Device Servers

For More Information:
For more information on this product and all of the products and services provided by Lantronix, please visit us at **www.lantronix.com**. For immediate needs, you may contact us directly at any of our corporate and regional headquarters. A complete listing of all our sales offices can be found at our web site.

Corporate Offices
15353 Barranca Parkway
Irvine, CA 92618
USA
949 453 3990
949 453 3995 fax
sales@lantronix.com

Europe, Middle East & Africa (EMEA)
Minervum 1707
4817 ZK Breda
The Netherlands
+31 (0) 76 565 8176
+31 (0) 76 565 8179 fax
eu_sales@lantronix.com

Pacific Rim
46 East Coast Road
East Gate #10-01
Singapore 428766
+65 447 4222
+65 344 0614 fax
asiapacsales@lantronix.com

Part Number: 900-193

LANTRONIX®

LANTRONIX®

Installation Guide

MSS Installation Guide

For MSS100 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.

DEC and LAT are trademarks of Compaq. Ethernet is a trademark of XEROX Corporation. NetWare is a trademark of Novell 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 **20 July, 2001**

Part Number: 900-193
Rev. B

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. The MSS achieves this by providing a serial port on one end and a 10/100BASE-T Ethernet I/O port on the other.

Throughout this manual, the MSS100 may be referred to as the **MSS** or as the **Server**.

1.1 MSS100 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 connects serial devices directly to a wired 10/100BASE-T Ethernet network.

- Ease of Use

  The MSS 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 and LAT 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 3-5.

- 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 Device Server 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.

1.2 Protocols

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

- TCP/IP

  Support includes Telnet, Rlogin, UDP, DNS, and WINS. The Telnet terminal protocol, supported on most UNIX systems, 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 Device Server Reference Manual.

- IPX/ SPX (NetWare)

  The MSS provides IPX/SPX access to the serial device from NetWare and any other IPX/SPX nodes. It allows users to download system files from NetWare hosts and log into the MSS via NetWare for remote configuration.

  The MSS supports all four NetWare frame types: Ethernet v2, Native mode, 802.2, and 802.2 SNAP.

- Local Area Transport (LAT)

  LAT is a protocol developed by Digital Equipment Corporation (DEC) for local network connections and is supported on most DEC operating systems. The MSS provides logins to remote hosts and host-initiated connections, as well as access to the MSS serial port from LAT hosts.

1.3 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.

1.4 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 the MSS in your situation.
- 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 *Device Server Reference Manual*, located on the CD-ROM in PDF format, provides the full MSS family command set as well as additional configuration information.

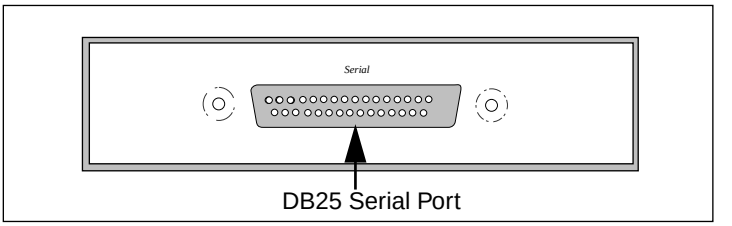
2: Installation

This chapter covers the installation of the MSS in an Ethernet network and the attachment of a serial device. Basic knowledge of networking installation is assumed. Read this chapter completely before continuing.

2.1 Components

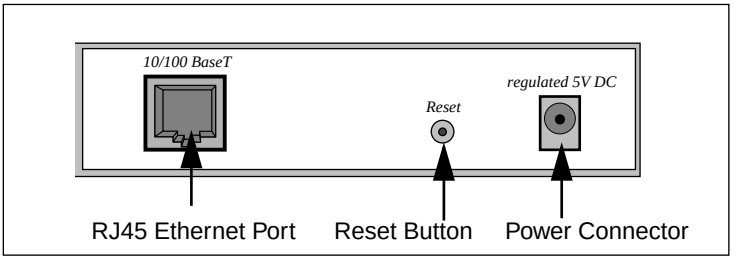
The MSS front panel has a male DB25 serial connector. The following figure shows an MSS front panel.

Figure 2-1: MSS Front Panel



The MSS rear panel has an RJ45 Ethernet connector, a reset button, and a power connector. The following figure shows an MSS rear panel.

Figure 2-2: MSS Rear Panel



Note: *When the reset button is pressed and held during the power up and boot procedures, the MSS returns to its factory default configuration.*

Five LEDs are located on the top of the unit. The following table explains their functions.

