MSS Installation Guide

For MSS4 Device Servers

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

Ethernet is a trademark of XEROX Corporation. UNIX is a registered trademark of The Open Group. Windows 95, Windows 98, Windows 2000, and Windows NT are trademarks of Microsoft Corporation.

The revision date for this manual is **30 January, 2001**.

Part Number: 900-224

WARNING

This product has been designed to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause harmful interference to radio communications.

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.

Cet appareil doit se soumettre avec la section 15 des statuts et règlements de FCC. Le fonctionnement est subjecté aux conditions suivantes:

(1) Cet appareil ne doit pas causer une interférence malfaisante.

(2) Cet appareil doît accepter n'importé quelle interférence reìue qui peut causer une opération indésirable.

Contents

1: Introduction

The Lantronix MSS family of Device Servers allows you to network-enable a variety of serial devices that were not originally designed to be networked: personal computers, terminals, modems, industrial machinery, and more. This capability brings the advantages of remote management and data accessibility to thousands of serial devices.

The MSS4 offers a solution for almost every networking need. All MSS4 models provide four serial ports, which are capable of RS-232, RS-422, and RS-485 communications, and a 10/100BASE-T Ethernet port. In addition, certain models of the MSS4 include a 100BASE-FX fiber link Ethernet port and two PC card slots. The slots can be used for 802.11 wireless Ethernet, flash storage, and modem cards.

Note: *For a current list of supported PC card technologies, please check the Lantronix Web site, www.lantronix.com.*

Parts of this manual assume knowledge of the IEEE 802.11 Standard governing wireless networking. If you are not familiar with wireless networking concepts and implementation, please refer to the Standard or the documentation that came with your wireless PC card.

Throughout this manual, the MSS4 may be referred to as the **MSS** or as the **Server**.

1.1 Model Overview

There are four MSS4 models, designated as -D, -S, -DFP, and -SFP. The models are differentiated by whether or not they have a DB9 serial connector, screw terminal blocks, PC card slots, and fiber link Ethernet.

Table 1-1: MSS4 Models At-A-Glance

Feature	MSS4-D	MSS4-S	MSS4-DFP	MSS4-SFP
DB9 Serial Ports	4	0	4	0
Screw Terminal Ports	0	4	0	4
PC Card Slots	0	0	2	2
Fiber Link Ethernet (100BASE-FX)	No	No	Yes	Yes

1.2 MSS Features

- TCP/IP and UNIX Compatibility

  The MSS supports a variety of TCP/IP features, including Telnet, Rlogin, UDP, DNS, SNMP, WINS, FTP, DHCP, BOOTP, RARP, and HTTP.

- Connectivity

  The MSS can connect serial devices directly to a 10/100BASE-T or 100BASE-FX wired Ethernet network or an 802.11 wireless Ethernet network.

- Ease of Use

  The MSS4 has a simple but powerful command interface for both users and system managers. The MSS Local mode supports command line editing and command line recall. An extensive **Help** facility is included.

  The EZWebCon utility (provided on the CD-ROM) allows you to configure the MSS from any host machine running the Java Virtual Machine (JVM). It also allows remote host logins into the MSS, which are similar to Telnet logins.

  The Lantronix ThinWeb Manager, a set of HTML pages stored on the MSS, allows you to configure server information via a JavaScript-enabled web browser. For more information, see *Web Browser Login and Configuration* on page 3-6.

- Remote Configuration

  The MSS can be logged into and remotely configured via a network login, a Telnet login to the remote console port, EZWebCon, or a web browser connection to the MSS’s internal HTTP server.

- Context-Sensitive Help

  Context-sensitive on-line help is available at any time. You may type **Help** by itself for overall help, **Help <command>** for help on a specific command, or a partial command line followed by a question mark for help on what is appropriate at that particular point.

Note: *See the MSS Reference Manual for more information.*

- Reloadable Operating Software

  The MSS stores its operating code in Flash ROM, which means that it does not have to download code at boot time. If necessary, you can upgrade the MSS’s operating code to support additional features as newer code becomes available. Also, you can configure the MSS to request a downloaded configuration file at boot time.

- Security

  The MSS includes several configurable security features:

  - Automatic session logouts when a port is disconnected or a device is turned off.
  - Password protection for privileges, ports, services, maintenance commands, and the remote console.
  - An IP security table, which allows the MSS manager to restrict incoming and outgoing TCP/IP connections to certain ports and hosts. This allows managers to restrict MSS access to a particular local network segment or host.

- Diagnostics

  Power-up and interactive diagnostics help system managers troubleshoot network and serial line problems.

- SDK Support

  The MSS supports the Lantronix Software Developer Kit (SDK), which allows users to customize the MSS and add functionality. For more information about the SDK, please contact Lantronix directly.

Note: *The SDK does not allow users to configure custom PC card support.*

1.3 TCP/IP Support

The MSS supports the TCP/IP network protocol. A network protocol is a method of communicating over Ethernet. The protocol specifies a certain arrangement of data in the Ethernet packets, and provides different services for its users.

TCP/IP support includes Telnet, Rlogin, UDP, DNS, and WINS. The Telnet terminal protocol is an easy-to-use interface that creates terminal connections to any network host supporting Telnet. Rlogin is a protocol that allows users to initiate a TCP/IP login session. UDP (User Datagram Protocol) is a connectionless protocol that results in smaller packet headers, no session overhead, and the ability to send to multiple hosts. The MSS also supports the use of Domain Name Servers (DNS), allowing a network nameserver to translate text node names into numeric IP addresses. For WINS support, the MSS can be configured to announce itself as a WINS node.

The MSS also implements basic Simple Network Management Protocol (SNMP) functionality. SNMP commands enable users, usually system administrators, to get information from and control other nodes on a local area network (LAN), and respond to queries from other network hosts. The MSS allows configuration of one community name with read/write access. Instructions for SNMP configuration are available in the *SNMP* section of this guide, page 4-5.

1.4 Terms

The following terms are used throughout this manual.

Host	A computer attached to the network. The term host is generally used to denote interactive computers, or computers that people can log into.
Local Mode	The MSS user interface. It is used to issue configuration and session management commands and to establish connections. When in Local mode, users will see a **Local>** prompt.
Node	Any intelligent device directly connected to the Ethernet network such as a host, a printer, or a terminal server. All nodes have their own Ethernet addresses. The MSS is a node. Devices connected to the MSS are not nodes.
Server/server	Server, when capitalized, refers to your Lantronix MSS server product. When not capitalized, it refers to a generic network server machine.
Session	A logical connection to a service. A typical session is a terminal connected to a host through the server.

1.5 About The Manual

The rest of this documentation is divided into chapters as follows:

- Chapter 2, *Installation*, explains the MSS connectors and the installation process.
- Chapter 3, *Getting Started*, contains configuration information to get the unit up and running. Read this chapter in its entirety, and be sure to configure the required items.
- Chapter 4, *Configuration*, contains additional configuration information.
- Chapter 5, *Using the MSS*, contains information about how the MSS can be used in different applications. Read this chapter to get the most out of using your MSS.
- Appendices include *Contact Information*, *Troubleshooting*, *Pinouts*, *Updating Software*, and *Specifications*. Read them as necessary.
- The comprehensive *Index* can be used to find specific information.

The *MSS Reference Manual*, located on the CD-ROM in PDF format, provides the full MSS family command set.

2: Installation

This chapter covers the physical installation of the MSS in a wired or wireless Ethernet network. If you are installing the MSS for the first time, you must either attach a terminal to one of the serial ports or connect the MSS to a wired Ethernet network so you can configure the proper 802.11 settings for wireless networking.

In addition, this chapter explains:

- The components of all MSS4 models, including front panel, back panel, and LEDs (see *MSS4 Components* on page 2-1).
- How to install the MSS4 in a wired networking environment (see *Installing in a Wired Network* on page 2-5).
- How to install an 802.11 card in the MSS4 for use in a wireless networking environment (see *Installing an 802.11 Card* on page 2-7).
- How to install an ATA Flash card (*Installing an ATA Flash Card* on page 2-8).
- How to install a modem card (*Installing a Modem Card* on page 2-9).

Basic knowledge of networking installation is assumed. Read this chapter completely before continuing.

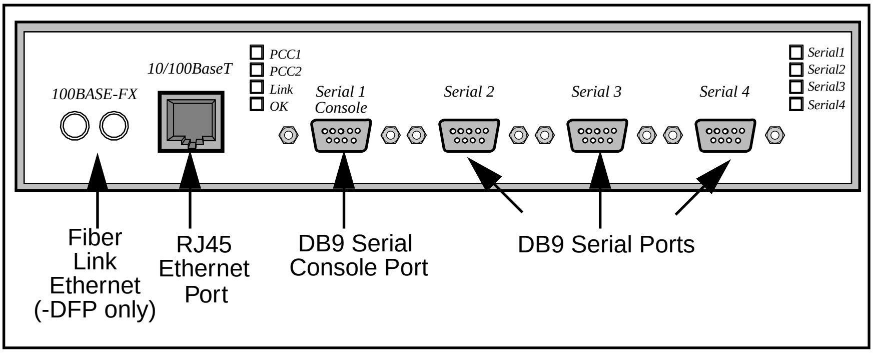
2.1 MSS4 Components

There are currently four different models of the MSS4. The following sections will discuss the specific components for each model. The LEDs are identical across all models.

2.1.1 MSS4-D/DFP Front Panel

The MSS4-D and MSS4-DFP front panels have four DB9 serial port connectors and an RJ45 Ethernet connector. The MSS4-DFP also has a 100BASE-FX fiber link Ethernet connector.

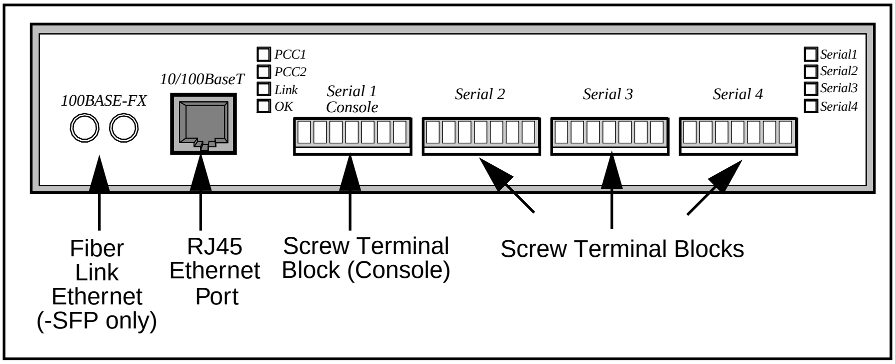
Figure 2-1: MSS4-D/DFP Front Panel



2.1.2 MSS4-S/SFP Front Panel

The MSS4-S and MSS4-SFP front panels have four screw terminal blocks and an RJ45 Ethernet connector. The MSS4-SFP also has a 100BASE-FX fiber link Ethernet connector.

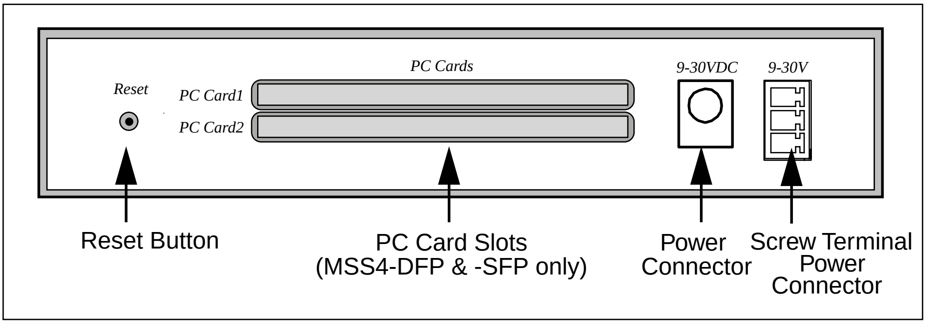
Figure 2-2: MSS4-S/SFP Front Panel



2.1.3 MSS4 Side Panel

All models include a reset button, and two power connectors. The MSS4-DFP and -SFP side panels also have two PC card slots. The following figure shows an MSS side panel.

Figure 2-3: MSS Side Panel



2.1.4 MSS4 LEDs

LEDs are located on the front panel of the unit. All MSS4 units have four LEDs that indicate serial activity for each serial port and two status LEDs. PC card models include two additional LEDs for slot status. The PC Card LEDs have different meanings depending on what type of PC card is currently in use.

Note: *On MSS models that do not have PC card slots, the PC Card LEDs will never light up.*

The following tables explains the function of the LEDs.

Table 2-1: MSS4 LEDs

LED	Function
Serial (1-4)	Blinks green to indicate MSS serial activity.
OK	Blinks yellow, green, or red to indicate MSS activity.
Link	Glows green or yellow to indicate a wired Ethernet connection. Off: Not connected to a wired Ethernet network Green: Connected to a 10BASE-T network Yellow: Connected to either a 100BASE-T or 100BASE-FX network

The PCC1 and PCC2 LEDs, which correspond to the top and bottom PC card slot respectively, vary in meaning depending on what kind of card is currently installed.

Table 2-2: PCC1 and PCC2 LEDs

LED State	802.11 Cards	ATA Cards	Modem cards
Off	No card inserted	No card inserted	No card inserted
Green Solid	802.11 link established, PC card ready for use	PC card ready for use	PC card ready for use
Green Blinking	Negotiating settings with AP or ad-hoc peer	PC card is not properly formatted	n/a
Red Solid	PC card hardware failure	PC card hardware failure	PC card hardware failure
Red Blinking	PC card not read or supported	PC card not read or supported	PC card not read or supported
Yellow Solid	PC card identified, initialization in progress	PC card identified, initialization in progress	PC card identified, initialization in progress
Yellow Blinking	Scanning for Access Point (AP) or ad-hoc peer	n/a	Card identified, initialization problem

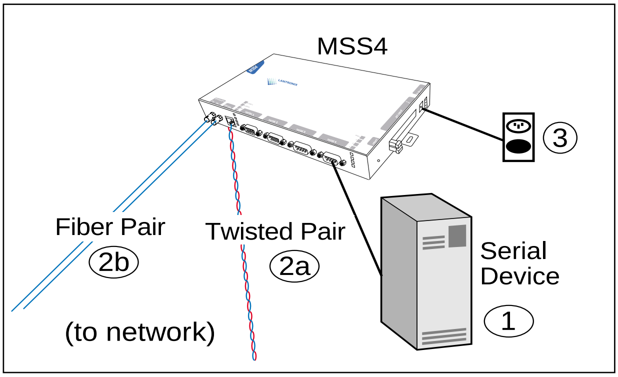
Note: *Although a red LED during boot mode usually signals an error, red LED patterns are part of the normal operation of the MSS and are not necessarily indicative of errors or dangerous operation.*

2.2 Installing in a Wired Network

The MSS should be positioned close to the device it will be servicing. Since powering down the unit will terminate any active sessions, it may be desirable to place the server in a location secure from user access. Also be aware of the unit's environmental operating limits and cabling requirements. See *Appendix C* and *Appendix E* for details.

The following diagram shows a properly-installed MSS in a wired Ethernet network. The numbers in the diagram refer to the installation steps in this section.

Figure 2-4: MSS Connected to Serial Device and Network



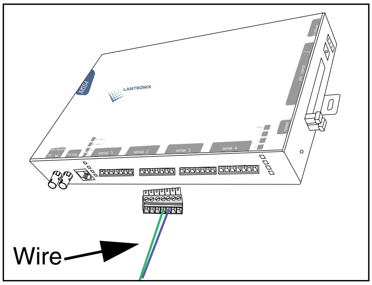
1 Connect the MSS to a serial device. Note that all serial ports are initially configured for RS-232 networking.

