LX-Series Configuration Guide

Corporate Headquarters

MRV Communications, Inc. Corporate Center
20415 Nordhoff Street
Chatsworth, CA 91311
Tel: 818-773-0900
Fax: 818-773-0906
www.mrv.com (Internet)

Sales and Customer Support

MRV Americas
295 Foster Street
Littleton, MA 01460
Tel: 800-338-5316 (U.S.)
Tel: +011 978-952-4888 (Outside U.S.)
sales@mrv.com (email)
www.mrv.com (Internet)

MRV International
Industrial Zone
P.O. Box 614
Yokneam, Israel 20682
Tel: 972-4-993-6200
sales@mrv.com (email)
www.mrv.com (Internet)

451-0311B

Service Information

Should you experience trouble with this equipment, please contact one of the following support locations:

- **If you purchased your equipment in the Americas,** contact MRV Americas Service and Support in the U.S. at 978-952-4888. (If you are calling from outside the U.S., call +011 978-952-4888.)
- **If you purchased your equipment outside the Americas (Europe, EU, Middle-East, Africa, Asia),** contact MRV International Service and Support at 972-4-993-6200.

Secure Shell Disclaimer

THE SECURE SHELL SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OR SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Table of Contents

Figures

Preface

This guide describes how to manage and configure the LX unit and provides background information on all of the configurable features of the LX unit.

How This Book is Organized

This guide is organized as follows:

- **Chapter 1** – Describes how to do the initial setup of the LX unit.
- **Chapter 2** – Describes how to set up remote console management on the LX unit.
- **Chapter 3** – Describes how to perform system administration on the LX unit.
- **Chapter 4** – Describes how to set up the Notification Feature.
- **Chapter 5** – Describes how to set up the Data Broadcast Feature.
- **Chapter 6** – Describes how to configure IP interfaces.
- **Chapter 7** – Describes how to configure subscriber accounts.
- **Chapter 8** – Describes how to configure ports for Temperature/Humidity sensors.
- **Chapter 9** – Describes how to configure ports for power management.
- **Chapter 10** – Describes how to use the `iptables` command to configure packet filters for the LX unit.
- **Appendix A** – Provides an overview of the RADIUS authentication feature and describes the RADIUS authentication attributes.
- **Appendix B** – Provides an overview of the RADIUS accounting feature and the TACACS+ accounting feature and describes the RADIUS and TACACS+ accounting attributes.

- **Appendix C** – Provides an overview of the TACACS+ authentication feature and describes the TACACS+ authentication attributes.
- **Appendix D** – Lists the Linux man pages for the `iptables` command.

Conventions

The following conventions are used throughout this guide:

- **Command execution –** Unless otherwise specified, commands are executed when you press <RETURN>.
- **Keyboard characters (keys)** – Keyboard characters are represented using left and right angle brackets (< and >). For example, the notation <CTRL> refers to the CTRL key; <A> refers to the letter A; and <RETURN> refers to the RETURN key.
- **Command syntax –** Where command options or command syntax are shown, keywords and commands are shown in lowercase letters.
- **Typographical conventions –** The following typographical conventions are used:

  `Monospace Typeface` – indicates text that can be displayed or typed at a terminal (i.e., displays, user input, messages, prompts, etc.).

  italics – are used to indicate variables in command syntax descriptions.

Using the Function Keys

The LX Command Line Interface (CLI) supports the following function keys:

- **Ctrl-F –** Moves forward to the next session.
- **Ctrl-B –** Moves back to the previous session.
- **Ctrl-L –** Returns you to the Local Command Mode.

  NOTE: You must press the Enter key after you type **Ctrl-F**, **Ctrl-B**, or **Ctrl-L**.

- **Up arrow –** Recalls the last command.

- **Tab key** – Autocompletes a partially typed command. For example, if you type the tab key after you type **show ver** at the Superuser command prompt, the `show version` command will be autocompleted. (**Note:** You must type the first three characters in a command keyword before you can autocomplete it with the Tab key.)

Online Help

The question mark character (?), and the Tab key, are used to display online help in the LX Command Line Interface (CLI). The following guidelines will help you to navigate the online help system:

- Type the ? character (or press the Tab key) at the command prompt in any command mode, to display the first keyword of each command that can be executed in that command mode. For example, the following is displayed when you type the ? character at the User command prompt:

```
InReach:0 >
  User Commands:
 clear          Clear screen and reset terminal line
 disconnect     Disconnect session
 enable         Turn on privileged commands
 exit           Exits and disconnects user
 no             Negate a command
 pause          Pause enable
 ping           Send echo messages
 show           Show running system information
 ssh            Secure Shell (Triple-DES/Blowfish)
 telnet         Open a telnet connection
 terminal       Set the terminal type
```

- Type the ? character (or press the Tab key) after the displayed keyword to list the options for that keyword. For example, type `show?` to list the options of the `show` keyword. You could then type `show port?` to list the next item in the syntax of the `show port` command.

