keep toggling, and you can connect locally through VNC and Telnet, this could be a configuration issue.
	Be sure the Java plug-in is installed. Use only the latest release of Java 2 runtime environment (J2RE). (See www.java.com.) Check the "Java- Viewer port number (clear)" and "JavaViewer port number (SSL)". These must be different port numbers than the Web server, whose default is 80 and 443. Reset the two ports to the factory- default settings of 19900 and 19901 respectively.
There is a black bar to the left and/or top of your screen.	Part of the image is cut off at the left or top edge of the screen:
	This should not occur in any VESA- standard video mode. Switch to a typical video mode (1024x768 at 60 Hz, for example). Note that some video cards do not generate VESA modes precisely, so this may not help.
	If using a non-standard VESA mode, or an unknown video source, use VNC to correct the position error manually:
	a) Start VNC and enter the VNC menu.
	b) Press twice.
	<ul> <li>c) Use the arrow keys to move the screen around.</li> </ul>
	If black bars are showing, move left (or up) until the first non-black area touches the edge of the VNC window.
	If the screen is cut off, move the window right (or down) a large amount (the edge
	will smear). Press to quit the menu. This causes a redraw. Start the process over.
	Press <b>Esc</b> at any time to redraw the whole screen and check the result. The VNC screen is an approximation of the new position. You can fine- tune the position by observing the remote mouse position relative to the VNC local cursor (small box). When the two are precisely aligned you should have the optimal screen position. The SLK remembers the new X,Y position automatically. You may need to repeat this process for other video modes.

# 8: Uploading Flash Files and Certificates

This chapter describes how to upload flash files and certificates. Topics in this chapter include:

Торіс	Page Number
"Uploading Firmware"	8-1
"Using Security and Encryption"	8-3

# **Uploading Firmware**

The firmware-upload procedure consists of the following steps:

- 1 Check the current version of the SLK's firmware.
- 2 Download the latest firmware from the Lantronix Web site.
- 3 Upload the firmware to the SLK's Flash memory.

#### Checking the Current SLK Firmware Version

Before you upgrade the SLK firmware, check the current firmware version. If your installed version matches the most recent version available on the Lantronix Web site, no download is necessary.

- 1 Click the **Version** button on the web control interface menu (see "Viewing Version Information" on page 4-48).
- 2 Note the Firmware identification string. This string should be similar to the one in Figure 8-1.

Figure 8-1. Example of a Version Number

# Product: SLK16 Firmware: 1.5e-050301.1738 Video FPGA Hardware: 2.1 Cross FPGA Hardware: 1.3

- KM Board FPGA Hardware: 1.8
- Boot EPROM: 0.1.2-040227.1754
- Serial Number/MAC Address: 00:80:a3:88:27:4a

#### Downloading Firmware from the Lantronix Web Site

Go to the Lantronix Web site at www.lantronix.com and see whether the latest firmware version is the one currently installed in your SLK. If it is, you do not need to download the firmware.

Firmware upgrades and release notes are in zipped format. The zip file contains a Flash file with the extension.frm along with release notes. You can review the release notes to see whether upgrading the firmware will benefit you.

#### **Uploading Firmware to Flash**

After you download firmware from the Lantronix Web site, you can upload it into the SLK. Uploading firmware is a straightforward operation. However, if you upload the wrong version, recovery can be time-consuming.

To upgrade the SLK Flash files:

- 1 Start the web control interface and go to the SLK home page.
- 2 In the menu pane on the left, under **Operation**, click **Flash File System**.
- 3 In the Flash File System page, under **Upload File to Flash**, click **Browse**.

Figure 8-2. Controls for Locating and Uploading Firmware

_		
File to upload:		Browse
	Start Upload	

4 Click the correct . frm file you downloaded from the Lantronix Web site; then click the **Start Upload** button to upload the firmware to the SLK Flash memory.

- 5 After the firmware has been uploaded, a message tells you that upload was successful. Click the **Reboot now** link in the bottom-right corner of the Flash File System page. Reboot disconnects you and logs you out of your current session.
- 6 Log in again to the web control interface.
- 7 From the home page, under **Information**, click **Version** to confirm that the new firmware has been installed successfully.

**Note:** Some versions of Internet Explorer cannot upload the firmware image (or any other file) if any part of the file path contains a space. If this occurs, the message **file not found** appears when you try to upload the firmware. One solution is to use Netscape, which accepts space. Another solution is to move the firmware file to another directory that does not contain spaces in its file path.