Table 2-1: MSS LEDs

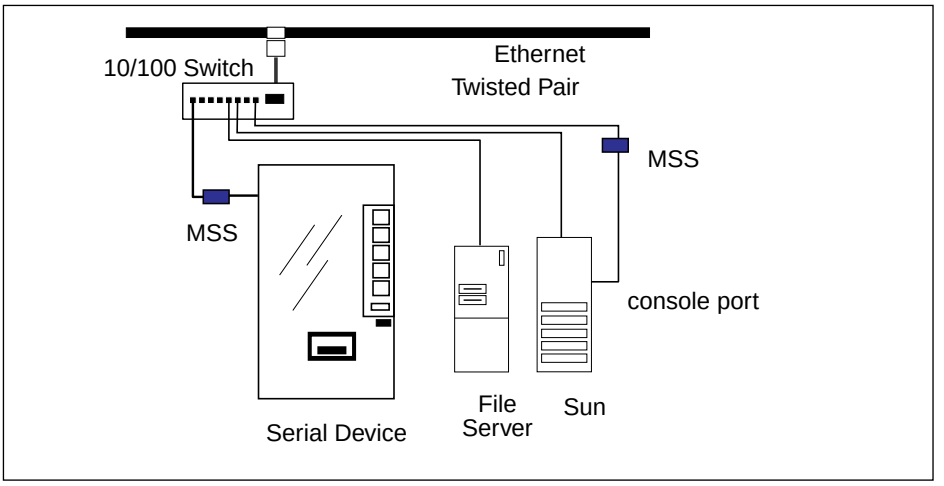
LED	Function
Power	Glows green when power is supplied to the MSS
Link	Glows green while the MSS is connected properly to a 10BASE-T or 100BASE-T Ethernet network
100	Glows green to indicate a 100BASE-T Ethernet connection
OK	Blinks yellow, green, or red to indicate MSS activity.
Serial	Blinks yellow, green, or red to indicate MSS activity.

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 Installation Procedure

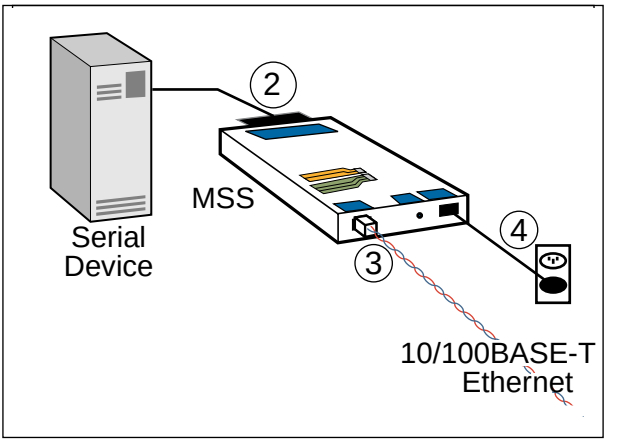
The MSS can be used to network-enable serial devices as shown in the figure below. Any device with a serial port can be connected to the network via an MSS.

Figure 2-3: MSS Network Layout



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

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



1 Select a location.

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 as listed in *Appendix D*.

2 Connect the MSS to an RS232-based serial device.

A Connect one end of a serial cable to the DB25 connector on the front of the MSS. You may want to use a serial terminal for the first connection both to ensure that your server is working and to configure the necessary network settings.

Note: *The serial port is initially set for 9600 baud, 8 data bits, one stop bit, and no parity.*

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

3 Connect the MSS to the Ethernet.

A Connect one end of a twisted-pair 10/100BASE-T cable to the Ethernet network via a switch or hub, depending on network topology.

B Connect the other end of the twisted-pair cable to the RJ45 Ethernet port on the back of the MSS. The MSS will autosense whether the attached Ethernet cable is 10BASE-T or 100BASE-T.

4 Supply power to the MSS.

A Connect one end of the power cable to the MSS power jack.

B Connect the power cube end of the power cable to a standard wall outlet.

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

- The MSS runs through a set of power-up diagnostics for approximately five seconds. The Power and Link LEDs should remain solid green. The Link LED should remain solid green. The OK and Serial LEDs should show varying patterns corresponding to the test being run.

Note: *The Power and Link LEDs should remain solid green if the unit is plugged in and there is a valid connection to a 10/100BASE-T network.*

- The MSS tries to obtain TCP/IP configuration information via DHCP, BOOTP, and/or RARP. This procedure takes approximately 45 seconds if no hosts answer the request. 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 unit is running normally, the **Power** LED should be solidly lit to indicate the unit is ON, the **Link** LED should be solidly lit to indicate a functioning Ethernet connection, and the **OK** LED should blink green once every two seconds.