A Connect one end of a serial cable to either one of the MSS DB9 connectors or screw terminal blocks (depending on the model). See *Appendix C* for MSS connector pinout information.

Note: *For the first connection, you may want to connect a serial terminal to the console port, designated as the first serial port. This will allow you to verify that your server is working and to configure the necessary network settings. The console port is initially set for 9600 baud, 8 data bits, one stop bit, and no parity.*

When using a screw terminal block, you may have to connect from 2 to 6 wires depending upon the desired MSS usage mode. Do not over-tighten the screws, but make sure the wire is secure in the block.

Figure 2-5: Connecting Wire to Screw Terminal Blocks



B Connect the other end of the cable to your serial device's serial port.

2 Connect the MSS to the network via **one** of the following methods.

❍ Connect one end of a twisted-pair 10/100BASE-T cable to the Ethernet network. Connect the other end of the cable to the RJ45 Ethernet port on the front of the MSS.

❍ Connect one end of a fiber optic cable to the Ethernet network. Connect the other end of the cable to the fiber link ports (ST-style connector) on the front of the MSS.

3 Supply power to the MSS. This can be done through either the MSS power jack or the screw terminal power connector. Do not supply power to both the power jack and the screw terminal at the same time.

A Connect one end of a power connector to the MSS via **one** of the following.

➜ Connect the barrel jack end of the power cable to the MSS power jack.

➜ Connect power to the 9-30V screw terminal power connector and to ground and chassis ground.

B Supply power to the MSS by connecting the power cube end of the power cable to a standard wall outlet.

When the MSS receives power, it will begin a three-step boot process.

❍ The MSS runs through a set of power-up diagnostics for approximately five seconds. The **OK** and **Serial** LEDs should show varying patterns corresponding to the test being run.

Note: *If there is a valid connection to a wired Ethernet network, the Link LED should remain solid green or yellow once the unit has completed booting.*

❍ The MSS tries to obtain TCP/IP configuration information via DHCP, BOOTP, and/or RARP. This procedure takes approximately 40 seconds if no hosts answer the request, and boot messages will be sent to the console port. The **OK** LED will blink green approximately three times per second, and occasionally yellow as packets are sent and received.

Note: *For more information on BOOTP, RARP, or DHCP, refer to your operating system's documentation.*

❍ The MSS determines if the code in the Flash ROMs is valid. If so, it loads the code and begins normal execution. This step takes approximately five seconds.

Once the MSS is running normally, the **Link** LED should be solidly lit to indicate a functioning wired Ethernet connection and the **OK** LED should blink once every two seconds.

4 Supply power to the attached serial device(s), if necessary.

5 Ensure the MSS is working. There are a couple ways to check:

❍ Wait for approximately 30 seconds after powering the unit up. If the **Link** LED is solidly lit and the **OK** LED blinks green once every two seconds, the MSS is operating normally.

❍ If you have connected a serial terminal to the console port, press the **Return** key. You should see several lines of start-up messages followed by a **Local>** prompt.

2.3 Installing PC Cards

The following sections explain how to install different kinds of cards in the MSS PC card slots. Not all PC card types or brands are supported. Check the Lantronix web site for a complete list of currently supported technologies.

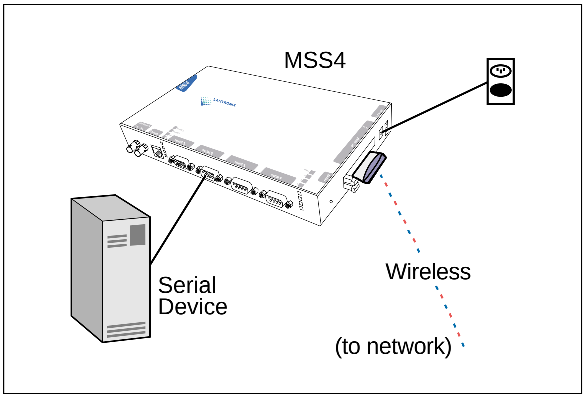
2.3.1 Installing an 802.11 Card

Although 802.11 networking is enabled by default, you may need to configure other 802.11 settings before the wireless card will work properly. To view your current 802.11 configuration, enter the **Show 80211** command. This command may also be useful if you experience any problems with your wireless network. See *802.11 Configuration* on page 4-16 for more details.

Note: *You cannot have more than one 802.11 card installed in the MSS at one time.*

The following diagram shows a properly-installed MSS in a wireless Ethernet network. Be sure to read your PC card manual for specific placement and distance requirements.

Figure 2-6: MSS Connected to Serial Device and Wireless Network



Follow these steps to properly install an 802.11 card.

1. Power off the MSS by removing the plug from the outlet.
2. Insert a supported 802.11 card into one of the PC card slots.
3. Power up the MSS by plugging the power supply back in the outlet.

   The MSS should begin its normal boot process. Once the process is complete, one of the **PC Card** LEDs should remain lit as long as there is an 802.11 card inserted in the corresponding PC card slot.

   ❍ When the PC card LED corresponding to the installed card is solid green, the MSS is ready for use.

   ❍ If your PC card LED is any other color, refer to Table 2-1 on page 2-3 for information on what that color means.

2.3.2 Installing an ATA Flash Card

Follow these steps to properly install supported ATA flash and disk storage cards.

1. Power off the MSS by removing the plug from the outlet.
2. Insert a supported ATA Flash card into one of the PC card slots.
3. If desired, insert another supported ATA Flash card into the other PC card slot.
4. Power up the MSS by plugging the power supply back in the outlet.

   The MSS should boot up normally.

- ❍ If a PC card LED is a solid green, the ATA card in the corresponding slot is ready for use.
- ❍ If a PC card LED blinks green, the ATA card in the corresponding slot must be formatted before it can be used. Proceed to *Formatting an ATA Flash Card* on page 4-22 for details.
- ❍ If a PC card LED is any other color, refer to Table 2-1 on page 2-3 for information on what that color means.

2.3.3 Installing a Modem Card

An installed modem card will appear as an additional serial port on the MSS. If only one card is installed, the card will appear as Port 5 regardless of which slot it is in. If two cards are installed, the card installed in the top slot (slot 1) will appear as Port 5 and the card in the bottom slot (slot 2) will appear as Port 6.

If you are an SDK user, you can access the port by using device “tt4” for port 5 or “tt5” for port 6.

Follow these steps to properly install supported modem cards.

1. Power off the MSS by removing the plug from the outlet..
2. Insert a supported modem card into one of the PC card slots.
3. If desired, insert another supported modem card into the other PC card slot.
4. Power up the MSS by plugging the power supply back in the outlet.

   The MSS should boot up normally.

For instructions on how to use the modem card, see *Modem Cards* on page 4-22.

3: Getting Started

This chapter covers all of the steps needed to get the MSS on-line and working. There are three basic methods you can use to log into the MSS and begin configuration:

- Incoming (Remote) Logins: EZWebCon is the preferred method for initial MSS configuration. Users can also use the MSS's internal HTTP server via a standard web browser. After the initial configuration, the MSS can be accessed remotely across TCP/IP networks through Telnet connections. Incoming connections also include network socket port connections (ports 2001-2004 and 3001-3004).

- Serial Port Logins: Users can connect a terminal directly to one of the serial ports, log in, and use the command line interface to configure the unit.

- Remote Console Logins: TCP/IP users can make a Telnet connection to the remote console port (port 7000).

Consider the following points before you log in and configure the MSS:

- Most configuration commands require privileged user status. Connecting a terminal to a serial port or logging into the remote console port does not automatically create privileged user status—you must enter the **Set Privileged** command to become the privileged user (see *Privileged Password* on page 3-2).

- The MSS IP address must be configured before any TCP/IP functionality is available (see *IP Address Configuration* on page 3-3).

- Only one person at a time may be logged into the remote console port (port 7000). This eliminates the possibility of several people simultaneously attempting to configure the MSS.

- Although passwords can be required, remote console logins cannot be disabled. This ensures that the system manager will always be able to access the unit.

3.1 System Passwords

The MSS has both a privileged password and a login password. These passwords have default settings and are discussed in the following sections.

Note: *Default passwords pose a security risk and should be changed as soon as possible. This is especially true of the privileged password.*

3.1.1 Privileged Password

Only the privileged user can change server or port settings. To become the privileged user, enter the **Set Privileged** command, followed by the privileged password. The default privileged password is **system**.

Figure 3-1: Set Privileged Command

```
Local> SET PRIVILEGED
Password> system (not echoed)
```

If another user is currently the privileged user for the MSS, use the **Set Privileged Override** command to forcibly become the privileged user. To relinquish privileged status, enter the **Set Noprivileged** command.

The privileged password can be changed with the **Change Privpass** command. Specify a new password of up to six alphanumeric characters. Note that only the privileged user can change the privileged password.

Figure 3-2: Changing Privileged Password

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> CHANGE SERVER PRIVPASS “walrus”
```

3.1.2 Login Passwords

Login passwords for all connections except remote console logins (port 7000) are disabled by default. The login password is always required for remote console logins. The default login password for all connections is **access**.

To specify a new login password, use the **Change Server Loginpass** command. You will be prompted to enter a new password of up to six alphabetic characters. Note that you must be the privileged user (i.e. you must enter the **Set Privileged** command) to change the login password.

Figure 3-3: Changing the Login Password

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> CHANGE SERVER LOGINPASS “badger”
```

3.1.2.1 Serial Port Logins

To require a password for any connections to the MSS from its serial ports, enable password protection with the **Change Password Protect Enabled** command. The command allows you to specify the serial ports for which you want to provide password protection.

Figure 3-4: Enabling Password Protection for Serial Port Logins

```
Local>> CHANGE PORT 1-4 PASSWORD PROTECT ENABLED
```

3.1.2.2 Telnet and Rlogin Connections

To require a password for Telnet and Rlogin connections, enter the **Change Server Incoming Password** command.

Figure 3-5: Enabling Password Protection for Telnet/Rlogin Connections

```
Local>> CHANGE SERVER INCOMING PASSWORD
```

3.1.2.3 Network Socket Connections

To enable the login password for network socket connections, enter the **Change Password Incoming Enabled** command. The command allows you to specify the serial ports for which you want to provide password proection.

Figure 3-6: Enabling Password Protection for Network Socket Connections

```
Local>> CHANGE PORT 2 PASSWORD INCOMING ENABLED
```

3.2 IP Address Configuration

Note: *When you set an IP address, you may also need to change the subnet mask from the default subnet configuration. See Subnet Mask on page 4-2 for more information.*

3.2.1 Using EZWebCon

Note: *If your version of EZWebCon is earlier than v.2.0, refer to the Readme that was included with it.*

Use the following steps to assign an IP address using EZWebCon.

1. Start EZWebCon. Instructions for installing, running, and using EZWebCon can be found on the distribution CD-ROM.

2. From the **Action** menu, select **Assign IP Address**.

3 Enter or change the IP-related settings:

- **A** For **Ethernet Address**, enter the number that appears on the bottom label of your MSS.
- **B** For **IP Address**, enter the desired IP address to use for this MSS.
- **C** For **Subnet Mask**, change the values provided only if you wish to use a mask other than the default. The default value should be correct in most cases.
- **D** For **Loadhost**, enter the IP address of the loadhost where you intend to store your operating code and SDK files (if used).

4 Click **OK**.

5 Reboot the MSS. EZWebCon will let you know whether the configuration was successful.

3.2.2 Using ARP and Ping

The ARP/ping method is available under UNIX and Windows. If the MSS has no IP address, it will set its address from the first directed IP packet it receives.

On a **UNIX** host, create an entry in the host's ARP table and substitute the intended IP address and the hardware address of the server, then ping the server (see Figure 3-7). This process typically requires superuser privileges.

Figure 3-7: Entering ARP and Ping (UNIX)

```
# arp -s 192.0.1.228 00:80:a3:xx:xx:xx
% ping 192.0.1.228
```

On a **Windows** host, type **ARP -A** at the DOS command prompt to verify that there is at least one entry in the ARP table. If there is no other entry beside the local machine, ping another IP machine on your network to build the ARP table. This has to be a host other than the machine on which you're working.

Use the following commands to ARP the IP address to the MSS and make the MSS acknowledge the IP assignment.

Figure 3-8: Entering ARP and Ping (Windows)

```
C:\ ARP -S 192.0.1.228 00-80-A3-XX-XX-XX
C:\ PING 192.0.1.228
```

Note: *There should be replies from the IP address if the ARP command worked.*

When the MSS receives the ping packet, it will notice that its IP address is not set and will send out broadcasts to see if another node is using the specified address. If no duplicate is found, the server will use the IP address and will respond to the ping packet.

The MSS will not save the learned IP address permanently. This procedure is intended as a temporary measure to enable EZWebCon to communicate with the server, allow configuration with a web browser, or allow an administrator to Telnet into the MSS. Once logged in, the administrator can enter the **Change IPaddress** command to make the address permanent.

Figure 3-9: Changing the IP Address

```
% telnet 192.0.1.228

Trying 192.0.1.228

Lantronix Version n.n/n (yymmdd)
Type Help at the ‘Local_>’ prompt for assistance.

Username> gopher
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> CHANGE SERVER IPADDRESS 192.0.1.228
```

3.2.3 Using a DHCP, BOOTP, or RARP Reply

A host-based DHCP, BOOTP, or RARP server can provide information for the MSS to use to configure an IP address when the unit boots. See the host-based documentation pages for configuration information. Keep in mind that many BOOTP daemons will not reply to a BOOTP request if the download file name in the configuration file does not exist. If this is the case, create a file in the download path to get the BOOTP daemon to respond.

BOOTP and RARP are enabled by default on the MSS. If you wish to disable them, use the **Change BOOTP Disabled** and **Change RARP Disabled** commands. To enable DHCP, use the **Change DHCP Enabled** command.

3.2.4 Using the Serial Console

Connect a terminal to the serial console port and press the **Return** key. If the MSS is functioning normally, you will see the **Local>** prompt. Become the privileged user and enter the **Change IPaddress** command.