# **Using Security and Encryption**

SecureLinx SLK Remote KVMs provide security on several levels, including Secure Sockets Layer (SSL) encryption. For this feature to work, install a valid server certificate and key into the SLK. You can purchase certificates and keys from many sources.

# Using SSL with a Browser

If you use a browser, you must have the **Sun Java Plug-in 1.4.0** or higher installed to take advantage of SSL encryption. The Java plug-in can be obtained from Sun Microsystems at: www.java.sun.com/products/plugin/index.html. Alternatively, you can search the Web for the keywords "Sun," "Java," and "plugin."

# Using SSL without a Browser

SSL is not available through VNC. Consequently, some type of browser is required.

#### **Locating Internet Resources**

A site that offers official certificates is <u>www.thawte.com.</u> You can locate other certificate providers on the Web by searching using keywords *SSL* and *certificate*.

# **Uploading Certificates**

After you obtain a certificate and key, unzip them if necessary and upload them to the SLK's Flash memory.

*Note:* The files to be uploaded must have suitable extensions. The certificate and key must be in PEM format and the name of the files should be *servercert.crt* and *server-cert.key*.

- 1 Start the web control interface and go to the SLK home page.
- 2 In the menu pane on the left, under **Operation**, click **Flash File System**.
- 3 In the Flash File System page, under **Upload File to Flash**, click **Browse**.

Figure 8-3. Controls for Locating and Uploading Firmware

File to upload:		Browse
	Start Upload	

- 4 Click the first file (certificate or key) you want to upload; then click the **Start Upload** button to upload the file to the SLK's Flash memory. When the upload finishes, repeat this step for the other file (certificate or key) you need to upload.
- 5 After the files have been uploaded, click the **Reboot now** link in the bottom-right corner of the Flash File System page. Reboot disconnects you and logs you out of your current session.
- 6 Log in again to the web control interface.
- 7 From the home page, under **Operation**, click **Flash File System** to confirm that the new certificate has been installed successfully.

*Note:* Uploading corrupted or incorrect files can render your SLK inoperable. If this occurs, contact Lantronix for assistance.

# 9: Defining Custom Send Keys

The Send Keys feature provides pre-programmed "hot" keys for functions that require specific key combinations. The SLK comes pre-configured with an extensive list of the most common key combinations (for example, **Ctrl+Alt+Delete**). If an attached server requires a new key combination, you must create a custom key file. Once you create the file, you select your new keys from **Custom Keys** on the **Send** menu.

# **Custom Key Creation**

To customize send keys values on an SLK, you need to create and upload a file with an extension of .jvcf. You can create the file using a simple text editor such as Windows Notepad. (There is not an existing .jvcf file that can be edited.)

The file name is not important, but it must be saved with the .jvcf file extension. (Please see "Examples" on page 9-2 for appropriate syntax.) Examples of file names are:

custom.jvcf
sendkeys.jvcf

# The flash system only allows one . jvcf file, so this file must include all of the desired custom key sequences.

Once you create the custom key sequence file, you upload it using the Flash File System page in the web interface. (See "Flash File System" on page 4-17.)

Browsers will not recognize the new keyboard macros until the browser has been closed and re-opened (this will re-load the new applet). If the custom keys do not display in the **Custom Keys** option of the **Send** menu after the browser has been re-opened, the new .jvcf file may have a syntax or typographical error. Delete the file (from the Flash File System page), review the .jvcf file, and then reload the file.

# **Custom Key Guidelines**

#### Definitions

- [keylist] indicates beginning of document.
- [newitem] "Itemname" indicates beginning of item description with "Itemname" being the descriptor.
- [end] indicates end of item description.
- [down] indicates depress and hold key commands listed hereafter.
- [up] indicates release key commands listed hereafter.
- [type] indicates depress and release key commands hereafter.

#### **Requirements**

- Each key command has to be separated from the next by a space.
- The hex equivalent of the key command can be used in its place.
- The hex equivalent has to be in the format 0x0041. (See "Potential Send Keys" on page 9-3.)
- Upload the file as you would a firmware upgrade, but you do not need to reset the device.
- When loading the new configuration file, make sure all browsers are closed and a new session is started.