5 Supply power to the serial device.

6 Verify that the MSS is working. There are a few ways to check:

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

B If you have connected a serial terminal to the MSS DB25 port, press the **Return** key. You should see several lines of start-up messages followed by a **Local>** prompt.

C If an IP address has been configured for the MSS, ping the MSS from a TCP/IP host. For more instructions, see the *IP Address Configuration* section in *Getting Started*.

Figure 2-5: Pinging the MSS

```
% ping XXX.XXX.XXX.XXX
```

3: Getting Started

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

- Incoming (Remote) Logins: EZWebCon is the preferred configuration method. Users can also use the internal HTTP server via a standard web browser.
- Serial Port Logins: Users can connect a terminal directly to the serial port, 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).

It is important to consider the following points before logging into and configuring the MSS:

- The MSS IP address must be configured before any TCP/IP functionality is available (see *IP Address Configuration* on page 3-2).
- Connecting a terminal to the serial port or logging into the remote console port does not automatically create privileged user status. You must use the **Set Privileged** command to configure the unit (see *Privileged User Status* on page 3-1).
- 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 Privileged User Status

Many MSS commands require privileged user (superuser) status. For example, only the privileged user can change server-wide or port-specific settings.

To become the privileged user, enter the following command. The default privileged password is **system**.

Figure 3-1: Set Privileged Command

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

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

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 Noprivilege** command.

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

Figure 3-2: Changing Privileged Password

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

3.2 IP Address Configuration

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

3.2.1 Using EZWebCon

Note: *If you have an older version of EZWebCon, refer to the Readme that was included with it.*

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

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 3-3). This process typically requires superuser privileges.

Figure 3-3: 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 3-4: 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 3-5: 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 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 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 3-6: Entering the IP Address at the Local Prompt

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

If the MSS encounters a problem with the Ethernet network, 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 a key during that time period, the MSS will display the Boot prompt at which you can enter the **Change IPaddress** command to set the unit's IP address.

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

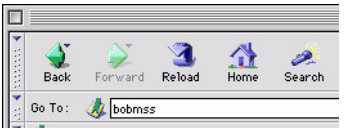
3.3 Incoming Logins

3.3.1 TCP/IP Logins

3.3.1.1 Web Browser Login and Configuration

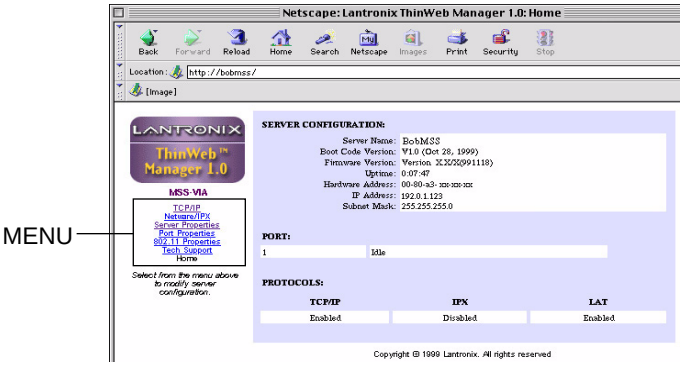
If your MSS has an IP address, you can log into it using a standard web browser with Java enabled. Simply type the MSS IP address or resolvable text name into the browser's URL/ Location field.

Figure 3-7: 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 as well as view statistics and other server information.

Figure 3-8: ThinWeb Manager Interface



3.3.1.2 EZWebCon Login and Configuration

EZWebCon enables users on TCP/IP networks to log into and configure the MSS. The program offers a simple interface that prompts the user 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 3-9: 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 3-10: An Rlogin Connection

```
% rlogin 192.0.1.88
```

3.3.2 Incoming LAT Logins

To get an MSS login prompt when connecting from a LAT host, use the command below. Substitute the last six digits of the MSS hardware address for xxxxxx.

Figure 3-11: LAT Login

```
$ SET HOST/LAT MSS_xxxxxx
```

3.3.3 Serial Port Logins

Attach a terminal to the serial port 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.*

3.3.4 Remote Console Logins

Users can configure the MSS via a single 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**.

Figure 3-12: 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
```

3.3.4.1 Changing the Login Password

The login password is required for remote console logins and when the MSS password protection feature is enabled. The default login password is **access**. To specify a new login password, use the **Change Loginpass** command and specify a new password of up to six alphabetic characters.

Figure 3-13: Changing the Login Password

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> CHANGE LOGINPASS "badger"
```

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

3.4 Outbound 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 3-14: 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 3-15: 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 the web browser interface or the EZWebCon graphical user interface, this chapter explains how to configure the MSS via the command line interface.