Figure 3-10: Entering the IP Address at the Local Prompt

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> CHANGE SERVER IPADDRESS 192.0.1.228
```

If the MSS encounters an Ethernet network problem while booting it will send an alert message to the console and wait ten seconds to detect serial port activity before attempting to finish booting. If you press the Return key when the error message is displayed, you will access the Boot> prompt.

If the MSS fails to properly download code and displays a “will try again” message, you can access the Boot> prompt by pressing the Return key. You can then enter the **Change Server IPaddress** command at the Boot> prompt to set the unit’s IP address.

> **Note:** *For more information on Boot Configuration Program (BCP) commands, see the Troubleshooting appendix.*

3.3 Incoming Logins

Incoming Telnet logins, including connections to network socket ports and the remote console, are enabled by default. This behavior can be changed with the **Change Incoming** command and one of the following parameters:

Telnet	Enables incoming Telnet logins
None	Disables all incoming logins

For security reasons, you may wish to disable incoming logins. Incoming logins for a port can be disabled with the **Change Access** command (see *Access Mode* on page 4-9 for more information).

> **Note:** *Access to the remote console port can never be disabled.*

If you do not want to completely disable incoming logins, you can configure the MSS to require a login password for incoming connections with various commands, depending on the type of incoming connection. See *Login Passwords* on page 3-2 for more information.

3.3.1 TCP/IP Logins

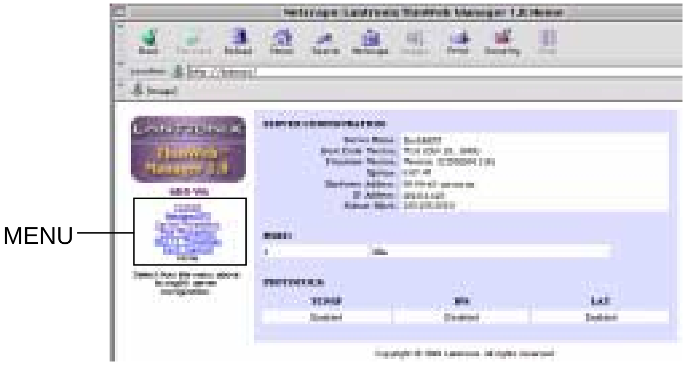
3.3.1.1 Web Browser Login and Configuration

If your MSS has an IP address, you can log into it using a standard web browser with Java enabled. Simply type the MSS IP address or resolvable text name into the browser’s URL/ Location field.

Figure 3-11: Sample Web Browser Login

Once you have connected to the MSS, you will see the Lantronix ThinWeb Manager interface. Use the left-hand menu to navigate to subpages where you can configure important settings and view statistics and other server information.

Figure 3-12: ThinWeb Manager Interface



3.3.1.2 EZWebCon Login and Configuration

If you are on a TCP/IP network, you can log into and configure the MSS with EZWebCon. The program offers a simple interface that prompts you for the information necessary to configure the server. Instructions for installing, running, and using EZWebCon are included on the CD-ROM.

3.3.1.3 Telnet

To log into the MSS, type **telnet** followed by the MSS IP address. The MSS must have an IP address assigned in order for this command to work.

Figure 3-13: A Telnet Connection

```
% telnet 192.0.1.88
```

3.3.1.4 Rlogin

Rlogin allows users to connect to a remote device as if they were on the local network. Rlogin is enabled by default.

To log into the MSS, type **rlogin** followed by the MSS IP address

Figure 3-14: An Rlogin Connection

```
% rlogin 192.0.1.88
```

3.3.2 Serial Port Logins

Attach a terminal to one of the serial ports and press the **Return** key. The **Local>** prompt should be displayed. Proceed to the *Configuration* chapter to configure the unit using the command line interface.

If there was a problem during the boot process, pressing any key will display the Boot prompt. This prompt enables you to enter a special set of commands, called Boot Configuration Program (BCP) commands, which are discussed in *Appendix B*.

3.3.3 Remote Console Logins

You can configure the MSS via a Telnet connection to the remote console port, designated as port 7000. Connections to the console port cannot be disabled. This ensures that administrators will always be able to log into the port.

To connect to the remote console port, use the **Telnet** command followed by the MSS IP address and the remote console port number (7000). You will have to enter the login password. The default login password is **access**. For more information on the login password, see *Login Passwords* on page 3-2.

After you issue the appropriate password, you will see a Username> prompt. Enter a username to identify yourself as the current user.

Note: *This username is arbitrary and used only for convenience. It is not associated with authentication.*

Figure 3-15: Connecting to the Console Port

```
% telnet 192.0.1.88 7000
Trying 192.0.1.88
Connected to 192.0.1.88
Escape character is ‘^]’

# access (not echoed)

Lantronix MSS Version n.n/n (yymmdd)
Type Help at the ‘Local>’ prompt for assistance.

Enter Username> jerry
```

3.4 Outbound Connections

When logged into the MSS, users can make basic outgoing connections using the methods described in this section. See the *MSS Reference Manual* on the CD-ROM for more information about incoming and outgoing connections.

Note: *If you Telnet into the MSS, you cannot make outgoing connections.*

To start an outgoing Telnet session, type **Telnet** at the **Local>** prompt, followed by either the host's name or its numeric IP address.

Figure 3-16: Telnet Connection

```
Local> TELNET 192.0.1.66
```

3.5 Logout

To manually log out of the MSS, type **Logout** or **Logout Port** at the **Local>** prompt, or press Ctrl-D.

Figure 3-17: Logging out of the MSS

```
Local> LOGOUT
```

4: Configuration

Certain parameters must be configured before the MSS can function in the network. Although many users will prefer to use either EZWebCon or the web browser interface, this chapter explains how to configure more advanced MSS features via the command line interface.

The command line interface allows you to enter commands at the **Local>** prompt to configure, monitor, and use the MSS. This chapter covers important MSS functionality such as:

- Rebooting the MSS on page 4-1
- TCP/IP Configuration on page 4-2
- RS-485 Configuration, with a special note on using the MSS in RS-422 applications on page 4-6
- Serial Port Configuration on page 4-9
- 802.11 Configuration on page 4-16
- Formatting an ATA Flash Card on page 4-22
- Modem Cards on page 4-22

The full command set is discussed in detail in the *MSS Reference Manual*.

4.1 Rebooting the MSS

There are two types of reboots for the MSS. A normal reboot simply restarts the MSS. A factory reboot restores default configurations for the MSS, removing any custom settings.

4.1.1 Normal Reboot

You should use use a normal reboot if you have configured custom settings that will not take effect until after the MSS has rebooted. You should also reboot the MSS if you add or swap PC cards, as PC cards are only scanned at boot time.

To reboot the MSS, perform **one** of the following:

- At the **Local>** prompt, enter the **Initialize Delay 0** command.
- At the **Boot>** prompt, enter the **Initialize 451** command. See *Entering Commands at the Boot Prompt* on page B-4 for more details.
- Remove the power cord from the MSS, then plug it back in.

4.1.2 Factory Defaults

You should only restore factory default settings if you want to remove all custom configuration from the MSS, including password settings.

To restore factory settings to the MSS:

- Enter the **Initialize Factory** command at the **Local>** prompt.
- Press and hold the reset button down while cycling power to the unit. You must hold the reset button for at least 3 seconds after power is restored.

4.2 TCP/IP Configuration

For more information on TCP/IP protocol configuration, refer to the *MSS Reference Manual*.

4.2.1 IP Address

You can change the IP address with the **Change IPAddress** command.

Figure 4-1: Changing the IP Address

```
Local>> CHANGE SERVER IP ADDRESS 192.0.1.228
```

4.2.2 Subnet Mask

IP networks can be divided into several smaller networks by subnetting. When you request a connection, the MSS decides whether the desired TCP/IP host is on the local network segment with the help of the subnet mask. This mask identifies the network and node parts of the IP address, which is then applied to the addresses of both the MSS and the remote host. If the resulting addresses are identical, the connection is deemed local and the host is contacted directly. If not, the connection attempt and all subsequent messages to this host will be directed to the MSS's gateway host for forwarding. All hosts must agree on the subnet mask for a given network.

When you configure the MSS IP address for the first time, a default subnet mask will be configured automatically. This default subnet mask should work for most networks. If your network is divided into subnetworks, you will need to create a custom subnet mask. To set a new subnet mask, use the **Change Subnet Mask** command.

Figure 4-2: Setting the Subnet Mask

```
Local>> CHANGE SERVER SUBNET MASK 255.255.255.248
```

4.2.3 Gateway

Usually, a TCP/IP internet is broken down into networks and subnetworks, and a host is only able to see the hosts on its own network. TCP/IP networks rely on routers, or gateways, to transfer network traffic to hosts on other networks. Gateways are typically connected to two or more networks and will pass (or route) TCP/IP packets across network boundaries.

The MSS can be told which hosts are the gateways for the local network. If no gateway is specified, the MSS will listen to network broadcasts to decide which hosts are acting as gateways. The command below tells the MSS which host is the preferred gateway.

Figure 4-3: Specifying a Gateway

```
Local>> CHANGE SERVER GATEWAY 192.0.1.173
```

Note: *A secondary gateway can also be configured in case the primary gateway is unavailable.*

If you do not wish to use a preferred gateway, specify 0.0.0.0 as the IP address in the above command. See **Change Gateway** in the *MSS Reference Manual* for more information.

4.2.4 Name Server

A TCP/IP host generally has an alphanumeric host name, such as Phred, in addition to its IP address. The alphanumeric host name is usually more descriptive or easier to remember. For this reason, the MSS supports domain name system servers (DNS). A DNS server is a host that can translate text host names into the numeric addresses needed to make a connection. To specify a domain name server, use the following command:

Figure 4-4: Configuring a Nameserver

```
Local>> CHANGE SERVER NAMESERVER 192.0.1.167
```

A secondary nameserver can also be specified for use when the primary nameserver is unavailable. See **Change Nameserver** in the *MSS Reference Manual* for more information.

Note: *If the MSS cannot resolve a text host name, use the numeric IP address.*

The MSS also allows you to set a default domain name to be appended to any host name for the purpose of name resolution. When a user types a host name, the MSS will add this domain name and attempt the connection. Name checking applies to any MSS commands that require text name resolution, such as Telnet, Rlogin, and Ping. To set the default domain, enter the **Change Domain** command followed by the desired domain name in quotes

Figure 4-5: Configuring the Default Domain

```
Local>> CHANGE SERVER DOMAIN “xyzcorp.com”
```

Note: *Some nameservers will not resolve host names that do not have a domain at the end.*

4.2.5 IP Security

The IP Security feature allows the system administrator to restrict incoming and outgoing TCP/IP sessions and access to the serial ports. Every time a connection is requested, the MSS will check the IP local host table to determine whether or not that connection should be allowed. Connections are allowed or denied based upon the source IP address (for incoming connections) or the destination IP address (for outgoing connections).

The IP local host table stores a list of allowed (Enabled) and denied (Disabled) IP addresses in either the form of individual addresses (e.g. 192.71.2.88) or wildcards, with a 255 in one or more of the trailing segments (e.g. 192.255.255.255). Wildcard addresses match all addresses in that range. To add an entry, specify an IP address and whether to allow or deny connections.

Connections can also be denied based on which port is attempting the connection and whether the connections are incoming or outgoing. For example, the command below disables outgoing connections for all addresses between 192.0.1.1 and 192.0.1.254 from all four serial ports.

Figure 4-6: IP Security Command

```
Local>> CHANGE IPSECURITY 192.0.1.255 OUTGOING DISABLED
```

See **Change IPSecurity** in the *MSS Reference Manual* for more information on this command.

To view the host table entries, enter the **Show IPsecurity** command. To remove an entry, use the **Delete IPSecurity** command followed by the IP address that you want to remove.

4.2.6 WINS

If WINS is enabled, the MSS will broadcast a WINS name announcement at boot time, and answer broadcast WINS name queries. Other hosts can locate the MSS this way. The MSS will rebroadcast whenever its IP address or name changes.

To enable WINS, enter the following command.

Figure 4-7: Enabling WINS

```
Local>> CHANGE WINS ENABLED
```

4.2.7 SNMP

The MSS supports the SNMP network protocol, which allows hosts on the network to query nodes for counters and network statistics and to change some parameters on those nodes. The form of these requests is documented by RFC 1098. The list of items that can be queried and/or set and the type of data used, such as integer and string, are both documented in various Management Information Bases (MIBs). MIBs cover a variety of things, such as counters and IP address resolution tables.

The MSS supports the following MIBs:

Table 4-1: Supported MIBS

MIB-II (RFC 1213)	System, Interface, Address Translation, IP, ICMP, TCP, and UDP, but not the EGP group.
Character MIB (RFC 1318)	All character-oriented devices.
RS232 MIB (RFC 1317)	All objects (RS-232-style objects).

The MSS will respond to queries for unknown MIBs with a “not in MIB” error to the to the requesting host.

4.2.7.1 SNMP Trap Support

The MSS will generate limited forms of three of the SNMP **traps**. Traps are sent to a host when certain events occur on the MSS.

The MSS will generate a Coldstart trap when it first boots, and will send a Linkup trap when the startupfile (if any) has been read from a host and normal operation commences. If a startupfile has been configured but the download fails, the MSS will send an Authentication trap. In all three cases, the trap will be directed to the IP address of the loadhost for the MSS. If a loadhost has not been specified, the traps will not be sent.

The MSS will not generate traps other than the ones listed here.

4.2.7.2 Configuring SNMP

The MSS has a single community (“public”) with read-only access. You can optionally add a single community with read-write access using the **Change SNMPSetComm** command. See the *MSS Reference Manual* for more details.

Once you enable an SNMP write community, you can use SNMP SET operations to configure the following things on the MSS. Items marked with an asterisk (*) are saved to non-volatile RAM (NVR) and therefore may take longer to complete.

RS232 MIB:	PortInSpeed* (also changes PortOutSpeed) PortOutSpeed* (also changes PortInSpeed) PortInFlowType* (also changes PortOutFlowType) PortOutFlowType * (also changes PortInFlowType) AsyncPortBits* AsyncPortStopBits* AsyncPortParity * AsyncPortAutobaud*
Character MIB:	PortName PortReset PortInFlowType PortOutFlowType PortSessionMaximum SessionKill

4.3 RS-485 Configuration

While the MSS serial ports are initially configured for RS-232 networking, they can also be configured for RS-485 networking. The RS-485 standard allows a serial connection to be shared like a “party line.” As many as 32 devices can share the multidrop network. Typically, one device is the master and the other devices are slaves. There are a few important things to note about RS-485 networking with the MSS.

- The MSS can be used in either two-wire or four-wire mode. Refer to the following sections to determine which mode to use.
- The maximum RS-485 network cabling length (without repeaters) is 4,000 feet. Lantronix recommends the use of shielded twisted-pair cabling.
- A large number and varieties of protocols run over RS-485. However, the MSS does not convert or interpret serial data. It only moves data between serial and Ethernet. Any RS-485 protocol will have to be implemented by host software.

Note: *See Appendix C for the RS-485 pinouts.*

To enable RS-485 mode on the MSS, enter the **Change RS485 Enabled** command. This command can apply to any or all of the serial ports. RS-232 mode is enabled by default.

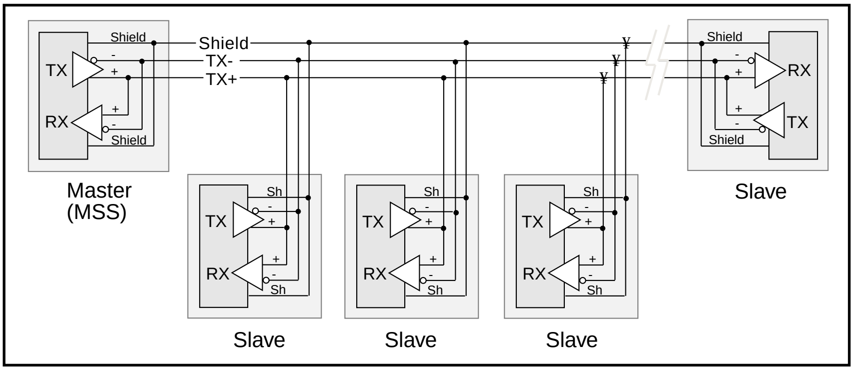
Figure 4-8: Enabling RS-485 Mode