# **Examples**

The following script is an example of creating new keys in a . jvcf file:

```
[keylist]
[newitem] "Ctrl-Alt-Del"
       [down] CONTROL ALT DELETE
       [up] DELETE ALT CONTROL
[end]
[newitem] "Ctrl-Esc"
       [down] CONTROL ESCAPE
       [up] ESCAPE CONTROL
[end]
[newitem] "Alt-Esc"
       [down] ALT ESCAPE
       [up] ESCAPE ALT
```

```
[end]
[newitem] "L+RShift+Alt-Esc"
          [down] LShift RShift ALT ESCAPE
          [up] ESCAPE ALT RShift LShift
[end]
[newitem]"TAB"
          [type] TAB
[end]
[newitem] "Shift-TAB"
          [down] SHIFT TAB
          [up] TAB SHIFT
[end]
[newitem] "Print Screen"
         [type] PRINTSCREEN
[end]
          [newitem] "Print Screen, Print Screen"
          [type] PRINTSCREEN PRINTSCREEN
[end]
[newitem] "Scroll Lock"
          [type] SCROLL_LOCK
[end]
[newitem] "2xScroll Lock"
         [type] SCROLL_LOCK SCROLL_LOCK
[end]
```

# **Potential Send Keys**

The following is a list of potential send keys and the appropriate command or hex values to identify that keystroke in a .jvcf file.

#### **Custom Send Key**

[keylist]	indicates beginning of document
[newitem] "Itemname"	indicates beginning of item description with "Itemname" being the descriptor
[end]	indicates end of item description
[down]	depress and hold key commands listed hereafter
[up]	release key commands listed hereafter
[type]	depress and release key commands hereafter

- each key command has to be separated from the next by a space

- the hex equivalent of the key command can be used in its place

- hex equivalent has to be in the format of eg 0x0041

- once created upload file much like a firmware upgrade but no need to reset device

- make sure all browsers are closed and new session is started to load the new configuration file

				Key	Command	Hex	
Virtual Keyco	des supported by J2R	E		8	8	0038	$\checkmark$
Kev	Command	Hex		9	9	0039	$\checkmark$
Enter	ENTER	0004	✓	;	SEMICOLON	003B	$\checkmark$
Backsnace	BACK SPACE	0008	✓	=	EQUALS	003D	$\checkmark$
Тар		0000	1	а	Α	0041	$\checkmark$
Cancel	CANCEL	0003		b	В	0042	$\checkmark$
Clear	CLEAR	000C		С	С	0043	$\checkmark$
Shft	SHIFT	0010	$\checkmark$	d	D	0044	$\checkmark$
Control	CONTROL	0011	$\checkmark$	е	E	0045	$\checkmark$
Alt	ALT	0012	$\checkmark$	f	F	0046	$\checkmark$
Pause	PAUSE	0013	$\checkmark$	g	G	0047	$\checkmark$
Caps Lock	CAPS LOCK	0014	$\checkmark$	h	Н	0048	$\checkmark$
Escape	ESCAPE	001B	$\checkmark$	I	I	0049	$\checkmark$
Space	SPACE	0020	$\checkmark$	j	J	004A	$\checkmark$
Page up	PAGE UP	0021	$\checkmark$	k	К	004B	$\checkmark$
Page down	PAGE DOWN	0022	$\checkmark$	I	L	004C	$\checkmark$
End	END	0023	$\checkmark$	m	Μ	004D	$\checkmark$
Home	HOME	0024	$\checkmark$	n	Ν	004E	$\checkmark$
Left	LEFT	0025	$\checkmark$	0	0	004F	$\checkmark$
Up	UP	0026	$\checkmark$	р	Р	0050	$\checkmark$
Right	RIGHT	0027	$\checkmark$	q	Q	0051	$\checkmark$
Down	DOWN	0028	$\checkmark$	r	R	0052	$\checkmark$
	COMMA	002C	$\checkmark$	S	S	0053	$\checkmark$
-	MINUS	002D	$\checkmark$	t	Т	0054	$\checkmark$
	PERIOD	002E	$\checkmark$	u	U	0055	$\checkmark$
1	SLASH	002F	$\checkmark$	V	V	0056	$\checkmark$
0	0	0030	$\checkmark$	W	W	0057	$\checkmark$
1	1	0031	$\checkmark$	х	Х	0058	$\checkmark$
2	2	0032	$\checkmark$	У	Y	0059	$\checkmark$
3	3	0033	$\checkmark$	Z	Z	005A	$\checkmark$
4	4	0034	$\checkmark$	(	OPEN_BRACKET	005B	$\checkmark$
5	5	0035	$\checkmark$	١	BACK_SLASH	005C	$\checkmark$
6	6	0036	$\checkmark$	)	CLOSE_BRACKET	005D	$\checkmark$
7	7	0037	$\checkmark$	0 on Num Pad	NUMPAD0	0060	$\checkmark$