Note: *Instructions for using EZWebCon are included on the distribution CD-ROM. EZWebCon has on-line help to assist you with configuration.*

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:

- Passwords on page 4-1
- Protocol Configuration for TCP/IP, NetWare, and LAT protocols on page 4-2
- Serial Port Configuration on page 4-7

Note: *To return to factory defaults, press and hold the Reset button while cycling power on the unit, or enter the Initialize Factory command at the **Local>** prompt. Keep in mind that doing so will remove all custom configurations.*

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

4.1 Passwords

There are two types of passwords on the MSS: privileged and login.

- You must enter the *privileged password* to change most settings. The default privileged password is **system**. To change it, enter the **Change Privpass** command.
- When the *login password* is enabled, users must enter the login password to connect to the MSS. The default login password is **access**. To change it, enter the **Change Loginpass** command.

  The login password is disabled by default. To enable the login password:

  - If you are connecting from a network to the MSS, enter the **Change Incoming** [Password] command at the **Local>** prompt.
  - If you are connecting from the serial port to the MSS, enter the **Change Password Protect** command at the **Local>** prompt.

- If you are connecting from the network to the MSS serial port, enter the **Change Password Incoming** command at the **Local>** prompt.

4.2 Protocol Configuration

Certain options can be configured for each of the protocols supported by the MSS. For more information on protocol configuration, refer to the *Device Server Reference Manual*.

4.2.1 TCP/IP Configuration

4.2.1.1 IP Address

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

Figure 4-1: Changing the IP Address

```
Local>> CHANGE IPADDRESS 192.0.1.228
```

4.2.1.2 Subnet Mask

IP networks can be divided into several smaller networks by subnetting. When a network is subnetted, some of the host part of the address range is allocated to the network part of the address. The subnet mask denotes what portion of an IP address is network and what portion is node number, and allows the server to decide at connection time whether a given TCP/IP host is part of the local network segment. All hosts must agree on the subnet mask for a given network.

When you configure the MSS IP address, 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. Use the **Change Subnet Mask** command.

Figure 4-2: Setting the Subnet Mask

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

4.2.1.3 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 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 *Device Server Reference Manual* for more information.

4.2.1.4 Name Server

A TCP/IP host generally has an alphanumeric host name, such as Phred, in addition to its IP address. 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 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 *Device Server 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 DOMAIN “xyzcorp.com”
```

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

4.2.1.5 IP Security

IP security allows the system administrator to restrict incoming and outgoing TCP/IP sessions and access to the serial port. Connections are allowed or denied based upon the source IP address (for incoming connections) or the destination IP address (for outgoing connections).

IP security information can be added to the IP local host table. To add an entry, specify an IP address and whether to allow (Enabled) or deny (Disabled) connections. An address with 0 or 255 in any segment restricts all addresses in that range. For example, the command below disables outgoing connections for all addresses between 192.0.1.1 and 192.0.1.254. Single addresses can also be specified. See **Change IPSecurity** in the *Device Server Reference Manual* for more information.

Figure 4-6: IP Security Command

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

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.

4.2.1.6 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
```

4.2.2 IPX (NetWare) Configuration

Four NetWare settings can be configured: routing and encapsulation parameters, the internal network number to use for internal routing, and the NetWare loadhost to use at boot time.

4.2.2.1 Routing and Encapsulation

The first layer of an IPX Ethernet packet is the frame type. It includes routing information. By default, the MSS is configured to handle packets of all four NetWare frame types.

If more than one frame type is in use on the LAN, the MSS will advertise itself as a router to the network using its internal network number. This behavior allows nodes and fileservers to access the MSS regardless of the frame type being used.

The MSS can be restricted to a single frame format, in which case it will not do internal routing. Two commands control this behavior: **Change NetWare Routing** and **Change NetWare Encapsulation**.

- **Change NetWare Routing** enables or disables the use of the internal network number. By default, internal routing is enabled.

Note: *If two or more frame types are enabled, internal routing must be enabled. To see which frame types are enabled, enter the Show NetWare command.*

- **Change NetWare Encapsulation** controls which of the frame types are used. The choices are Ether_II, Native, 802_2, and SNAP which provide for Ethernet v2, 802.3 Native mode, 802.2, and 802.2 SNAP encapsulation types.

Figure 4-8 displays an example routing and encapsulation configuration. The 802.3 Native mode and 802.2 SNAP frame types are enabled, while Ethernet v2 and 802.2 are disabled. Because more than one frame type is enabled, internal routing must also be enabled.