```
Local>> CHANGE RS485 PORT 3 ENABLED
```

4.3.1 Two-wire Mode

In two-wire mode, the MSS operates in half duplex: one pair of wires shares transmit and receive signals, and an optional third wire can be used for shield/ground. The main advantage of using two-wire mode is reduced cabling costs.

Figure 4-9: Example Two-wire Mode Network



In a two-wire RS-485 network, the MSS must turn its transmitter on when it is ready to send data and then off for a certain period of time after the data has been sent so that the line is available to receive again. At most baud rate settings, the timing delay is typically one character length with a maximum of 1.5 character lengths.

Figure 4-10: Enabling Two-Wire RS-485 Mode

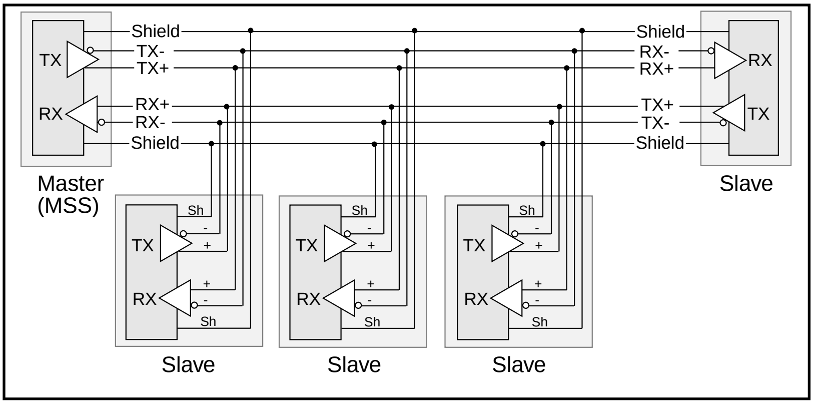
```
Local>> CHANGE RS485 PORT 3 MODE 2WIRE
```

Note: *For two-wire mode, the TXDrive setting must be set to Automatic (see TXDrive on page 4-8). If you enable two-wire mode and TXDrive is set for Always, the MSS will return an error.*

4.3.2 Four-wire Mode

In four-wire mode, the MSS operates in full duplex: one pair of wires functions as the transmit pair, another pair of wires functions as the receive pair, and there is a shield/ground wire for each pair. The MSS is able to send and receive data simultaneously. In a four-wire RS-485 network, one device acts as a master while the other devices are slaves. The advantages of four-wire mode are double the throughput of two-wire mode and a guaranteed open path to each slave device's receiver.

Figure 4-11: Example Four-Wire Mode Network



It is important to connect the transmitter of the master device to the wire that is connected to the receive terminals on the slave devices, and connect the receiver of the master device to the wire that is connected to the transmit terminals on the slave devices. In essence, the master device will be connected to the slave devices with a *swapped* cable.

Figure 4-12: Enabling Four-Wire RS-485 Mode

```
Local>> CHANGE RS485 PORT 3 MODE 4WIRE
```

4.3.2.1 TXDrive

The MSS can be configured to either always drive the TX (transmit) signal or to let the attached device control the TX signal (tristate) when not actively transmitting. The **Change RS485 TXDrive** command takes one of two parameters. The **Always** parameter sets the MSS for continuous TXDrive, so TX will never be tristated. The **Auto** parameter sets the MSS for TXDrive when transmitting and tristate while idle.

Figure 4-13: Changing TXDrive

```
Local>> CHANGE RS485 PORT 3 TXDRIVE AUTO
```

Note: *You can only set TXDrive for Always when using four-wire mode. The Always parameter has no effect for two-wire mode.*

4.3.3 Termination

RS-485 connections must be terminated properly in order to work. Termination is necessary when using long cable runs, although **only** end nodes should be terminated. The termination option is disabled by default.

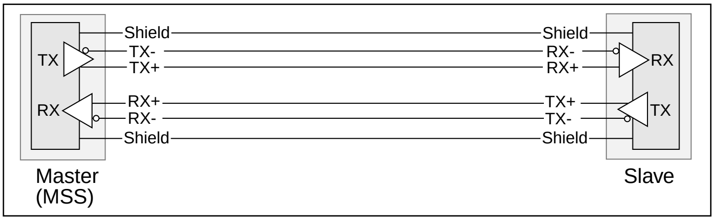
Figure 4-14: Enabling RS-485 Termination

```
Local>> CHANGE RS485 PORT 3 TERMINATION ENABLED
```

4.3.4 RS-422 Networking

The MSS is compatible with RS-422 networks in four-wire RS-485 mode. Connect the MSS to a single slave device using a swapped cable, as shown below, and configure the MSS as if you were going to use it for four-wire RS-485 networking.

Figure 4-15: RS-422 Connection



4.4 Serial Port Configuration

The serial ports are set at the factory for 9600 baud, 8 data bits, one stop bit, and no parity. Remember that ports should be logged out after configuration so the changes will go into effect.

On the MSS4, the first serial port is designated as the console port. However, this is not a dedicated console port and is fully configurable.

4.4.1 Access Mode

The serial port access mode governs what kind of connections each port can accept. **Local** access permits local logins on the serial port. **Remote** access allows network hosts to connect to the MSS. **Dynamic** access (the default) allows both local and remote access.

To change a serial port’s access mode, enter the **Change Access** command. The following example enables local logins to the first serial port.

Figure 4-16: Changing Serial Port Access Mode

```
Local>> CHANGE PORT 1 ACCESS LOCAL
```

If an attached serial device will be continuously transmitting data, the port should be set to **Access Remote** so the data will not accidentally cause the MSS to create a local connection.

4.4.2 Autostart

Normally, the serial port will wait for a carriage return before starting a connection. When the Autostart option is enabled, the MSS will establish a connection as soon as it boots (or, if modem control is enabled, as soon as the DSR signal is asserted). To control this feature, enter the **Change Autostart** command. The following example enables Autostart for the second serial port.

Figure 4-17: Enabling Autostart

```
Local>> CHANGE PORT 2 AUTOSTART ENABLED
```

A port set for Autostart will never be idle, and therefore will not be available for network connections. If network connections are desired, Autostart should remain disabled (the default).

Autostart can also be triggered by a specific input character. As the MSS does not have a default Autostart character, you will have to configure one. For example, when using modem emulation mode, you may want to use **A** so that Autostart will happen as soon as an **AT** modem command is entered. See *Modem Emulation Mode* on page 5-13 for more information. Keep in mind that when you configure an Autostart character, you can no longer use <CR> to get to the **Local>** prompt. The following example configures “A” as the Autostart character for the first serial port.

Figure 4-18: Configuring an Autostart Character

```
Local>> CHANGE PORT 1 AUTOSTART CHARACTER “A”
```

You can also specify a control character using escaped hex. For example, Ctrl-B (ASCII character 0x02) is “\02” in escaped hex.

4.4.2.1 Saving Autostart Characters

If the port is configured with a Dedicated port host and Autostart is enabled for that port, the autostart characters that start the connection can either be passed to the host as the first bytes of data or can be discarded. If you want to pass the characters along, you must configure the Autostart Save parameter, as the default is to discard autostart characters. The following example passes the first (or only) autostart character along to the host.

Figure 4-19: Saving Autostart Characters

```
Local>> CHANGE PORT 1 AUTOSTART SAVE 1
```

Another option is **Save None**, the default setting, which will not pass anything on to the host.

4.4.3 Serial Data

Once a connection has been started, several different triggers can be used to transmit all accumulated serial data to the host. These options are controlled with the **Change Datasend** command. The datasend process used by the MSS balances network traffic with latency concerns.

One kind of trigger can be set by specifying a “timeout” condition of either the time since the last character was received or the time since the current character burst was started. For example, to trigger data transmission 150 milliseconds after the current character burst began, enter the following command:

Figure 4-20: Transmitting Serial Data with Trigger Delay

```
Local>> CHANGE PORT 1 DATASEND DELAY FRAME 150
```

The example in Figure 4-20 can be visualized as:

```
x x x xxx xx (data) x x xx xxxxxxxx xx xxxx xx xxxx
|--------------------------------------------------|
                 150 milliseconds                   transmit packet
```

Another option is to set a one- or two-character trigger that will cause the MSS to transmit the data. You can also specify whether the trigger characters will be sent to the host as part of the serial data or whether they should be discarded (the default). For example, the following commands will cause the accumulated serial data to transmit as soon as the “Z” character is detected in the data stream and to send the matched character (“Z”) to the host as part of that data.

Figure 4-21: Transmitting Serial Data with a Character Trigger

```
Local>> CHANGE PORT 1 DATASEND CHARACTER Z
Local>> CHANGE PORT 1 DATASEND SAVE 1
```

The example in Figure 4-21 can be visualized as:

```
x x x xxx xx (data) x x xx xxxxxxxx xx xxx Z xx xxxx
|--------------------------------------------------|
                                                    transmit packet
```

For more information on the **Change Datasend** command, see the *MSS Reference Manual*.

4.4.4 Baud Rate

The MSS and the attached serial device must agree on a speed, or baud rate, to use for the serial connection. Valid baud rates for the MSS are 300, 600, 1200, 2400, 4800, 9600 (the default), 19200, 38400, 57600, 115200, and 230400 baud. The baud rate can be changed with the **Change Speed** command followed by a baud rate number. The following example changes the baud rate for the second serial port.

Figure 4-22: Changing the Baud Rate

```
Local>> CHANGE PORT 2 SPEED 19200
```

The MSS supports Autobaud, which allows a serial port to match its speed to the attached serial device upon connection (see **Change Autobaud** in the *MSS Reference Manual* for an explanation of the baud rate negotiation process). Autobaud is disabled by default, but can be enabled with the following command.

Figure 4-23: Enabling Autobaud

```
Local>> CHANGE PORT 1-4 AUTOBAUD ENABLED
```

4.4.5 Character Size, Parity, and Stop Bits

The default character size of 8 data bits can be changed to 7 data bits. Similarly, the default stop bit count of 1 bit can be changed to 2 bits. Parity is normally None, but can also be Even, Mark, Odd, or Space. To change these parameters, use the following commands. Note that in this example, the parameters are being changed for the second serial port only.

Figure 4-24: Configuring Serial Port Parameters

```
Local>> CHANGE PORT 2 CHARSIZE 7
Local>> CHANGE PORT 2 STOPBITS 2
Local>> CHANGE PORT 2 PARITY EVEN
```

4.4.6 Flow Control

Note: *RTS/CTS Flow Control is not available in RS-485 mode.*

Both RTS/CTS (hardware) and XON/XOFF (software) flow control methods can be used on the MSS. RTS/CTS controls data flow by sending serial port signals between two connected devices. XON/XOFF controls data flow by sending particular characters through the data stream: **Ctrl-Q** to accept data (XON) and **Ctrl-S** when data cannot be accepted (XOFF).

Note: *Applications that use Ctrl-Q and Ctrl-S will conflict with XON/XOFF flow control, in which case RTS/CTS is recommended.*

To switch between flow control methods for a serial port, use the **Change Flow Control** command followed by the preferred method. If you do not wish to use flow control at all, specify **None**.

Figure 4-25: Enabling Recommended Flow Control

```
Local>> CHANGE PORT 2 FLOW CONTROL CTSRTS
or
Local>> CHANGE PORT 2 FLOW CONTROL XONXOFF
```

If you're using XON/XOFF flow control, the XON/XOFF characters will be removed from the data stream by default. To prevent this removal, enable Passflow with the **Change Passflow** option. However, passflow is unnecessary in most situations.

4.4.7 Modems and Modem Signaling

Note: *These modem-related commands can not be used with RS-485 networking.*

The following sections explain some of the MSS options that are typically considered to be modem-related. They do not apply exclusively to modems, but to communications devices in general. Most options are mutually exclusive when enabled.

Note: *Modem Emulation Mode, in which the MSS acts like a modem and only accepts AT modem commands, is discussed in Chapter 5.*

After configuring modem-related settings, refer to the *Modem Configuration Checklist* on page B-4.

4.4.7.1 Modem Control

When enabled, this feature allows the MSS to check for signals coming from the modem (or other attached serial device) to establish whether a valid connection exists. If a connection has ended, the MSS should be able to log out the port and prepare to accept a new connection. Similarly, if no connection is open, the MSS should know to ignore spurious characters from the port and only accept valid connection attempts. The MSS can do both of these when modem control is enabled.

Modem control implies three things:

- The MSS will log out the port when DSR is dropped (as if DSRLogout were enabled).
- The MSS will hold DTR low for approximately 3 seconds after the port is logged out.
- The MSS will not Autostart a new connection until the attached device asserts DSR.

To enable modem control for a serial port, enter the **Change Modem Control** command. The following example enables modem control for all four serial ports.

Figure 4-26: Enabling Modem Control

```
Local>> CHANGE PORT 1-4 MODEM CONTROL ENABLED
```

4.4.7.2 Signal Checking

When signal checking is enabled, the MSS will check for the presence of an asserted Data Signal Ready (DSR) input signal before allowing incoming network connections to the enabled serial port. Network connections to the serial port will not be permitted unless the DSR signal is asserted.

To enable DSR signal checking, use the **Change Signal Check** command. The following example enables signal checking for the first serial port.

Figure 4-27: Enabling Signal Checking

```
Local>> CHANGE PORT 1 SIGNAL CHECK ENABLED
```

4.4.7.3 DSRLogout

Note: *DSRLogout is not available in RS-485 mode.*

When a device connected to the MSS is disconnected or powered off, the DSR signal is de-asserted. The MSS can be configured to automatically log out the port when this occurs using the **Change DSRLogout Enabled** command. This also prevents users from accessing other sessions by switching physical terminal lines. The following example enables DSRLogout for the first serial port.

Figure 4-28: Enabling DSRLogout

```
Local>> CHANGE PORT 1 DSRLOGOUT ENABLED
```

4.4.7.4 DTRWait

Note: *DTRWait is not available in RS-485 mode.*

Spurious characters from the attached serial device may be interpreted as a login attempt, which could cause the port to be unavailable for network connections. To avoid this behavior, the MSS uses the Data Transmit Ready (DTR) output line to signal an attached serial device that a connection attempt is valid.

Normally DTR will be asserted when the port is idle. The DTRWait feature keeps the MSS from asserting DTR until the port is actually in use (whether due to a login or a network connection). To control DTRWait, use the **Change DTRWait** command. The following example enables DTRWait for the first serial port.

Figure 4-29: Enabling DTRWait

```
Local>> CHANGE PORT 1 DTRWAIT ENABLED
```

When DTRWait is enabled, the MSS will assert DTR when a connection begins and de-assert DTR when the connection ends.

4.4.8 Logouts

In addition to DSRLogouts, a port can be manually logged out, or it can be configured to automatically log out when it has been inactive for a pre-determined length of time. To manually log out of the MSS, type **Logout** at the **Local>** prompt, or press **Ctrl-D**.

Figure 4-30: Logging out of the MSS

```
Local>> LOGOUT
```

To log out a port after a specified period of inactivity, use the **Change Inactive Logout** command. This command works in conjunction with **Change Inactive Timer,** which defines how long a port must remain idle before it is automatically logged out. For example, to make the MSS log out the first serial port after one minute of inactivity, use the following commands. The inactivity logout timer period can be specified in seconds (s) or minutes (m). Changing **1m** to **60s** in the following example produces the same results.

Figure 4-31: Enabling Timed Inactivity Logout

```
Local>> CHANGE PORT 1 INACTIVE LOGOUT ENABLED
Local>> CHANGE PORT 1 INACTIVE TIMER 1m
```

4.4.9 Preferred Port Host

A default host for a port can be defined using the **Change Preferred** command. The MSS attempts to use the preferred host for connections on a specified port when no host name is specified in a connection command.

Figure 4-32: Defining a Preferred Service

```
Local>> CHANGE PORT 1 PREFERRED TCP 192.0.1.66
```

4.4.10 Dedicated Port Host

A dedicated host can be defined for a port using the **Change Dedicated** command. When a serial user logs in to a dedicated port, the MSS will automatically connect him to the specified host; he cannot access the MSS **Local>** prompt. When the connection is closed, the MSS automatically logs him out.

Figure 4-33: Defining a Dedicated Service