Key	Command	Hex
1 on Num Pad	NUMPAD1	0061
2 on Num Pad	NUMPAD2	0062
3 on Num Pad	NUMPAD3	0063
4 on Num Pad	NUMPAD4	0064
5 on Num Pad	NUMPAD5	0065
6 on Num Pad	NUMPAD6	0066
7 on Num Pad	NUMPAD7	0067
8 on Num Pad	NUMPAD8	0068
9 on Num Pad	NUMPAD9	0069
*	MULTIPLY	006A
+	ADD	006B
Separator	SEPARATOR	0060
Subtract	SUBTRACT	0060
Decimal	DECIMAL	006E
Divide		0065
E1	F1	0070
F2	F2	0070
F3	F3	0071
F 4	F4	0072
F5	F5	0073
FJ	FJ	0074
F0 E7	F0 E7	0075
		0070
		0077
F9 E10	F9 E10	0070
		0079
F11 F12	F11 F12	0078
F 12 Delete		0075
Delete Num Look		007
		0090
Sciuli Lock		0091
Printscreen		009A
Heln	HELP	0090
Meta	META	0090
Backquote	BACK QUOTE	00C0
Quote	QUOTE	00DF
Final	FINAL	0018
Convert	CONVERT	001C
Nonconvert	NONCONVERT	001D
Accept	ACCEPT	001E
Modechange	MODECHANGE	001F
Kana	KANA	0015
Kanji	KANJI	0019
Undefined	UNDEFINED	00FF
Dash	DASH	00BD
Dash	DASH2	0000
Semicolon	SEMICOLON2	00BA
Open Bracket2	OPEN_BRACKET2	00DB
Backslash2	BACK_SLASH2	00DC
Close Bracket2	CLOSE_BRACKET2	00DD

Key	Command	Hex	
Equals2	EQUALS2	00BB	$\checkmark$
Comma2	COMMA2	00BC	$\checkmark$
Period2	PERIOD2	00BE	$\checkmark$
Slash2	SLASH2	00BF	$\checkmark$

#### DV6-Specific Hex Equivalents to keys

 $\checkmark \checkmark \checkmark \checkmark \checkmark \checkmark \checkmark \checkmark \checkmark \checkmark \checkmark$ 

√ √

√ √

√

< < < < < < <<</p>

Key	Command	Hex	
Apps/ WinMenu	N/A	F001	$\checkmark$
Power	N/A	F002	$\checkmark$
Sleep	N/A	F003	$\checkmark$
Wake	N/A	F004	$\checkmark$
Left Shift	N/A	FFE1	$\checkmark$
Right Shift	N/A	FFE2	$\checkmark$
Left Control	N/A	FFE3	$\checkmark$
Right Control	N/A	FFE4	$\checkmark$
Left Alt	N/A	FFE5	$\checkmark$
Right Alt	N/A	FFE6	$\checkmark$
Left Windows	N/A	FFE7	$\checkmark$
Right Windows	N/A	FFE8	$\checkmark$
•			

**Defining Custom Send Keys** 

# A: Specifications

# **Hardware Specifications**

#### Ethernet

One 10/100BaseT connection Standard RJ45 connector LEDs for link, 10/100 indicator, and network activity

# **VGA** Input

Max resolution 1280 x 1024 at 75Hz.

Supports most VESA graphics modes and all text modes

DDC2B compatible

# **VGA Local Output**

Copy of input video with OSD (On-Screen Display) for setup

Optional use; no local screen is required after setup

# PS/2 Keyboard / Mouse

Emulates standard PS/2 keyboard and 2-button PS/2 mouse

Keyboard, video and mouse connect directly to server

Keep-alive feature means server is not affected by power failure on the SLK. Server still sees a normal connection for mouse and keyboard.

# Local PS/2 Keyboard/Mouse

Allows local access to the controlled server

Can be disabled or password protected to limit access

Used for initial setup of network address, subnet mask, etc.