Figure 4-8: Enabling Selected Frame Types

```
Local>> CHANGE NETWARE ENCAPSULATION NATIVE ENABLED
Local>> CHANGE NETWARE ENCAPSULATION SNAP ENABLED
Local>> CHANGE NETWARE ENCAPSULATION ETHER_2 DISABLED
Local>> CHANGE NETWARE ENCAPSULATION 802_2 DISABLED
Local>> CHANGE NETWARE ROUTING ENABLED
```

4.2.2.2 Internal Network Number

When internal routing is enabled, the MSS needs an internal network number that is unique on the network. When addressing IPX packets to a file server, devices use the file server's internal network number as the destination address.

The internal network number for the MSS is a four-byte number that defaults to the last four bytes of the unit's Ethernet address (for example, a3001234). It is unlikely that this number will need to be changed.

Note: *If you do change the internal network number, reboot the MSS.*

4.2.2.3 Loadhost

A loadhost is a NetWare fileserver from which the MSS will try to load code when the **Initialize Reload** command is entered. If the software loadfile or loadhost address changes, you will have to change the configured parameters for the next reboot. For the following example, the loadhost is *phred*, and the name of the loadfile is "MSS100.SYS".

Figure 4-9: Changing the NetWare Loadhost

```
Local_2>> CHANGE NETWARE LOADHOST phred
Local_2>> CHANGE SOFTWARE sys:login/MSS100.SYS
```

4.2.3 LAT Configuration

Three LAT parameters can be configured for the MSS: the server's identification string, its service group list, and its internal circuit timer.

4.2.3.1 Server Identification

The MSS has a default name that it uses when announcing itself to the LAT network (mss_*xxxxxx* where *xxxxxx* represents the last six characters of its hardware address). Users can change the name. Users can also configure a more descriptive identification string.

Figure 4-10: LAT Name and Identification

```
Local> CHANGE NAME "Bio5"
Local> CHANGE LAT IDENTIFICATION "Biolab 2"
```

4.2.3.2 Service Groups

A service is any resource on the network that can be accessed locally or via a network connection, such as a modem. The MSS serial port and the services on the network each belong to one or more service groups. When a user or device requests a connection to a service, the LAT host will check the service groups to which both the requester and the service belong. If any group number is common to both, the connection attempt will continue. If not, access will be denied.

The **Change LAT Groups** command establishes group numbers for the MSS and its serial port.

Figure 4-11: Changing Service Groups

```
Local>> CHANGE LAT GROUPS 1,7,13,105,210-216
```

Note: *Each time the Change LAT Groups command is entered, the previous group list is replaced.*

4.2.3.3 Circuit Timer

Message transmission on LAT networks is controlled by timers. The MSS circuit timer specifies when messages will be sent from the server to other network nodes. This timer value is set to a standard default at the factory and should not need to be changed.

If you need to change the length of the circuit timer, use the **Change LAT CircTimer** command followed by a timer value integer. The timer value can range from 30 to 200 milliseconds.

Figure 4-12: Changing Timer Delay

```
Local>> CHANGE LAT CIRCTIMER 50
```

4.3 Serial Port Configuration

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

4.3.1 Access Mode

The serial port access mode governs which connections the 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 the serial port's access mode, enter the **Change Access** command.

Figure 4-13: Changing Serial Port Access Mode

```
Local>> CHANGE ACCESS LOCAL
```

If the attached serial device will be continuously transmitting data to the MSS, the MSS port should be changed to Access Remote. This will prevent the MSS and serial device from babbling to each other.

4.3.2 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.

Figure 4-14: Enabling Autostart

```
Local>> CHANGE 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. There is no 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 *Enabling Modem Mode* on page 5-10 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.

Figure 4-15: Configuring an Autostart Character

```
Local>> CHANGE AUTOSTART CHARACTER "A"
```

4.3.3 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.

Figure 4-16: Changing the Baud Rate

```
Local>> CHANGE SPEED 19200
```

The MSS supports Autobaud, which allows the serial port to match its speed to the attached serial device upon connection (see **Change Autobaud** in the *Device Server 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 4-17: Enabling Autobaud

```
Local>> CHANGE AUTOBAUD ENABLED
```

4.3.4 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.

Figure 4-18: Configuring Serial Port Parameters

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

Note: *If the MSS is set to 8 bit characters, parity must be set to none.*

4.3.5 Flow Control

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, 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 4-19: Enabling Recommended Flow Control