```
Local>> CHANGE PORT 1 DEDICATED TCP 192.0.1.66
```

Environment strings can be added to the command to change connection characteristics. See the **Change Dedicated** command in the *MSS Reference Manual* for more information.

4.5 802.11 Configuration

Note: *The MSS does not support PC card hot-swapping. Any time you insert a PC card into an MSS PC card slot, you must reboot the MSS.*

The following parameters should be configured only if you are using the MSS for 802.11 wireless Ethernet networking and plan to use a wireless LAN PC card in one of the MSS PC card slots. Users in countries other than the United States must set the Region appropriately before using 802.11.

Not all configuration options will be available on all 802.11 cards. If you try to enter an option that is not supported by your card, you will receive an Error message.

Note: *Even though the MSS4 has two PC card slots, you can only install one 802.11 card. The card can be installed in either slot.*

This section assumes that you understand IEEE 802.11 concepts and architectures. If you do not, please refer to the IEEE 802.11 standard or the documentation that came with your PC card or Access Point (AP).

Any time you enable or disable 802.11 networking, you must reboot the MSS before the change takes effect. Any other changes you request with the **Change 80211** commands will not take place until you have entered the **Change 80211 Reset** command.

4.5.1 802.11 Terms

The following acronyms are used in this section:

AP

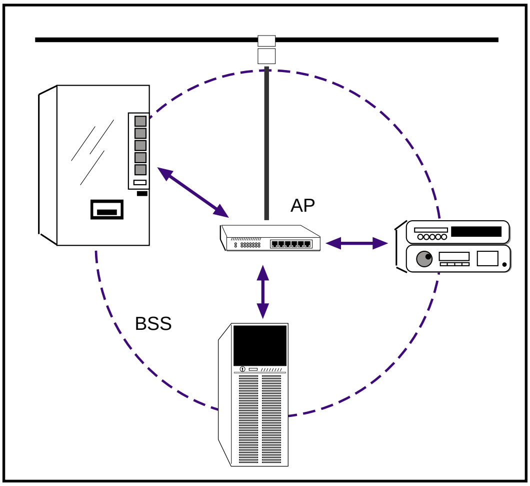
Access Point, a device that relays communications between one or more wireless devices and possibly other devices on a network. APs are usually connected to a physical network.

Note: *If you are using an AP and WEP is not enabled, set the AP to accept Open System Authentication. If WEP is enabled, set the AP to Shared Key Authentication. For more information about WEP, see the definition below.*

BSS

Basic Service Set (or Cell), a group of wireless devices that speak directly with each other. A BSS may consist of at most one AP.

Figure 4-34: Simple Wireless Network BSS



ESS

Extended Service Set, a network consisting of one or more BSSs that share the same ESSID. An ESS can contain multiple APs.

IBSS

Independent Basic Service Set, a BSS with no APs. Devices work in an ad-hoc networking mode.

WEP

Wireless Equivalent Privacy, a form of encryption for wireless communication.

4.5.2 Enabling 802.11 Networking

The MSS has 802.11 networking enabled by default. This allows the MSS to check for a compatible wireless networking card at startup. If a compatible card is present, the MSS will use the wireless network and ignore any wired Ethernet settings. If no compatible PC card is present, the MSS will use the 10/100BASE-T or 100BASE-FX Ethernet interface.

If you want the MSS to only look for a wired Ethernet connection, you must disable 802.11.

Figure 4-35: Disabling 802.11

```
Local>> CHANGE 80211 DISABLED
```

Note: *You must reboot the MSS after enabling or disabling 802.11 networking.*

4.5.3 802.11 Region

When using 802.11 networking, you **must** make sure the MSS is configured for the correct regulatory region. Configuring this option incorrectly may cause the MSS to broadcast on frequencies that are illegal in your area. The factory default setting is correct for the United States; users in other countries should change it to a value appropriate for their area before attempting 802.11 operation.

Recognized regions are:

FCC	United States (the default)
IC	Canada
ETSI	Europe (most countries—check with your local regulatory body to make sure that the entire ETSI frequency range is allowed in your area)
SPAIN	Spain
FRANCE	France
MKK	Japan

Figure 4-36: Setting the 802.11 Region

```
Local>> CHANGE 80211 REGION IC
Local>> CHANGE 80211 RESET
```

4.5.4 MAC Address

A MAC address is a unique identifier that distinguishes different devices on the 802.11 network. It is the same as the unit’s hardware address.

For networking purposes, the MSS can be configured to use either the PC card’s MAC address or its own internal MAC address (the default) with the **Change 80211 MACADDRESS** command. Using the MSS MAC address allows for more seamless operation when switching between wired and wireless networking.

Figure 4-37: Configuring the MAC Address

```
Local>> CHANGE 80211 MACADDRESS CARD
Local>> CHANGE 80211 RESET
or
Local>> CHANGE 80211 MACADDRESS MSS
Local>> CHANGE 80211 RESET
```

4.5.5 Extended Service Set ID (ESSID)

Whenever there is more than one ESS in a wireless LAN architecture, devices need to be told which ESS they belong to. The ESSID ensures that devices communicate with the right AP.

To tell the MSS which ESS it belongs to, enter the **Change 80211 ESSID** command. The exact string you enter will be determined by the settings of the AP with which you want the MSS to communicate.

Figure 4-38: Configuring the ESS ID

```
Local>> CHANGE 80211 ESSID “floor3”
Local>> CHANGE 80211 RESET
```

Setting the ESSID to none (**Change 80211 ESSID None**) allows the MSS to associate with any AP within range.

4.5.6 Network Mode

There are two types of 802.11 networks: ad-hoc and infrastructure. In an ad-hoc network, devices communicate directly with one another on a peer-to-peer basis. In an infrastructure network (the default), several devices communicate with one or more APs. The APs may or may not be connected to a physical Ethernet network. You must tell your MSS which type of network is present with the **Change 80211 Networkmode** command.

Figure 4-39: Configuring the Network Mode

```
Local>> CHANGE 80211 NETWORKMODE ADHOC
Local>> CHANGE 80211 RESET
or
Local>> CHANGE 80211 NETWORKMODE INFRASTRUCTURE
Local>> CHANGE 80211 RESET
```

The network mode setting relates to the channel setting, explained next.

4.5.7 Channel

The frequency band allocated to 802.11 wireless communications is subdivided into different channels to allow subnetworking. Your MSS needs to know which channel it should use for communications—the channel will be the same as the one being used by the local AP. The default setting, **Any**, causes the MSS to use the same channel used by the strongest AP with the same ESSID.

The channel setting relates to the network mode setting. For infrastructure network mode, you should set the channel to Any so that the MSS can synchronize with an AP. For Ad-Hoc network mode, you should set a specific channel number so that the MSS can start a new IBSS if needed. When the channel is set to Any, the MSS can only join an existing IBSS.

Figure 4-40: Configuring the 802.11 Channel

```
Local>> CHANGE 80211 CHANNEL 7
Local>> CHANGE 80211 RESET
```

A direct-sequence 802.11 network on one channel will affect reception on channels up to two numbers away. For best performance on collocated wireless networks, you should select channels that are at least five channels apart from each other. For example, three networks could be put on channels 1, 6, and 11 (depending on your regulatory region). See your PC card documentation for specific information about which channels are available in your area.

4.5.8 WEP

Some 802.11 cards can be set with a WEP key, which will encrypt any data you transmit through wireless communication.

To enable WEP, enter the following command:

Figure 4-41: Enabling WEP

```
Local>> CHANGE 80211 WEP ENABLED
Local>> CHANGE 80211 RESET
```

4.5.8.1 Setting the WEP Key and Index Number

When WEP is enabled and a WEP key is set, the MSS will only connect to an AP (in infrastructure mode) or communicate with other ad-hoc peers (in ad-hoc mode) that have been programmed with the same WEP key as the MSS. For a key to match, both the key data and the index number must be identical.

Once WEP is enabled, you must enter a WEP key if you have not previously done so. The key can be either 40-bits or 128-bits. To enter a WEP key, use the **Change 80211 WEP Key** command.

Each key is also assigned an index number, which is an integer between 1 and 4. To enter the index number, use the **Change 80211 WEP Index** command**.**

Figure 4-42: Setting the WEP Key and Index Number

```
Local>> CHANGE 80211 WEP KEY 26-e4-97-db-1f
Local>> CHANGE 80211 WEP INDEX 3
Local>> CHANGE 80211 RESET
```

4.5.8.2 Encrypted Traffic

Once WEP is enabled, the MSS will allow reception of both encrypted and unencrypted traffic. You can disable the reception of unencrypted traffic by entering the following command:

Figure 4-43: Disabling WEP Unencrypted Traffic Reception

```
Local>> CHANGE 80211 WEP RECEIVE ENCRYPTED
Local>> CHANGE 80211 RESET
```

This command will cause the MSS to discard and ignore any unencrypted wireless frames that it receives and accept only frames encrypted with its WEP key.

4.6 Formatting an ATA Flash Card

Certain kinds of ATA flash memory and disk storage cards can also be used in the PC card slots. Before you insert any kind of card into the MSS, please check the Lantronix web site to make sure that your card is supported and read this section carefully.

Note: *The MSS does not support PC card hot-swapping. Any time you insert a PC card into an MSS PC card slot, you must reboot the MSS.*

ATA cards must be formatted before you can use them with your MSS. To format an installed ATA card, issue the **Disk Format** command for either **/pccard1** (if the card is in the top PC card slot) or for **/pccard2** (for the bottom slot). This command erases all the existing data on the card and formats the card for use with the MSS.

Figure 4-44: Formatting a PC Card

```
Local>> DISK FORMAT /PCCARD1
```

Once a card has been formatted for use with the MSS, it will be available for immediate use anytime the MSS is started up. The formatted card can be used the same as the on-board MSS Flash disk (see *Disk Management* on page 5-7 for more information). If the card is ever reformatted for use with another system, such as a laptop, you will need to reformat it before using it again with the MSS.

4.7 Modem Cards

Certain kinds of modem PC cards can be used with the MSS. Check the Lantronix web site for a list of currently supported cards.

Note: *The MSS does not support PC card hot-swapping. Any time you insert a PC card into an MSS PC card slot, you must reboot the MSS.*

A properly installed modem card will be treated like an additional MSS serial port. If only one card is installed, it will always appear as Port 5. If two cards are installed, the card installed in the top slot (slot 1) will appear as Port 5 and the card in the bottom slot (slot 2) will appear as Port 6. The **Show Port** and **Logout Port** commands will respond appropriately to the modem card ports.

The modem ports will always have modem control enabled and should respond to a standard Hayes-style AT command set. However, you should not configure the modem—its default configuration will work properly with the MSS. If you change the reply codes and status strings, the MSS may not be able to respond correctly. This is in contrast to most other types of PC cards, which the MSS cannot use until properly configured.

SDK users can access the ports by using device “tt4” for Port 5 or “tt5” for Port 6. See your SDK documentation for more information on the SDK environment.

4.7.1 Incoming Calls

The MSS will attempt to answer any incoming call that it detects. You will get a Local> prompt after the modems are fully connected.

4.7.2 Outgoing Calls

To make a call from the MSS modem port, you must connect to the modem card via Telnet or a local serial port. You can then issue AT commands to the modem to dial out.

To connect to the modem from a local serial port, use the **Connect Local** command.

Figure 4-45: Connecting to the Modem

```
Local> CONNECT LOCAL PORT_5
```

To connect to the modem from the network, Telnet to the modem port (port 2005).

Figure 4-46: Connecting to the Modem

```
% telnet 192.0.1.35 2005
```

5: Using the MSS

This chapter explains how to use the MSS once it is running. Users can make host-initiated (incoming) connections and use the host applications and code examples included on the MSS distribution CD-ROM. Users can also use the MSS interactively to make outgoing connections, manipulate sessions, and view server and network information with the help of **Show** commands.

In addition, this chapter explains:

- Using the MSS Flash disk and removable ATA flash cards (see *Disk Management* on page 5-7).
- Configuring an MSS-to-MSS encrypted session (see *Encrypted Sessions* on page 5-9).
- Setting up two MSS units to emulate a direct serial connection over the LAN (see *Serial Tunnel* on page 5-10).
- Using the MSS as a data pipe between a serial device and multiple hosts on the network (see *Multihost Mode* on page 5-11).
- Making the MSS look like a modem so that it can be used with existing communications software (see *Modem Emulation Mode* on page 5-13).
- Using the Lantronix COM Port Redirector software to redirect PC COM ports (see *COM Port Redirector* on page 5-15).

5.1 Incoming Connections

5.1.1 Socket Connections

Each node on a network has a node address, and each node address can allow connections on one or more sockets. Sometimes these sockets are referred to as ports. TCP/IP connections can be made directly to one of the MSS serial ports using sockets.

Note: *If a serial port is in use, the socket connection will be refused.*

There are two categories of sockets. Well-known sockets are those that have been defined in RFCs (Requests for Comments); for example, port 23 is used for Telnet connections. There are also custom sockets that users and developers define for their own specific needs.

There are some important points to remember when making a socket connection:

- Port access **must** be set to either Dynamic or Remote to allow network connection requests. Local access does not allow a port to receive connection requests from the network. To change the port's access type, use the **Change Access** command followed by either Dynamic or Remote.
- The port **must** be idle. Use the **Show Ports** command to verify that the port is not in use. To further ensure that the port will be idle, Telnet to the remote console port rather than attaching a terminal to one of the serial ports.
- If an attached serial device will be continuously transmitting data to the MSS, the MSS port access should be changed to Access Remote (see Section 4.4.2).
- Each serial port only allows one connection at a time, except in the case of *Multihost Mode* (see Section 5.6).
- Timing between serial signals (such as DSR, RTS, and CD) is not preserved, and the state of such signals is not transmitted when using socket connections.

5.1.1.1 TCP/IP Socket Connections

The MSS supports TCP/IP socket connections to ports 2001-2006 and 3001-3006. Ports 2001-2004 and 3001-3004 are physical MSS serial ports, and ports 2005-2006 and 3005-3006 are installed modem cards. To specify a connection to a socket, use the **Telnet** command followed by the MSS IP address (or resolvable name) and the desired socket number.

Open a TCP session to port 300x to form a raw TCP/IP connection to the serial port. Use port 200x when you need Telnet IAC interpretation.

5.1.2 Host Applications

The MSS can be used with applications on UNIX , Windows, Windows NT, OS/2, and Macintosh hosts, and any other hosts that have a TCP/IP socket interface.

When a host application makes a socket connection to the MSS, it uses the socket as a data pipe to send and receive data. The host application performs general read/write tasks, and works with the MSS as if it were a directly-attached serial device.

5.1.3 Code Examples

The MSS distribution CD-ROM includes example code for TCP applications. Refer to the *Readme* file included with the code examples for further information and instructions.

5.2 Interactive Connections

Interactive mode refers to entering commands at the **Local>** prompt. Users can enter commands to configure the MSS, connect to remote services, manipulate a connection, or receive feedback. Interactive use requires an input device, such as a terminal.

5.2.1 Outgoing Connections

The MSS can make outgoing connections to hosts on TCP/IP networks via one of its serial ports. It supports Telnet and Rlogin connections, and environment strings added to the connection commands. See the *Command Reference* chapter of the *MSS Reference Manual* for more information.

5.2.1.1 Telnet

To start an outgoing Telnet session to a remote host on a TCP/IP network, type **Telnet** at the **Local>** prompt, followed by either the host's name or its numeric IP address.

Figure 5-1: Opening a Telnet Connection