Optional once system is deployed

May be connected/removed without affecting server

# Serial Port 1 (RS-232-C)

DB9 Female connector (DCE)

Standard baud rates up to 115,200 bps

Can be used for multiple functions:

Telnet access (console server mode). Provides access to a serial console server (e.g., Lantronix SLC) or serial management port of a connected server.



- Watchdog mode. With appropriate server software, the SLK can detect a string pattern which can trigger an alert or kill the power to reset failed software/hardware.
- Power control. When connected to an optional third-party power control unit, the serial port may be used to control the power to multiple computers.
- Log. Outputs the log from the SLK to a serial port.

# Serial Port 2

SLK1 and SLK8: have an 8-pin mini-DIN that requires the supplied mini-DIN DB9 adapter (DCE).

SLK16: Identical to Serial Port 1.



# Serial Port 3 (SLK16)

DB9 male connector (DTE)

Functions same as Serial Ports 1 and 2

Additional RS-232-C modem function

#### Reset

SLK hardware reset switch

## Power

Auto-sensing power supply

Input Voltage Range: 100 - 240 VAC

Frequency: 50 - 60 Hz

Max. Input Current:1.5A max. (RMS) @ 115VAC

Fused IEC320 mains connector, detachable power cord

Two 2.5A fast-blow fuses and a power cord provided

#### Mechanical

Each SLK is a fully independent system

Dimensions (height x width x depth)

SLK1:	1.75 in x 5.7 in x 16 in (4.45 cm x 14.48 cm x 40.60 cm)
SLK8:	1.75 in x 17 in x 12.5 in (4.45 cm x 43.18 cm x 31.75 cm)
SLK16:	3.5 in x 17 in x 11.25 in (8.89 cm x 43.17 cm x 28.58 cm)

Shipping Weight

SLK1:	6 lbs
SLK8:	11 lbs
SLK16:	13 lbs

Painted aluminum sheet-metal construction

#### Internal

Contains hardware random number generator

Flash-memory-based firmware may be field-upgraded using the web control interface

Dedicated 32-bit micro-processor



# **RJ-45 to DB9M Adapter**



Figure A-1. RJ-45 to DB9M Adapter for Serial Connection of SLP Remote Power Manager
# **Software Specifications**

#### **Network Protocols**

HTTP/1.1 and HTTPS (secure) web server used for control and setup

VNC server (implements RFB 3.3 protocol with Hextile encoding)

Requires one dedicated IP address

TCP/IP port numbers for all services may be changed to confuse attackers

SMTP is used to deliver email notifications

Does not require a DNS server (Domain Name Service), so it will continue to operate during this network failure

#### System Software

Specialized RTOS (Real Time OS)

Proprietary software, with published open-standard based interfaces

#### **System Requirements**

Web browser: Microsoft Internet Explorer 6+ with Java plug-in JRE 1.4.0

Optional VNC viewer supports version 3.3 of RFB protocol

An SMTP server required for email notification feature

Telnet client required for serial port terminal server access

#### **Public Keys/Encryption**

Supports X.509 certificates

True hardware RNG (random number generator) used to create session keys and seed values

128-bit or 56-bit encryption for SSL v2

Supports RC4 and DES algorithms

Compatible with both import and export browsers

### **Special Features**

SLK1 and 8: Up to 10 unique users and passwords SLK16: Up to 32 unique users and passwords

Stealth mode: prevents port scans and other network probes

Turtle mode: disables self when attacked; requires access to local console to re-enable

Idle time-out causes logout from session

Multiple users can connect to same system

Compatible with most existing KVMs

#### Environment

Operating Temperature	SLK1 and SLK8: 0° to 40° C (32° to 104° F) SLK16: 10° to 40° C (50° to 104° F)
Operating Humidity	40-60%
Storage Temperature	SLK1 and SLK8: -40° to 74° C (-40° to 165° F) SLK16: 0° to 60° C (32° to 140° F)
Storage Humidity	35-70%

# **Agency Statements**

#### Notification

**Warning:** changes or modifications to SecureLinx SLK Remote KVMs not expressly approved by Lantronix could void the user's authority to operate the equipment.