```
Local>> CHANGE FLOW CONTROL CTS
or
Local>> CHANGE FLOW CONTROL XON
```

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 the Passflow option. However, passflow is unnecessary in most situations. See **Change Flow Control** in the *Device Server Reference Manual* for more information.

4.3.6 Modems and Modem Signaling

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.

4.3.6.1 Modem Control

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 (DSRLogout enabled).
- The MSS will hold DTR low for approximately 3 seconds after the port is logged out.
- Autostart will not happen until the attached device asserts DSR.

To enable modem control, enter the **Change Modem Control** command.

Figure 4-20: Enabling Modem Control

```
Local>> CHANGE MODEM CONTROL ENABLED
```

4.3.6.2 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 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.

Figure 4-21: Enabling Signal Checking

```
Local>> CHANGE SIGNAL CHECK ENABLED
```

4.3.6.3 DSRLogout

When a connection is lost, the MSS should log out the port and close any sessions. If it does not do so, security problems may result.

When a device connected to the MSS is disconnected or powered off, the DSR signal is deasserted. The MSS can be configured to automatically close the network connection to a port when this occurs using the **Change DSRLogout Enabled** command. This also prevents users from accessing other sessions by switching physical terminal lines.

Figure 4-22: Enabling DSRLogout

```
Local>> CHANGE DSRLOGOUT ENABLED
```

4.3.6.4 DTRWait

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 the serial device that a connection is possible and acceptable.

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.

Figure 4-23: Enabling DTRWait

```
Local>> CHANGE DTRWAIT ENABLED
```

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

4.3.7 Logouts

In addition to DSRLogouts, the 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 4-24: Logging out of the MSS

```
Local>> LOGOUT
```

To log out the 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 port after two minutes of inactivity, use the following commands. The inactivity logout timer period can be specified in seconds (s) or minutes (m). For example, in the following figure changing **1m** to **60s** produces the same results.

Figure 4-25: Enabling Timed Inactivity Logout

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

4.3.8 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 when no host name is specified in a connection command.

Figure 4-26: Defining a Preferred Service

```
Local>> CHANGE PREFERRED TCP 192.0.1.66
```

4.3.9 Dedicated Port Host

A dedicated host can also be defined for a port using the **Change Dedicated** command. When a serial user logs into 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 4-27: Defining a Dedicated Service

```
Local>> CHANGE 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 *Device Server Reference Manual* for more information.

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:

- Setting up two MSS units to emulate a direct serial connection over the LAN (see *Serial Tunnel* on page 5-7).
- Using the MSS as a data pipe between a serial device and multiple hosts on the network (see *Multihost Mode* on page 5-8).
- Making the MSS look like a modem so that it can be used with existing communications software (see *Modem Emulation Mode* on page 5-9).
- Using the Lantronix COM Port Redirector software to redirect PC COM ports (see *COM Port Redirector* on page 5-11).

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 and IPX connections can be made directly to the MSS serial port using sockets.

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 the serial port.
- If the attached serial device will be continuously transmitting data to the MSS, the MSS port should be changed to Access Remote (see Section 4.3.2).
- Only one serial port connection is allowed at a time, except in the case of *Multihost Mode* (see Section 5.4).
- 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 and 3001. 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. Do not add spaces.

Open a TCP session to port 3001 to form a raw TCP/IP connection to the serial port. Use port 2001 when you need Telnet IAC interpretation.

5.1.2 Host Applications

The MSS can be used with applications on Unix 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 its serial port. It supports Telnet and Rlogin connections, and environment strings added to the connection commands. See the *Command Reference* chapter of the *Device Server Reference Manual* on the CD-ROM 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.*

You can also make a Telnet connection to a specific port number, as described in *Serial Tunnel* on page 5-7.

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 5-2: 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 command 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 5-3: 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.

Figure 5-4: Defining a Local Switch

```
Local>> CHANGE LOCAL SWITCH ^L
```

Note: *To specify a control character, precede it with a carat (^x). To specify an escaped hex character, preceed it with a backslash (\xx).*

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.

Figure 5-5: Defining Switches

```
Local>> CHANGE BACKWARD SWITCH ^B
Local>> CHANGE FORWARD SWITCH ^F
```

Note: *To specify a control character, precede it with a carat (^x). To specify an escaped hex character, preceed it with a backslash (\xx).*

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 Hostlist

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

5.2.3.2 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.

5.2.3.3 Show Ports

Show Ports displays the configuration and connection status of the serial port—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.

5.2.3.4 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.

5.2.3.5 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.

5.2.3.6 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.