```
Local> TELNET 192.0.1.66
```

Note: *If you have configured a preferred host, no host name is required.*

The **Telnet** command can be followed by one or more environment strings. This table shows the most commonly used strings—see the *MSS Reference Manual* for the complete list.

Table 5-1: Commonly Used Environment Strings

R	Rlogin protocol (sets port number to 513 if not already set)
T	TCP mode (raw uninterpreted data stream)
U	UDP mode (the default UDP socket is 4096)
Y	Encrypted mode (raw TCP socket that encrypts all data using a 56-bit key)
nnnn	socket number (TCP and UDP only)

These environment strings can be used to make a Telnet connection to a specific port number. For example, to form a raw Telnet connection to socket 2001, follow the host's name or numeric IP address with :2001 and the environment string T.

Figure 5-2: Opening a Telnet Connection to a Specific Port

```
Local> TELNET 192.0.1.66:2001T
```

5.2.1.2 Rlogin

Rlogin allows a user to log into a remote host as if he or she were a local user. In the example below, **shark** is the remote host and **lola** is the username. Unless the username is password protected, the user will be logged in normally.

Figure 5-3: Connecting with Rlogin

```
Local> RLOGIN shark “lola”
```

Note: *Because Rlogin can bypass the normal password/login sequence and is therefore a potential security problem, it may be disabled on some hosts. It is disabled by default on the MSS.*

5.2.2 Session Control

When a user connects to a network service (via Telnet, Rlogin), a session is created. A user can open several connections to various hosts at once, although only one is displayed on the screen at a time. Each separate connection is a session. The following section explains commands used to manipulate sessions.

5.2.2.1 Break Key and Local Switch

The Break key allows users to leave an active session and return to the MSS **Local>** prompt without disconnecting sessions. By default, the MSS handles the Break key locally. Users can change whether the Break key is processed by the MSS (Local), processed by the remote host (Remote), or ignored (None) using the **Change Break** command.

Figure 5-4: Changing the Break Key

```
Local>> CHANGE BREAK REMOTE
```

If your terminal does not have a Break key, you can configure a local break switch key. To specify an escaped hex character, preceed it with a backslash (\xx). The example below sets Ctrl-B (ASCII character 0x02) as the local switch character.

Figure 5-5: Defining a Local Switch

```
Local>> CHANGE LOCAL SWITCH \02
```

5.2.2.2 Backward, Forward, and Switches

The **Backward** and **Forward** commands, when entered at the **Local>** prompt, allow users to navigate through current sessions.

You can think of a user’s open sessions as a list from the earliest to the most recently created. *Forward* refers to a more recent connection, while *Backward* refers to a session started earlier. The list is also circular; going forward from the most recently created session takes you to the earliest session, and going backward from the earliest session resumes the most recent session. For example, user Bob connects to host Thor. He then breaks to local mode and connects to host Duff. After working, he breaks and connects to host Conan. His session list, shown with the **Show Session** command, would be:

Thor

Duff

Conan

Conan is the **current session**, meaning the session to which the user is currently connected (or the last session the user was in before entering local mode). If Bob pressed the backward key while working in Conan, he would resume his session on Duff. If he pressed the forward key while working in Conan, he would move to his session on Thor.

The **Change Backward Switch** and **Change Forward Switch** commands define keys used to switch sessions without returning to local mode. Backward and forward switch keys must be explicitly defined. To specify a control character, use escaped hex (\xx). The example below sets Ctrl-B (ASCII character 0x02) as the backward switch character and Ctrl-Z (ASCII character 0x1a) as the forward switch character.

Figure 5-6: Defining Switches

```
Local>> CHANGE BACKWARD SWITCH \02
Local>> CHANGE FORWARD SWITCH \1a
```

Note: *The MSS intercepts and processes switch keys; it does not pass them to the remote host.*

5.2.2.3 Disconnect and Resume

Users need a method of controlling and disconnecting sessions from local mode. For example, if a session on a remote host freezes or hangs while executing code, the user can exit the session using the Break key, then terminate the connection by entering the **Disconnect** command at the **Local>** prompt. A user may resume a session after returning to local mode by entering the **Resume** command. Both commands can affect any active sessions, not just the current session.

5.2.2.4 Session Limits

The number of active sessions a user can have on the MSS is limited by three factors: available server memory resources, a server-wide limit, and a port-specific limit. The absolute maximum number of sessions for the MSS is eight. To reduce the limit further, enter the **Change Session Limit** command followed by a number from one to seven.

5.2.3 Status Displays

The commands listed in this section display information about the current configuration and operating status of the MSS. The following sections describe what a user will see when typing the **Show** commands in interactive (local) mode.

5.2.3.1 Show 80211

Show 80211 displays the current 802.11 (wireless Ethernet) networking settings, including MAC address, ESSID, network mode, channel number, length of the current WEP key, and the current WEP index number. These settings are effective whenever there is a compatible wireless LAN PC card in one of the MSS PC card slots.

You can also enter **Show 80211 Antenna** to display the card's current antenna settings, and **Show 80211 Power** to display the current power settings.

5.2.3.2 Show Hostlist

Show Hostlist displays the current contents of the host table used for multihost mode connections. Host entries are numbered from 1 to 12.

5.2.3.3 Show IPsecurity

Show IPsecurity displays the current TCP/IP security table, if one exists. Addresses or ranges of addresses are listed according to the kind of restrictions placed upon them.

5.2.3.4 Show Ports

Show Ports displays the configuration and connection status of the specified serial port, including settings such as flow control, baud rate, parity, and default hosts. In addition, it shows the status of DSR and DTR serial signals, port access type, and login status. Errors are summarized, although in less detail than in the **Show Server Counters** display.

5.2.3.5 Show RS485

Show RS485 displays the current settings for RS-485 serial connections, including wire mode (two-wire or four-wire), termination, and driving of the TX (transmit) signal.

Note: *This command is only valid on the MSS-VIA and the MSS4.*

5.2.3.6 Show Server Bootparams

Show Server Bootparams displays MSS identification and boot procedure information. The first lines display the MSS version, hardware address, network name and node number, identification string, and how long the MSS has been running. You will also see the software and ROM versions, configured loadhost, and startup file name.

5.2.3.7 Show Server Characteristics

Show Server Characteristics displays network-related server identification information including the MSS hardware address, node address, IP address, domain, any configured gateways and nameservers, and the subnet mask. In addition, it shows inactivity and retransmission limits, password restrictions, and the types of incoming logins permitted.

5.2.3.8 Show Server Counters

Show Server Counters displays quantitative information about send and receive errors. It also displays error information for the Ethernet and TCP/IP protocols that can be used to diagnose network transmission problems.

5.2.3.9 Show Session

Show Session displays information about current sessions including each active port, user, and type of session.

5.2.3.10 Show Users

Show Users displays the name, port number, and connection status of all current users, or a specified user.

5.3 Disk Management

The MSS contains three filesystems:

/flash Flash is re-writeable memory that allows you to customize your MSS. Any data that you want the MSS to save after it is rebooted should be stored on the Flash disk.

/ram The RAM disk stores temporary information for the MSS. The MSS will hold information stored on this disk until it is turned off or rebooted. At startup, the RAM disk will be empty. FTP connections automatically use the RAM disk as the default working directory.

/rom The ROM disk is read-only and cannot be modified by users.

In addition to the onboard Flash disk, the PC card slots (installed on certain MSS models) can be used with ATA Flash cards for portable storage of local MSS files.

For more details on creating and managing files, read the **Disk** command section in the *MSS Reference Manual*.

5.3.1 Flash Disk

The MSS contains a Flash disk (/flash), rewriteable memory that allows you to customize your MSS. Any data that you want the MSS to save after it is rebooted should be stored on the Flash disk.

> **Note:** *If there is a power glitch during rewrite, you can lose the entire contents of the Flash disk. Therefore, it is a good idea to back up any important files to an ATA flash card or to another server.*

The **Disk** commands can be used to manage files on the Flash disk. For example, the following command creates a new directory on the Flash disk that could be used for custom application files:

Figure 5-7: Creating a New Directory on the Flash Disk

```
Local>> DISK MKDIR /flash/customapps/
```

To view all of the files and directories currently on the Flash disk, enter the **Disk Ls** command with or without flags. The following example will display all the files as well as the modification date, size, owner, and permissions:

Figure 5-8: Listing Directory Contents

```
Local>> DISK LS -l /flash
```

5.3.2 ATA Flash Cards

Once an ATA card is formatted, the card can be used the same as the on-board MSS Flash disk. Files on the card can be referenced as “/pccard1/<directory>/<filename>” for cards installed in the top slot or “/pccard2/<directory>/<filename>” for cards installed in the bottom slot.

The **Disk** commands described above and in the *MSS Reference Manual* can also be used with an ATA Flash card. For example, to back up a Flash disk file (data.txt) onto an ATA card in the top slot, use the following commands to create a backups folder on the card and to copy the desired file into that folder:

Figure 5-9: Backing Up Files onto an ATA Card

```
Local>> DISK MKDIR /pccard1/backups/
Local>> DISK CP /flash/customapps/data.txt /pccard1/backups
```

The maximum number of files and directories (total sum) that can fit on the card is a function of the size of the card: divide the size of the card by 5k (5120 bytes). This assumes that the average size of all the files that will fill up the card will be smaller than 5k.

Data can be corrupted if power is lost in the middle of a write (for example, if the cord is pulled). If the **Disk Sync** command is issued and power is removed after the command is completed, data will be stored correctly on the card. Likewise, there should be no problems with data integrity if the **Initialize Delay 0** command is used to reboot the unit.

5.3.3 SDK

The Lantronix Software Developers Kit (SDK) allows you to customize the behavior of your MSS in more ways than are available via the standard command set. You can write programs for the MSS that handle serial and network data, and store the finished programs on the /flash disk so they always run when the MSS boots.

For more information on the Lantronix SDK, contact Lantronix directly.

5.4 Encrypted Sessions

The MSS supports encrypted connections from one MSS to another MSS, or from a Win32 PC to the MSS. For more information on using the MSS with Win32, contact Lantronix directly.

To configure an MSS-to-MSS encrypted session, set the same encryption password on both units. The password can be up to 7 alphanumeric or escaped hex (\xx) characters and is case-sensitive.

Figure 5-10: Setting the Encryption Password

```
Local>> CRYPT PASSWORD “giraffe”
```

After the encryption password has been configured, reboot both units. Establish an encrypted session to either one of the unit’s local prompts or to a serial port using the following command:

Figure 5-11: Establishing an Encrypted Connection

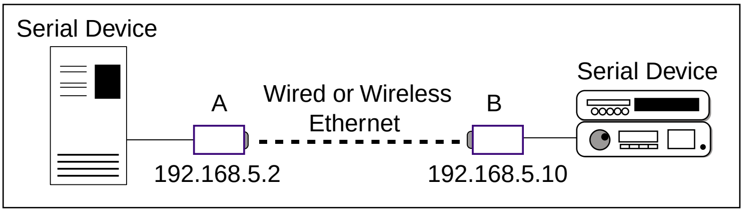
```
Local_1> TELNET n.n.n.n:2100Y
or
Local_1> TELNET n.n.n.n:2101Y
```

The first example shows the command to connect to the unit’s local prompt. The second example shows how to connect directly to the first serial port (for other ports, substitute the last 1 with the desired port number). The “Y” environment string specifies that the connection should be encrypted.

5.5 Serial Tunnel

Two MSS servers can be connected to emulate a direct serial connection across a LAN or WAN. Servers connected in this way can pass data only—they will not be able to pass status signals (DSR/DTR, RTS/CTS, etc.) or preserve timing between characters. The basic network configuration for this virtual serial line is shown in Figure 5-12.

Figure 5-12: Back-to-Back MSS Connections



Note: *Because each MSS can have multiple attached serial devices, there can be up to four active serial tunnels at one time. For example, a second serial device on MSS_A above could form a second serial tunnel to another serial device on MSS_B.*

For more information on environment strings, which are used in the following sections to create serial tunnels, see Table 5-1 on page 5-3.

5.5.1 TCP Configuration

Assuming the MSS network and serial port parameters have been configured properly, and *n* represents the port number of the attached device for that MSS, the two Servers would be configured as follows:

MSS_A

```
Local>> CHANGE PORT n DEDICATED TCP  192.168.5.10:3001T
Local>> CHANGE PORT n AUTOSTART ENABLED
```

MSS_B

```
Local>> CHANGE PORT n ACCESS REMOTE
Local>> CHANGE PORT n DEDICATED NONE
Local>> CHANGE PORT n AUTOSTART DISABLED
```

Note: *If the Servers are on different IP subnets, configure the default gateway on each unit with the* ***Change Gateway*** *command.*

Repeat the above steps for each additional serial tunnel.

The above commands create a raw (8-bit clean) TCP connection between the specified serial ports of the two Servers once the units have been power-cycled. The commands for the specified **MSS_A** ports ensure that they will automatically connect to the specified **MSS_B** ports each time the **MSS_A** is booted. The commands for **MSS_B** ensure that it is always available to accept connections from **MSS_A**.

5.5.2 UDP Configuration

When the UDP protocol is used, there is no connection; each MSS serial port must be told explicitly which host it is allowed to accept packets from. For UDP, each MSS port has to be configured to both send packets to and accept packets from the other MSS.

MSS_A

```
Local>> CHANGE PORT n DEDICATED TCP 192.168.5.10:4096U
Local>> CHANGE PORT n AUTOSTART ENABLED
Local>> CHANGE PORT n ACCESS DYNAMIC
```

MSS_B

```
Local>> CHANGE PORT n DEDICATED TCP 192.168.5.2:4096U
Local>> CHANGE PORT n AUTOSTART ENABLED
Local>> CHANGE PORT n ACCESS DYNAMIC
```

Repeat the above steps for each additional serial tunnel.

Setting up Dedicated hosts ensures that the specified ports will always talk only to each other. Enabling Autostart for both ports enables one MSS to send data to the other MSS without having to wait for a serial carriage return to start the session. The second MSS knows exactly which other MSS to accept connections from. Finally, when Autostart is enabled, the access mode must be either Local or Dynamic (Dynamic is more flexible).

5.6 Multihost Mode

Multihost mode sets up a data pipe between one of the serial devices attached to the MSS and multiple hosts on the network. Data from a network host goes out of the specified MSS serial port, and data from the serial port is sent to all connected network hosts. The MSS does not alter the data in any way, it merely forwards the data from one point to another.

There are a few important things to note about multihost connections:

- The MSS attempts to send data in the order it is received. That is, it reads in and sends data from one host before reading in data from another host.
- The MSS will ping TCP and UDP hosts before sending connect attempts to make sure the remote hosts are alive. If they are alive, the MSS connects for real and passes the data. If not, the MSS will retry later. Similarly, if one of the host connections is terminated prematurely, the MSS will attempt to reconnect at preset intervals.

Note: *Retry affects the data flow to all hosts, so you should remove unreliable hosts from the host list.*

- If a host’s flow control or other settings block the MSS from sending, the MSS will skip that host and send the data to the other hosts. This will result in data loss for the unavailable host.
- When one of the MSS serial ports logs out, all host sessions are disconnected, leaving the port idle.

5.6.1 Enabling Multihost Mode

To configure one of the MSS serial ports for a dedicated multihost connection, use the **Change Dedicated** command with **Hostlist** as the host name.

Figure 5-13: Enabling Multihost Mode

```
Local>> CHANGE PORT n DEDICATED HOSTLIST
Local>> LOGOUT PORT
```

When you enable a dedicated connection, the MSS disables local mode hotkeys for session manipulation.

5.6.2 Adding Hosts

The host list can include up to 12 host entries in any combination of TCP (raw, Telnet, and Rlogin) and UDP addresses.

Figure 5-14: Adding Entries to the Host Table