**Note:** 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 instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

### **Agency Approvals**

- FCC Part 15, Subpart B, Sec. 15.107(B) and 15.109(B). Equipment Class A.
- EUROPEAN CISPR 22:1997 AND EN 55022:1988. Equipment Class A.
- EUROPEAN CISPR 24:1997/EN 55024:1998.
- CAN/CSA-C22.2 No. 60950.00/UL 60950, Third Edition dated Dec. 01, 2000

# **B: Binary to Hexadecimals**

Some of the procedures require you to assemble a series of options (represented as bits) into a complete command (represented as a byte). The resulting binary value must be converted to a hexadecimal representation. Use this appendix to learn to convert binary values to hexadecimals.

# **Converting Binary to Hexadecimal**

Following are two simple ways to convert binary numbers to hexadecimal notation.

#### **Conversion Table**

Hexadecimal digits have values ranging from 0 to F, which are represented as 0-9, A (for 10), B (for 11), etc. To convert a binary value (for example, 0100 1100) to a hexadecimal representation, treat the upper and lower four bits separately to produce a two-digit hexadecimal number (in this case, 4C). Use the following table to convert values from binary to hexadecimal.

Decimal	Binary	Hex
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	В
12	1100	С
13	1101	D
14	1110	E
15	1111	F

#### Table B-1. Binary to Hex Conversions

### **Scientific Calculator**

Another simple way to convert binary to hexadecimals is to use a scientific calculator, such as the one available on Windows' operating systems. For example:

- 1 On the Windows' Start menu, click **Programs**-->**Accessories**-->**Calculator**.
- 2 On the View menu, select **Scientific**. The scientific calculator displays.
- 3 Click **Bin** (Binary), and type the number you want to convert.

Calculator \_ 🗆 🗵 Edit View Help 1001100 ○ Hex ○ Dec ○ Oct ● Bin Qword ○ Dword ○ Word
O Byte □ Inv 🗌 Нур Backspace CE Ċ 8 F-E MC 7 9 Sta 7 Mod And MR. 5 6 × 0r Ave dms Exp 4 Xor In Sum MS 1 2 Lsh Not sin log M+ 0 +7-Int n! + = В D Е F Dat 1/sA pi tan

Figure B-1. Scientific Calculator with Binary Values

4 Click **Hex**. The hexadecimal value displays.

#### Figure B-2. Scientific Calculator with Hex Value

📕 Calcula	tor	A CONTRACTOR OF	- 🗆 ×
Edit View	Help		
			4C
• Hex	C Dec C Oct C Bin	C Qword C Dword C Word	C Byte

# C: Glossary

This appendix defines the technical terms in this User Guide.

Authentication	The process of identifying an individual, usually based on a user- name and password.
Channel	The path between the SLK unit and the target server being man- aged. The SLK1, SLK8, and SLK16 support one, eight, and 16 channels, respectively.
Compression	Storing data in a format that requires less space than usual.
Cookie	A message given to a web browser by a web server. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly pre- pare customized web pages for them.
Data Terminal Equipment (DTE)	A device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232-C standard.
Debug	To find and remove errors (bugs).
Default gateway	The gateway in a network that a computer uses to access another network.
Home page	The main page of the SLK web control interface. The home page serves as the starting location for managing the SLK.
HTTPS	HTTPS (HTTP Secure Socket Layer) uses a default port number of 443 (80 for HTTP) and automatically performs SSL negotiation that sends data in encrypted form (that is, web servers accessed through HTTPS have to be "secure web servers").
IP address	An identifier for a computer or device on a TCP/IP network. Net- works using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255. For example, 216.254.154.11.
KVM switch	Short for keyboard, video, mouse switch: a hardware device that allows a single keyboard, video monitor, and mouse to control more than one computer one at a time.
Local port	A port on the back of the SLK that accepts a single keyboard, video monitor, and mouse from a local computer that will be used to manage the target servers.
Master account password	The password you enter to perform administrative activities using the web control interface.