5.2.3.7 Show Session

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

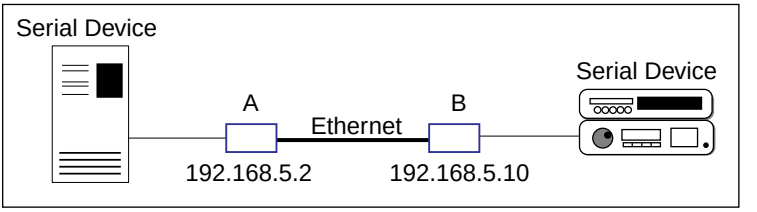
5.2.3.8 Show Users

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

5.3 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, CTS/RTS, etc.) or preserve timing between characters. The basic network configuration for this virtual serial line is shown in Figure 5-6.

Figure 5-6: Back-to-Back MSS Connections



5.3.1 TCP Configuration

Assuming the MSS network and serial port parameters have been configured properly, the Servers would be configured as follows:

MSS_A (192.168.5.2)
```
Local>> CHANGE DEDICATED TCP 192.168.5.10:3001T
Local>> CHANGE AUTOSTART ENABLED
```

MSS_B (192.168.5.10)
```
Local>> CHANGE ACCESS REMOTE
Local>> CHANGE DEDICATED NONE
Local>> CHANGE AUTOSTART DISABLED
```

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

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

5.3.2 UDP Configuration

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

MSS_A (192.168.5.2)
```
Local>> CHANGE DEDICATED TCP 192.168.5.10:4096U
Local>> CHANGE AUTOSTART ENABLED
Local>> CHANGE ACCESS DYNAMIC
```

MSS_B (192.168.5.10)
```
Local>> CHANGE DEDICATED TCP 192.168.5.2:4096U
Local>> CHANGE AUTOSTART ENABLED
Local>> CHANGE ACCESS DYNAMIC
```

Setting up Dedicated hosts ensures that the units will always talk only to each other. Enabling Autostart for both units 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).

5.4 Multihost Mode

Multihost mode sets up a data pipe between a serial device attached to the MSS and multiple hosts on the network. Data from a network host goes out of the 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 it 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 it and send the data to the other hosts. This will result in data loss for the unavailable host.
- When the MSS serial port logs out, all host sessions are disconnected, leaving the port idle.

5.4.1 Enabling Multihost Mode

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

Figure 5-7: Enabling Multihost Mode

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

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

5.4.2 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 5-8: Adding Entries to the Host Table

```
Local>> CHANGE DEDICATED HOSTLIST
Local>> HOST ADD TCP 192.0.1.35:5000T
Local>> HOST 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.

5.4.3 Removing Hosts

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

Figure 5-9: 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>> HOST DELETE 2
```

5.5 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. Instead of making phone calls, this mode provides network connections to remote machines.

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 5-10: Enabling Modem 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.

5.5.1 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. For a complete list of the AT commands supported by the MSS, check the MSS Reference Manual.

Table 5-1: Modem Mode Commands

Command	Function
AT?	Help; gives list of valid AT commands.
ATDT <ipaddress>	Forms a TCP connection to the specified host. Two IP address formats are allowed. The first uses periods, while the second omits periods and adds zeroes to segments less than 3 characters long: **Ex:** `ATDT 192.0.55.22:3001T` **Ex:** `ATDT 192000055022` Users can specify sockets as well; in the examples, **:3001T** tells the MSS to form a raw TCP connection to socket 3001.
ATE	Echo mode off (ATE0) or on (ATE1, the default).
ATH	Disconnects the network session.
ATQ	Result codes on (ATQ0, the default) or off (ATQ1).
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.
+++	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.

5.5.2 Wiring Requirements

Serial signals work differently when the MSS 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 5.5.1). Second, the MSS will drop DTR whenever the TCP session is disconnected. DSRLogout is enabled implicitly. The intent is that the MSS DTR signal will be used as a simulated CD signal to the attached serial device.

When using an MSS 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.

5.6 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 the MSS serial port. This enables the PC to use the MSS serial port as if it were one of the PC COM ports.

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 to diagnose and fix errors quickly yourself 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.	Reboot the unit. If you get the same message, you will need to reload Flash ROM. See *Reloading Software* on page D-2.
	If you did not request a TFTP boot, the flash ROM code is corrupt. The unit will remain in boot mode.	

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.
- MSS Modem control must be enabled. 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 it 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/MSS100.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 MSS100.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.

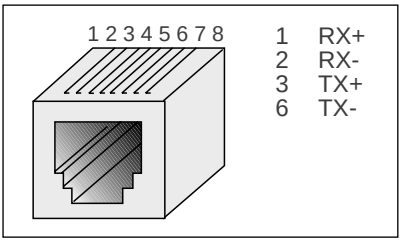
C: Pinouts

In the following diagrams, unlabeled pins are not connected.