```
Local>> CHANGE PORT n DEDICATED HOSTLIST
Local>> HOSTLIST ADD TCP 192.0.1.35:5000T
Local>> HOSTLIST ADD UDP 192.0.2.255:5500
```

In the example, the UDP host entry is actually a broadcast IP address. Data is sent to all hosts on that particular subnet.

5.6.3 Removing Hosts

To remove an entry from the host table, use the **Show Hostlist** command to find out its entry number, then use the **Hostlist Delete** command to delete it.

Figure 5-15: Removing Entries from the Host Table

```
Local>> SHOW HOSTLIST
1 192.73.0.233:5000
2 192.0.1.176:5500
3 192.0.4.255:6000
Local>> HOSTLIST DELETE 2
```

5.7 Modem Emulation Mode

In modem emulation mode, the MSS presents a modem interface to the attached serial device: it accepts AT-style modem commands and handles the modem signals correctly. The MSS forms a network connection based on the ATDT commands issued from the serial device.

Normally there is a modem connected to a PC and a modem connected to some other remote machine. A user must dial from his PC to the remote machine and accumulate phone charges for each connection. With the MSS in modem mode, you can replace your modems with MSS units and use an Ethernet connection instead of a phone call, all without having to change communications applications. You can then connect to any remote machine that has an MSS without making potentially-expensive phone calls.

Note: *If the MSS is in modem emulation mode and the serial port is idle, the MSS can still accept network TCP connections to the serial port.*

To use modem mode, enable modem emulation and set your MSS for Autostart using **A** as the autostart character. This triggers the MSS to enter modem mode whenever it sees a modem-style **AT** command.

Figure 5-16: Enabling Modem Emulation Mode

```
Local>> CHANGE MODEM EMULATION ENABLED
Local>> CHANGE AUTOSTART CHARACTER “A”
Local>> LOGOUT PORT 1
```

As soon as someone types an **AT** command, the MSS will enter modem mode and begin processing the **AT** commands. While in modem mode, the MSS will not display a command line prompt.

5.7.1 Modem Mode Commands

The following commands are only available when the serial port is in Modem Emulation mode—they will have no effect when entered at the **Local>** prompt.

Table 5-2: Modem Mode Commands

Command	Function
AT?	Help; gives list of valid AT commands.
ATC <command>	Pass-through to normal command line interface.. **Ex:** `ATC CH NAMESERV 192.0.1.76`
ATDT <ipaddress>	**Ex:** `ATDT 192.0.55.22:3001T` **Ex:** `ATDT 192000055022:3001T` Users can specify sockets as well; in the examples, **:3001T** tells the MSS to form a raw TCP connection to socket 3001.

Table 5-2: Modem Mode Commands, cont.

Command	Function
ATE	Echo mode off (ATE0) or on (ATE1, the default).
ATH	Disconnects the network session.
ATI	Displays modem version information.
ATQ	Result codes on (ATQ0, the default) or off (ATQ1).
ATS	Allows serially-attached devices to control how the MSS accepts a network call. ATS0=0 will cause the MSS to send the RING string to the serial device when it receives a network connection request. The serial device must reply with the ATA string. ATS0=1 allows the MSS to automatically accept network connections (the default).
ATV	Displays result codes. There are four options: ATV0 = text codes, unknown commands cause an error. ATV1 = numeric codes, unknown commands cause an error. ATV2 = numeric codes, discard unknown commands. ATV3 = text codes, discard unknown commands.
ATZ	Accepted but ignored.
AT&F	Resets modem NVR to factory default settings.
AT&W	Writes modem settings to NVR.
AT&Z	Restores modem settings from NVR.
+++	Returns the user to the command prompt when entered from the serial port during a remote host connection.

Multiple commands can be entered on the same line (for example, `ATE0Q1V0` will be processed the same as if each command were entered separately). However, if the MSS encounters a command that it doesn’t recognize, it will ignore the whole command line. For this reason, you should enter only one command per line.

5.7.2 Wiring Requirements

Serial signals work differently when one or more of the MSS serial ports is in modem mode. First, the MSS will enable DTRWait and will not drive DTR until a valid connection is made with the ATDT command (see Section 5.7.1). Second, the MSS will drop DTR whenever the TCP session is disconnected. DSRLogout is enabled implicitly. The MSS DTR signal will be used as a simulated CD signal to the attached serial device.

When using an MSS serial port in modem mode:

- The serial device's **DTR** goes out to BOTH its own **DSR in** and the MSS **DSR in**. When the device asserts its DTR, it will see its DSR asserted. That way the device thinks that the "modem" (the MSS) is ready to accept commands all the time and the MSS can close the network connection when the device disconnects.

- The MSS **DTR out** goes to the serial device's **CD in**. That way the MSS can signal the serial device that there is a valid connection, and the serial device will know it can send data to the remote device.

5.8 COM Port Redirector

The Lantronix Com Port Redirector application allows PCs to share modems and other serial devices connected to an MSS using Microsoft Windows applications.

The Redirector intercepts communications to specified PC COM ports and sends them over a network connection to one of the MSS serial ports. This enables the PC to use an MSS serial port as if it were one of the PC COM ports.

Note: *The redirector works over 802.11 connections.*

The COM Port Redirector software is included on the distribution CD-ROM.

A: Contact Information

If you are experiencing an error that is not listed in *Appendix B* or if you are unable to fix the error, contact your dealer or Lantronix Technical Support at 800-422-7044 (US) or 949-453-3990. Technical Support is also available via Internet email at **support@lantronix.com**.

A.1 Problem Report Procedure

When you report a problem, please provide the following information:

- Your name, and your company name, address, and phone number
- Lantronix MSS model number
- Lantronix MSS serial number
- Software version (use the **Show Server** command to display)
- Network configuration, including the information from a **Netstat** command
- Description of the problem
- Debug report (stack dump), if applicable
- Status of the unit when the problem occurred (please try to include information on user and network activity at the time of the problem)

A.2 Full Contact Information

Address: 15353 Barranca Parkway, Irvine, CA 92618 USA
Phone: 949/453-3990
Fax: 949/453-3995
World Wide Web: http://www.lantronix.com

North American Direct Sales: 800/422-7055
North American Reseller Sales: 800/422-7015
North American Sales Fax: 949/450-7232
Internet: sales@lantronix.com

International Sales: 949/450-7227
International Sales Fax: 949/450-7231
Internet: intsales@lantronix.com

Technical Support: 800/422-7044 or 949/453-3990
Technical Support Fax: 949/450-7226
Internet: support@lantronix.com

B: Troubleshooting

This Appendix discusses how you can diagnose and fix errors quickly without having to contact a dealer or Lantronix. It will help to connect a terminal to the serial port while diagnosing an error to view any summary messages that are displayed.

When troubleshooting, always ensure that the physical connections (power cable, network cable, and serial cable) are secure.

Note: *Some unexplained errors may be caused by duplicate IP addresses on the network. Make sure that your MSS IP address is unique.*

B.1 Power-up Troubleshooting

Problem situations and error messages are listed in Table B-1. If you cannot find an explanation for your problem, try to match it to one of the other errors. If you cannot remedy the problem, contact your dealer or Lantronix Technical Support.

Table B-1: Power-up Problems and Error Messages

Problem/Message	Error	Remedy
The MSS is connected to a power source, but there is no LED activity.	The unit or its power supply is damaged.	Contact your dealer or Lantronix Technical Support for a replacement.
The MSS is unable to complete power-up diagnostics.	This generally indicates a hardware fault. One of the LEDs will be solid red for three seconds, followed by one second of another color.	Note the blinking LED and its color, then contact your dealer or Lantronix Technical Support. The MSS will not be operational until the fault is fixed.
The MSS completes its power-up and boot procedures, but there's no noticeable serial activity.	There is a problem with the serial connection or the set-up of the serial device.	Check the terminal setup and the physical connections, including the cable pinouts (see *Appendix C*). Try another serial device or cable, or cycle power on the MSS.
	A rapidly-blinking OK LED may signal boot failure.	Reboot the unit. When the MSS is running normally, the OK LED blinks every two seconds.

Table B-1: Power-up Problems and Error Messages, cont.

Problem/Message	Error	Remedy
The terminal shows a Boot> prompt rather than a Local> prompt.	The MSS is not connected properly to the Ethernet.	Ensure that the MSS is firmly connected to a functional and properly-terminated network node.
	The MSS Ethernet address is invalid.	The MSS Ethernet address is located on the bottom of the unit. Use the **Change Hardware** command to set the correct address, then reboot.
	Init Noboot command was entered.	See *Entering Commands at the Boot Prompt* on page B-4.
The MSS passes power-up diagnostics, but attempts to download new Flash ROM code from a network host.	If the OK LED blinks rapidly, the Flash ROM code may be corrupt. If you did not request a TFTP boot, the flash ROM code is corrupt. The unit will remain in boot mode.	Reboot the unit. If you get the same message, you will need to reload Flash ROM. See *Reloading Software* on page D-2.

B.2 DHCP Troubleshooting

If the unit is unable to get the IP address from the DHCP server, check these areas:

Table B-2: DHCP Troubleshooting

Area to Check	Explanation
DHCP is enabled on the MSS.	Use the **Change Server DHCP Enabled** command. If you manually enter an IP address, DHCP is automatically disabled.
The DHCP server is operational.	Check to see that the DHCP server is on and is functioning correctly.
The MSS is getting its IP address from the DHCP server.	Refer to the **DHCP Manager** on your DHCP server for information about addresses in use. If the DHCP server doesn’t list your MSS IP address, there may be a problem.

B.3 BOOTP Troubleshooting

If the BOOTP request is failing and you have configured your host to respond to the request, check these areas:

Table B-3: BOOTP Troubleshooting

Area to Check	Explanation
BOOTP is in your system’s **/etc/services** file.	BOOTP must be an uncommented line in **/etc/services**.
The MSS is in the loadhost’s **/etc/hosts** file.	The MSS must be in this file for the host to answer a BOOTP or TFTP request.
The download file is in the correct directory and is world-readable.	The download file must be in the correct directory and world-readable. Specify the complete pathname for the download file in the BOOTP configuration file, or add a default pathname to the download filename.
The MSS and host are in the same IP network.	Some hosts will not allow BOOTP replies across routed IP networks. Either use a host running a different operating system or put the MSS in the same IP network as the host.

B.4 RARP Troubleshooting

If the unit is unable to get an IP address using RARP, check these areas:

Table B-4: RARP Troubleshooting

Area to Check	Explanation
The MSS name and hardware address in the host’s **/etc/ethers** file.	The MSS name and hardware address must be in this file for the host to answer a RARP request.
The MSS name and IP address in the **/etc/hosts** file.	The MSS name and IP address must be in this file for the host to answer a RARP request.
The operating system.	Many operating systems do not start a RARP server at boot time. Check the host’s RARPD documentation for details, or use the **ps** command to see if there is a RARPD process running.

B.5 Modem Configuration Checklist

Most modem problems are caused by cabling mistakes or incorrect modem configuration. However, the following items should be verified after any modem configuration, and re-checked when there is modem trouble.

- The modem must be configured to disconnect immediately when DTR is de-asserted.
- The modem must assert CD (or DSR, if connected) when connected to another modem. It must not assert CD when disconnected. The modem may optionally assert CD during outbound dialing.
- The modem and MSS must agree on the flow control method and baud rate scheme.
- The modem must not send result codes or messages to the MSS except optionally during outgoing calls.
- The modem should be set to restore its configuration from non-volatile memory when DTR is dropped.
- The modem should be configured to answer the phone if incoming connections are to be supported. Generally this is done with the **ats0=1** command.
- The modem should not be configured to answer the phone unless the MSS asserts DTR.
- Modem control must be enabled on the MSS. Using modems on ports without modem control enabled will lead to security problems.
- The MSS Autobaud feature should be enabled only when required.

B.6 Entering Commands at the Boot Prompt

If the Boot> prompt appears on the serial console instead of the **Local>** prompt, one of two things may be wrong. Either the MSS does not have enough information to boot, or the network or flash reloading procedure has failed. If pressing the **Return** key does not display a prompt, press any other key. The Boot> prompt should appear.

If the MSS does not have enough information to boot, or the network or flash reloading procedure has failed, it will print a message to the console and wait ten seconds for serial port activity. If the MSS detects serial port activity, it will continue booting provided the flash is good. However, if the user presses a key during that time period, the MSS will display the Boot> prompt.

Note: *If you see the message “Will attempt another download in x minutes,” press any key for the Boot> prompt.*

A series of commands called Boot Configuration Program (BCP) commands can be entered at the Boot> prompt to configure the MSS. These commands are a subset of the entire MSS command set. For example, a typical TCP/IP configuration might use the following commands:

Figure B-1: BCP Command Examples