Modem init string	A series (string) of commands sent by modem software to initialize the modem. These commands configure the modem's options for parameters such as error correction, data compression, and flow control. Init strings are fairly specific to each modem. Not all pro- grams use init strings. Some use settings files such as Windows . inf files.
Point-to-Point Protocol (PPP)	A data link protocol that provides dialup access over serial lines by encapsulating protocols in specialized packets. These packets can be used to replace a failed network connection and allow remote users to log onto the network as if they were in-house.
On Screen Display (OSD)	An alphanumeric, character-based interface for configuring SLK units. The OSD provides minimal prompting and guidance.
RJ45	Short for Registered Jack 45, an 8-wire connector used commonly to connect computers onto Local Area Networks (LANs). RJ45 con- nectors are wider and have more pins than the ubiquitous RJ11 connectors used for connecting telephone equipment.
Secure Sockets Layer (SSL)	A protocol for transmitting private documents over the Internet. SSL works by using a private key to encrypt data that has been transferred over the SSL connection.
VNC/OSD Hotkeys	A customized set of preprogrammed escape sequences.
SNMP	Short for Simple Network Management Protocol, a set of protocols for managing complex networks. SNMP works by sending mes- sages, called protocol data units (PDUs), to different parts of a net- work. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.
Stealth mode	An operating mode that disables the SLK to prevent unauthorized access.
Subnet	Part of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 216.254.154 are part of the same subnet. Dividing a network into subnets is useful for security and performance. IP networks are divided using a subnet mask.
Turtle mode	An operating mode that disables the SLK when attacked.
Virtual Network Computing (VNC)	VNC is remote-control software that lets you view and interact with one computer using a simple program on another computer any- where on the Internet. VNC is freely and publicly available.
Web control interface	A graphical interface for configuring SLK units. The web control interface is browser based and lets you perform configuration activities by pointing and clicking your mouse.

# Warranty

Lantronix warrants each Lantronix product to be free from defects in material and workmanship for a period of TWO YEARS. During this period, if a customer is unable to resolve a product problem with Lantronix Technical Support, a Return Material Authorization (RMA) will be issued. Following receipt of a RMA number, the customer shall return the product to Lantronix, freight prepaid. Upon verification of warranty, Lantronix will -- at its option -- repair or replace the product and return it to the customer freight prepaid. If the product is not under warranty, the customer may have Lantronix repair the unit on a fee basis or return it. No services are handled at the customer's site under this warranty. This warranty is voided if the customer uses the product in an unauthorized or improper way, or in an environment for which it was not designed.

Lantronix warrants the media containing its software product to be free from defects and warrants that the software will operate substantially according to Lantronix specifications for a period of 60 DAYS after the date of shipment. The customer will ship defective media to Lantronix. Lantronix will ship the replacement media to the customer.

In no event will Lantronix be responsible to the user in contract, in tort (including negligence), strict liability or otherwise for any special, indirect, incidental or consequential damage or loss of equipment, plant or power system, cost of capital, loss of profits or revenues, cost of replacement power, additional expenses in the use of existing software, hardware, equipment or facilities, or claims against the user by its employees or customers resulting from the use of the information, recommendations, descriptions and safety notations supplied by Lantronix. Lantronix liability is limited (at its election) to:

- Refund of buyer's purchase price for such affected products (without interest).
- Repair or replacement of such products, provided that the buyer follows the above procedures.

There are no understandings, agreements, representations or warranties, expressed or implied, including warranties of merchantability or fitness for a particular purpose, other than those specifically set out above or by any existing contract between the parties. Any such contract states the entire obligation of Lantronix. The contents of this document shall not become part of or modify any prior or existing agreement, commitment or relationship.

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

# Index

## Α

Accessing servers with a VNC viewer 6-1 Adjusting mouse 3-11 Agency approvals A-6 statements A-6

#### В

Benefits 2-3 Browse menu tree 4-46

## С

Capture settings 4-49 Components, unpacking 3-1 Configuration activities On Screen Display interface 5-1 VNC viewer 6-1 Web control interface 4-19 Configurations 2-4 connecting to different switches 2-5 connecting to the same network and switch as the server 2-4 using multiple servers 2-5 Connecting devices 3-13 KVM switches 3-16 local console 3-13 monitors, keyboards, and mice 3-13 serial devices 3-16 to a power source 3-16 to the network 3-16 Controlling hosts 4-9 Copyright information, Web control interface 4-50

### D

Date settings 4-41 Debug 4-18 Devices, connecting to the SLK 3-13

# Е

Encryption 8-3 Event log 4-16

### F

Features 2-3 Firmware upload instructions 8-1 Flash file system uploading certificate 5-13, 8-4 uploading firmware 8-2 uploading key 5-13, 8-4 Web control interface 4-17 Full menu tree 4-45