C.1 Ethernet Connector

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

Figure C-1: RJ45 Ethernet Connector

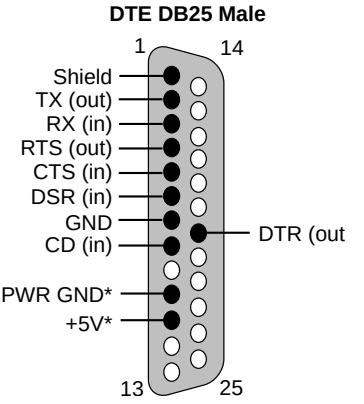


C.2 MSS Serial Connector

C.2.1 DB25 Connector

The figure below shows the pin connections of the MSS DB25 connector.

Figure C-2: DB25 Serial Connector



C.2.2 Modem Wiring

C.2.2.1 DSR (Data Signal Ready) versus CD (Carrier Detect)

By default, most modems assert CD only during a valid connection. In this case the modem's CD pin may be wired to the Server's DSR pin. Alternately, many modems can be configured such that DSR acts like CD. In this case, the modem's DSR pin may be wired to the Server's DSR pin.

C.2.2.2 DTR (Data Terminal Ready)

The MSS normally asserts DTR. When modem control is enabled on the MSS, the server will de-assert DTR for three seconds each time the port is logged out and each time a user disconnects from a modem service. The modem must be configured to hang up and recycle when DTR is de-asserted. If the modem is not configured in this way, sessions may not be properly disconnected.

D: Updating Software

D.1 Obtaining Software

A current software file (MSS100.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 MSS100.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, **MSS100.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 Trouble-shooting Flash ROM Updates on page D-4.*

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 MSS100.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 MSS100.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/MSS100.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 *Device Server Reference Manual* located on the CD-ROM.

D.2.1.2 NetWare

The MSS100.SYS file should be placed in the login directory on the NetWare file server. The MSS cannot actually log into the file server (since it knows no username/password); it can only access files in the login directory itself. On the MSS, specify the file server name, filename, and path.

Figure D-3: Configuring NetWare Reload

```
Local> SET PRIVILEGED
Password> SYSTEM (not echoed)
Local>>  CHANGE NETWARE LOADHOST fileserver
Local>>  CHANGE SOFTWARE SYS:\LOGIN\MSS100.SYS
Local>> INITIALIZE RELOAD
```

D.2.1.3 MOP

The MSS100.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 MSS100.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
NetWare	Ensure the file is in the login directory. Since the MSS cannot actually log into the file server, it has limited access to the NetWare server directories.
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.
MOP	Ensure that the Ethernet circuit must has the **service** characteristic enabled.
	Ensure that the MOM$LOAD search path includes the directory containing the MSS100.SYS file.

E: Specifications

E.1 Power Specifications

The MSS power cube adaptor has the following specifications:

Adapter input voltage:
110 VAC US, 220 VAC International

Adapter output voltage:
5 VDC at 700 mA

Operating current:
700 mA @ 5 V

Power consumption:
4.2 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 years from the date of shipment that each MSS100 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 return 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 & Address:	Lantronix 15353 Barranca Parkway, Irvine, CA 92618 USA
	Declares that the product:
Product Name:	Device Server
Model Name/Number:	MSS100
	Conforms to the following standards or other normative documents:
Safety:	EN60950:1988+A1, A2
Electromagnetic Emissions:	EN55022: 1998 (CISPR 22, Class A: 1993, A1: 1995, A2: 1996) IEC 1000-3-2/A14: 2000 IEC 1000-3-3: 1994
Electromagetic Immunity:	EN55024: 1998 Information Technology Equipment-Immunity Characteristics IEC 6100-4-2: 1995 Electro-Static Discharge Test IEC 6100-4-3: 1996 Radiated Immunity Field Test IEC 6100-4-4: 1995 Electrical Fast Transient Test IEC 6100-4-5: 1995 Power Supply Surge Test IEC 6100-4-6: 1996 Conducted Immunity Test IEC 6100-4-8: 1993 Magnetic Field Test IEC 6100-4-11: 1994 Voltage Dips & Interrupts Test (L.V.D. Directive 73/23/EEC)
Supplementary Information:	*This product has been verified as being compliant within the Class A limits of the FCC Radio Frequency Device Rules (FCC Title 47, Part 15, Subpart B CLASS A), measured to CISPR 22: 1993 limits and methods of measurement of Radio Disturbance Characteristics of Information TechnologyEquipment.* *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

R

S

T

U

W