```
Boot> Change IPADDRESS 192.0.1.229
Boot> Change SOFTWARE /tftpboot/MSS4.SYS
Boot> Change LOADHOST 192.0.1.188
Boot> Change SECONDARY 192.0.1.22
Boot> FLASH
% Initialization begins in 5 seconds.....
```

These commands set the Server's address, the software loadfile, and the loadhost's IP address (as well as that of a backup loadhost). The server then reboots using the **Flash** command and will attempt to load the file MSS4.SYS from the host at 192.0.1.188.

Flush NVR

This command is used to restore the MSS's non-volatile RAM to its factory default settings. It will reset everything that is configurable on the server, including the unit's IP address.

Flash

This command will force the MSS to download new operational code and reload it into Flash ROM. This is necessary when a new version of software is released and you wish to upgrade your unit. If the server cannot download the file, the code in Flash ROM will still be usable.

Help

Displays a one-page summary of available commands and what they do.

Change Bootgateway

Specifies a server to send packets to when downloading code. The packets will be addressed to the loadhost, but will be physically set to the bootgateway host.

Init 451

Reboots the MSS after it has been configured. If the MSS can find and load the specified software loadfile, it will restart itself with full functionality. If the loadfile is not found, the server will attempt to reload continuously. If there is an error, or if the console's **Return** key is pressed, the MSS will re-enter the Boot Configuration Program.

Change BOOTP {Enabled, Disabled}

Enables or disables the sending of BOOTP queries during the boot sequence. It is enabled by default.

Change DHCP {Enabled, Disabled}

Enables or disables the sending of DHCP queries during the boot sequence. It is enabled by default.

Change Hardware xx-xx-xx

Specifies the last three numbers of the server’s Ethernet address. The first three numbers will be supplied automatically.

The Ethernet address should have been set at the factory. Setting an incorrect address could cause serious network problems.

Change IPAddress ip_address

Specifies this server’s IP address. Uses the standard numeric format.

Change Loadhost ip_address

Specifies the host to attempt to load the file from. The IP address should be in standard numeric format (no text names are allowed).

Change RARP {Enabled, Disabled}

Enables or disables the sending of RARP queries during the boot sequence. It is enabled by default.

Change Secondary ip_address

Specifies a backup loadhost. The IP address should be in standard numeric format (no text names are allowed). The backup loadhost will be queried if the primary host cannot load the server.

Change Software filename

Specifies the name of the file to load. The MSS will automatically add **.SYS** to the filename you specify. Note that all protocols must have a filename specified (either the default or set by the user). For more information, see *Appendix D*.

TCP/IP users must use the Software option to specify the loadhost, the loadfile, and their own network address.

TFTP users can specify a complete path name (up to 31 characters) if the file is located in a directory other than the default.The case of the filename must match that of the filename loaded onto the host computer.

Show Server

Use this command when issuing other commands to view the current MSS setup.

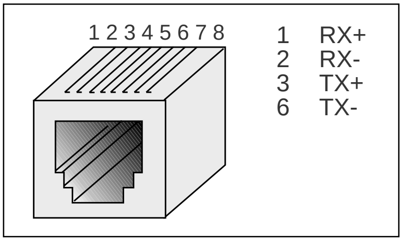
C: Pinouts

In the following diagrams, unlabeled pins are not connected.

C.1 Ethernet Connectors

The MSS uses a standard Ethernet pinout. The figure below shows the MSS RJ45 Ethernet connector pin connections.

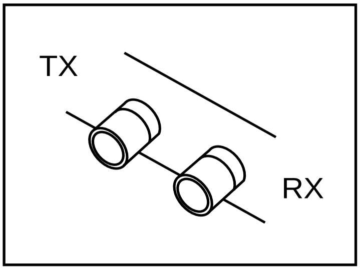
Figure C-1: RJ45 Ethernet Connector



C.1.1 Fiber Link Ethernet

The MSS4-SFP and MSS4-DFP also include a 100BASE-FX fiber optic Ethernet connector. The figure below shows the fiber link connector pin connections, which use the duplex ST connector interface (one transmitter, one receiver).

Figure C-2: Fiber Optic Connectors



C.2 MSS4 Serial Connectors

The MSS4 has four serial ports. The MSS4-D models have DB9 connectors, while the MSS4-S models have screw terminal blocks.

C.2.1 Screw Terminal Block

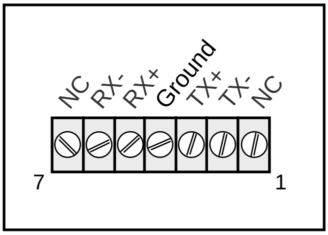
The following sections show the pin connections of the MSS4 screw terminal blocks, which provide dual RS-232/RS-485 serial ports.

The default serial port settings are 9600 baud, 8 bits, no parity, and 1 stop bit.

C.2.1.1 RS-485 Screw Terminal

The following shows the pin connections of the MSS4 RS-485 screw terminal block.

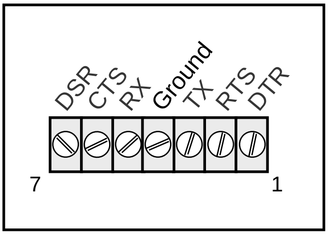
Figure C-3: RS-485 Screw Terminal Block



C.2.1.2 RS-232 Screw Terminal

The following figure shows the pin connections of the MSS4 RS-232 screw terminal block.

Figure C-4: RS-232 Screw Terminal Block.



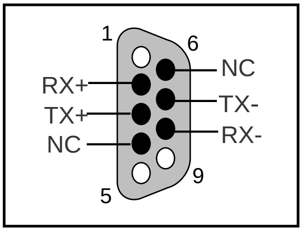
C.2.2 DB9 Connectors

The following sections show the pin connections of the MSS4 DB9 connectors, which provide dual RS-232/RS-485 serial ports.

C.2.2.1 RS-485 DB9 Connectors

The MSS4 DB9 connector provides an RS-485 serial port.

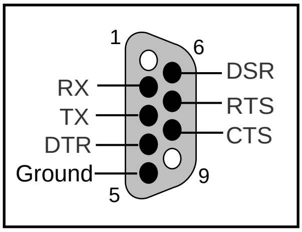
Figure C-5: DB9 RS-485 Serial Connector



C.2.2.2 RS-232 DB9 Connectors

The MSS4 DB9 connector also provides an RS-232 serial port.

Figure C-6: DB9 RS-232 Serial Connector



C.3 MSS4 PC Card Slots

The MSS4 PC card slots, available on the -DFP and -SFP models, accept Type I/II PC cards. The bottom slot also accepts Type III cards. The MSS4 software supports IEEE 802.11 wireless networking PC cards, modem cards, and a selection of ATA storage cards.

For the most current information on which PC card technologies are supported and which cards are compatible with the MSS4, please refer to the Lantronix web site.

Note: *Changes in firmware revision may affect compatibility.*

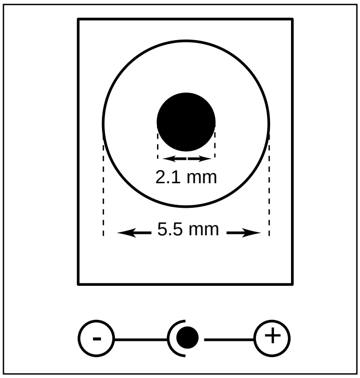
C.4 MSS4 Power Connectors

Power is supplied to the MSS using **one** of the connectors mentioned in this section.

C.4.1 Power Jack

The MSS4 ships with a standard barrel power jack whose inner conductor is positive.

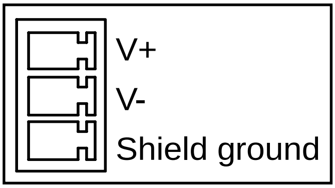
Figure C-7: Power Jack Connector



C.4.2 Screw Block Power

The MSS4 also has a 9-30V DC screw block power jack.

Figure C-8: Screw Block Power



D: Updating Software

D.1   Obtaining Software

A current software file (MSS4.SYS) is available on the distribution CD. You can obtain software updates and release notes for the MSS from the Lantronix World Wide Web site (www.lantronix.com), or by using anonymous FTP through the Internet (ftp.lantronix.com).

D.1.1   Via the Web

The latest version of MSS4.SYS can be downloaded from the Technical Support area of the Lantronix Web site.

> **Note:** *As a result of Netscape Navigator’s configuration, it may try to open the file as an ASCII text file. To avoid this, hold down the shift key when choosing the software file.*

D.1.2   Via FTP

The MSS software resides on the Lantronix FTP server (ftp.lantronix.com). Most of these files are binary data, so the binary option must be used to transfer the files. All released files are in the **pub** directory. Always download the README file in the pub directory before downloading anything else; it contains a list of available software files.

To log into the FTP server, enter a username of **anonymous** and enter your full email address as the password. The following text will be displayed:

Figure D-1: Sample FTP Login

```
230-Welcome to the Lantronix FTP Server.
230-
230-IMPORTANT: Please get the README file before proceeding.
230-IMPORTANT: Set BINARY mode before transferring executables.
220-
230-Direct questions to support@lantronix.com or 800-422-7044 (US) or
949-453-3990
230-
230 Guest login ok, access restrictions apply.
Remote system type is [your type will be displayed here].
ftp>
```

D.2 Reloading Software

The MSS stores software in Flash ROM to control the initialization process, operation, and command processing. The contents of Flash ROM can be updated by downloading a new version of the operational software via NetWare, TCP/IP, or MOP. Regardless of which protocol is used to update Flash ROM, the following points are important:

- The Flash ROM software file name, **MSS4.SYS**, should not be changed.
- The download file should be world-readable on the host.
- There is a sixteen character length limit for the path name.
- There is a twelve character limit for the filename.
- Use the **List Server Boot** command to check settings before rebooting.

Note: *It is important to check MSS settings before using the* ***Initialize Reload*** *command to ensure that you are reloading the correct software file.*

D.2.1 Reloading Sequence

If DHCP, BOOTP, or RARP is enabled on the MSS, the MSS will request assistance from a DHCP, BOOTP, or RARP server before starting the download attempts. The MSS will then try TFTP, NetWare, and MOP booting (in that order) provided that it has enough information to try each download method.

Downloading and rewriting the Flash ROM will take approximately two minutes from the time the **Initialize** command is issued. If the download file cannot be found or accessed, the MSS can be rebooted with the code still in Flash ROM. The OK/ACT LED will blink quickly while the MSS is booting (and reloading code) and then slowly when it returns to normal operation.

Note: *If you experience problems reloading Flash ROM, refer to Troubleshooting Flash ROM Updates on page D-3.*

D.2.1.1 TCP/IP

Before the MSS downloads the new software, it will send DHCP, BOOTP, and/or RARP queries (all are enabled by default). Next, the MSS will attempt to download the MSS4.SYS file using TFTP (Trivial File Transfer Protocol).

Note: *EZWebCon can also be used to reload software.*

If a host provides DHCP, BOOTP, or RARP support, it can be used to set the MSS IP address (all methods) and loadhost information (BOOTP and RARP only).

Some BOOTP and TFTP implementations require a specific directory for the MSS4.SYS file. See your host’s documentation for instructions.

To manually configure the MSS IP parameters for software reload when running operational software (not BCP mode), use the following commands.

Figure D-2: Configuring TCP/IP Reload

```
Local> SET PRIVILEGED
Password> SYSTEM (not echoed)
Local>> CHANGE IPADDRESS nnn.nnn.nnn.nnn
Local>> CHANGE SOFTWARE “/tftpboot/MSS4.SYS”
Local>> CHANGE LOADHOST nnn.nnn.nnn.nnn
Local>> SHOW SERVER BOOT
Local>> INITIALIZE RELOAD
```

Note: *For instructions on how to log into the MSS to enter these commands, see the Getting Started chapter.*

The path and filename are case-sensitive and must be enclosed in quotation marks. When attempting to boot across an IP router, you must configure the router to proxy-ARP for the MSS, or use the bootgateway feature. For more information, see **Bootgateway** in the *Commands* chapter of the *MSS Reference Manual* located on the CD-ROM.

D.2.1.2 MOP

The MSS4.SYS filename is the only parameter that the MSS needs to reload via MOP. Make sure the service characteristic is enabled on the host's Ethernet circuit, copy the MSS4.SYS file to the MOM$LOAD directory, and reload the MSS using the **Initialize Reload** command. Be sure to use binary mode for any file transfers.

D.3 Troubleshooting Flash ROM Updates

Many of the problems that occur when updating the Flash ROM can be solved by completing the following steps:

Table D-1: Flash ROM Troubleshooting

Protocol	Area to Check
TFTP	Check the file and directory permissions. Ensure the loadhost name and address are specified correctly and that their case matches that of the filenames on the host system. Ensure the file and pathnames are enclosed in quotes to preserve case. Ensure that TFTP is enabled on the host; several major UNIX vendors ship their systems with TFTP disabled by default.

Table D-1: Flash ROM Troubleshooting

Protocol	**Area to Check**
MOP	Ensure that the Ethernet circuit must has the **service** characteristic enabled. Ensure that the MOM$LOAD search path includes the directory containing the MSS4.SYS file.

E: Specifications

E.1 Power Specifications

The MSS4 has a screw terminal power jack and a power cube adaptor. Specifications for the adaptor varies depending on your MSS4 model.

E.1.1 MSS4 Screw Terminal Power

The MSS screw terminal power jack requires 9-30 V DC.

E.1.2 MSS4-D/-S Adaptor

The MSS4-D and MSS4-S power cube adaptor has the following specifications:

Adapter input voltage:	110 V AC US, 220 V AC International
Adapter output voltage:	12 V DC
Operating current:	0.8A @ 12 V
Power consumption:	10 Watts maximum

E.1.3 MSS4-DFP/-SFP Adaptor

The MSS4-DFP and MSS4-SFP power cube adaptor has the following specifications:

Adapter input voltage:	110 V AC US, 220 V AC International
Adapter output voltage:	12 V DC
Operating current:	1.5A @ 12 V
Power consumption:	18 Watts maximum

E.2 Environmental Information

E.2.1 Temperature Limitations

Operating range:	5˚ to 50˚ C (41˚ to 122˚ F)
Storage range:	-40˚ to 66˚ C (-40˚ to 151˚ F)
Max temp change:	20˚ C (36˚ F) per hour

Rapid temperature changes may affect operation. Do not operate the MSS near heating or cooling devices, large windows, or doors that open to the outdoors.

E.2.2 Relative Humidity Limitations

Operating range:	10% to 90% noncondensing, 40% to 60% recommended
Storage range:	10% to 90% noncondensing

E.2.3 Altitude Limitations

Operating:	2.4 km (8,000 ft)
Storage:	9.1 km (30,000 ft)

When operating the MSS above 2.4 km (8,000 ft), decrease the operating temperature rating by 1.8˚C for each 1,000 m (1˚F for each 1,000 ft).

Warranty Statement

Lantronix warrants for a period of 5 YEARS from the date of shipment that each MSS4 Device Server supplied shall be free from defects in material and workmanship. During this period, if the customer experiences difficulties with a product and is unable to resolve the problem by phone with Lantronix Technical Support, a Return Material Authorization (RMA) will be issued. Following receipt of a RMA number, the customer is responsible for returning the product to Lantronix, freight prepaid. Lantronix, upon verification of warranty will, at its option, repair or replace the product in question, and return it to the customer freight prepaid. No services are handled at the customer's site under this warranty.

Lantronix warrants software for a period of sixty (60) days from the date of shipment that each software package supplied shall be free from defects and shall operate according to Lantronix specifications. Any software revisions required hereunder cover supply of distribution media only and do not cover, or include, any installation. The customer is responsible for return of media to Lantronix and Lantronix for freight associated with replacement media being returned to the customer.

Lantronix shall have no obligation to make repairs or to cause replacement required through normal wear and tear of necessitated in whole or in part by catastrophe, fault or negligence of the user, improper or unauthorized use of the Product, or use of the Product in such a manner for which it was not designed, or by causes external to the Product, such as, but not limited to, power or failure of air conditioning.

There are no understandings, agreements, representations or warranties, express 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

The information, recommendation, description and safety notations in this or other documents supplied by Lantronix are based on general industry experience and judgment with respect to such hardware and software. THIS INFORMATION SHOULD NOT BE CONSIDERED TO BE ALL INCLUSIVE OR COVERING ALL CONTINGENCIES. NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE OR MERCHANTABILITY, OR WARRANTIES ARISING FROM COURSE OF DEALING OR USAGE OF TRADE, ARE MADE REGARDING THE INFORMATION, RECOMMENDATIONS, DESCRIPTIONS AND SAFETY NOTATIONS CONTAINED HEREBY AND IN HARDWARE AND SOFTWARE SPECIFICATION DOCUMENTATION, OR INSTRUCTIONS SUPPLIED BY Lantronix. 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 (1) refund of buyer's purchase price for such affected products (without interest); (2) repair of such products, or (3) replacement of such products, provided however, that the buyer follows the procedures set forth herein

Warranty claims must be received by Lantronix within the applicable warranty period. A replaced product, or part thereof, shall become the property of Lantronix and shall be returned to Lantronix at the Purchaser's expense. **All returned material must be accompanied by a return material authorization number assigned by Lantronix**.

Declaration of Conformity

(according to ISO/IEC Guide 22 and EN 45014)

Manufacturer's Name: Lantronix

Manufacturer's Address: 15353 Barranca Parkway, Irvine, CA 92618 USA

Declares that the product:

Product Name: Device Server

Model Name/Number: MSS4

Conforms to the following standards or other normative documents:

Safety: EN60950:1988+A1, A2

EMC: EN55022:1998 class A
EN50082-1: 1992
IEC 801-2:1991/prEN55024-2:1992-4KV CD, 8KV AD
IEC 801-3:1992/prEN55024-3:1991-3V/M
IEC 801-4:1998/prEN55024-4:1992-0.5kV Signal Lines,
1kV Power Lines

Supplementary Information: *The product complies with the requirements of the Low Voltage Directive 72/23/EEC and the EMC Directive 89/336/EEC.*

Manufacturer's Contact: Director of Quality Assurance, Lantronix
15353 Barranca Parkway, Irvine, CA 92618 USA

General Tel: 949/453-3990
Fax: 949/453-3995

Index