# G

General troubleshooting 7-2

# Н

Hardware description 3-3 SLK1 3-3 SLK16 3-7 SLK8 3-4 Hardware specifications A-1 Hosts controlling 4-9 viewing 4-12

### I

Information activities, Web control interface 4-44 Installation connecting a local console 3-13 connecting devices 3-13 connecting KVM switches 3-16 connecting monitors, keyboards, and mice 3-13 connecting serial devices 3-16 connecting to a power source 3-16 connecting to the network 3-16 overview 3-10 preparing target servers 3-10 rack-mounting 3-10 verifying target servers 3-18 Items supplied by user 3-2

## Κ

Keyboard troubleshooting 7-4 KVM switches, connecting to SLK 3-16

# L

Local console connecting to SLK 3-13 On Screen Display interface 5-1 security 4-33 verifying target servers 3-18 VNC Configuration screen 6-2 Local user control On Screen Display interface 5-18 Web control interface 4-39 Logging into the On Screen Display interface 5-2

#### Μ

Master account password 4-23 Models 2-2 Monitoring your configuration 4-35 Mouse adjustments 3-11 Mouse troubleshooting 7-5 Multiple server configurations 2-5

### Ν

Navigating through the On Screen Display interface 5-3 Network configuration, Web control interface 4-19 Network connection 3-16

# 0

On Screen Display interface Channel Switch menu 5-4 configuring serial ports 5-16

local user control 5-18 logging in 5-2 Monitoring Settings menu 5-8 navigating through 5-3 Network Configuration menu 5-5 Network Management Settings menu 5-11 overview 5-1 PPP options 5-7 security 5-13 Setup menu 5-5 SNMP 5-11 Syslog 5-12 user administration 5-15 Virtual Network Computing 5-20 Operation activities, Web control interface 4-8 Optimizing video 3-11

#### Ρ

Power control Web control interface 4-13 Power source connection 3-16 PPP On Screen Display interface 5-7 Web control interface 4-21 Preparing target servers 3-10

# Q

Quick Start instructions 1-1

# R

Rack-mounting 3-10 redefining 9-1

# S

Security 8-3 On Screen Display interface 5-13 Web control interface 4-29 Serial devices, connecting to SLK 3-16 Serial ports

On Screen Display interface 5-16 Web control interface 4-37 Servers accessed with a VNC viewer 6-1 accessed with the On Screen Display interface 5-4 accessed with the Web control interface 4-9 Setting the date and time 4-41 SLK components 3-1 configurations 2-4 features and benefits 2-3 hardware description 3-3 installation 3-10 models 2-2 quick start 1-1 rack-mounting 3-10 SLK1 hardware description 3-3 SLK16 hardware description 3-7 SLK8 hardware description 3-4 SNMP On Screen Display interface 5-11 Web control interface 4-43 Software specifications A-5 Specifications hardware A-1 software A-5 Starting a Web control interface session 4-2 Syslog On Screen Display interface 5-12 Web control interface 4-41

# T

Target servers mouse adjustments 3-11 optimizing the system 3-10 optimizing video 3-11 preparing 3-10 verifying 3-18 Time settings 4-41 Troubleshooting general 7-2 keyboard 7-4 mouse 7-5 video 7-8

### U

Unpacking components 3-1 Uploading firmware 8-1 User accounts 4-23 User activity functions 4-14 User administration, On Screen Display interface 5-15 User-supplied items 3-2

### V

Verifying target servers 3-18 Version 4-48 Video troubleshooting 7-8 Video, optimizing 3-11 View connections 4-47 Virtual Network Computing On Screen Display 5-20 VNC Web control interface 4-39 VNC viewer accessing target servers 6-1 overview 6-1 VNC/OSD Hotkeys 9-1

# W

Web control interface browse menu tree 4-46 capture settings 4-49 components 4-4 configuration activities 4-19 configuring serial ports 4-37 controlling hosts 4-9 copyright information 4-50 date and time 4-41 Debug 4-18 event log 4-16 flash file system 4-17 full menu tree 4-45 information activities 4-44 local user control 4-39 master account password 4-23 monitoring your configuration 4-35 network configuration 4-19 operation activities 4-8

overview 4-1 power control 4-13 PPP 4-21 security 4-29 SNMP 4-43 starting a session 4-2 Syslog 4-41 user accounts 4-23 user activity functions 4-14 version 4-48 view connections 4-47 viewing hosts 4-12 VNC settings 4-39 Index