Navigating the LX Command Line Interface (CLI)

The LX CLI is structured as a set of nested command modes. Each command mode is used to implement a group of related features or functions. Figure 1 lists the command modes in the LX CLI.

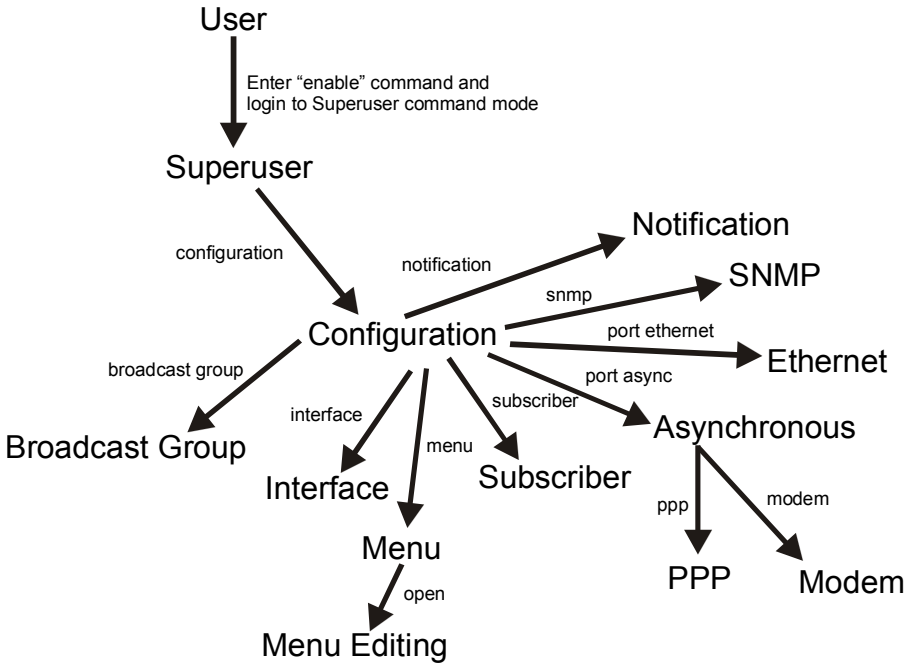

Figure 1 - LX Command Modes

Each command mode has its own command prompt (e.g., `Config:0 >>`) and its own set of commands.

Type a question mark (**?**) (or press the Tab key) at any of the LX CLI command prompts to display the commands that can be executed in the current command mode. For example, type a question mark at the `Menu :0 >>` prompt to display the commands that can be executed in the Menu command mode.

Except for the User command mode, each command mode is nested in a previous command mode. (The User command mode is the basic command mode of the LX CLI; you are in the User command mode when you log in to the LX unit.) For example, the Superuser command mode is nested in User command mode; the Configuration command mode is nested in the Superuser command mode, and so on.

To enter a nested command mode, you must enter the appropriate command from the previous command mode. For example, to enter the Configuration command mode you must enter the `configuration` command from the Superuser command mode.

You can use the `exit` command to return to the previous command mode. For example, you would enter the `exit` command in the Asynchronous command mode to return to the Configuration command mode.

You can use the end command to return to the Superuser Command Mode from the Configuration Command Mode or from any command mode that is nested in the Configuration Command Mode.

The rest of this section describes the LX command modes and the commands that are used to access each of them.

User Command Mode

When you log on to the LX unit, you are in the User command mode. This is indicated by the User command prompt (e.g., `InReach:0 >`). The User command mode includes commands for doing the following:

- Managing your LX session and terminal.
- Pinging remote hosts.
- Connecting to remote hosts via SSH and Telnet.
- Displaying your subscriber-specific information.
- Displaying information about the LX port to which you are connected.
- Accessing the Superuser command mode.

Refer to the "User Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the User Command Mode.

Superuser Command Mode

The Superuser command prompt (e.g., `InReach:0 >>`) is displayed when you are in the Superuser command mode. You can access the Superuser command mode by executing the `enable` command in the User command mode.

When you execute the `enable` command, the `Password:` prompt is displayed. To enter Superuser mode, you must enter a Superuser password at the `Password:` prompt.

In the Superuser command mode, you can perform all of the tasks that you can perform in User command mode, as well as the following:

- Manage the LX unit.
- Display global information for the LX unit.
- Access the Linux shell.
- Access the Configuration command mode.

Refer to the "Superuser Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Superuser Command Mode.

Configuration Command Mode

The Configuration command prompt (e.g., `Config:0 >>`) is displayed when you are in the Configuration command mode. You can access the Configuration command mode by executing the `configuration` command in the Superuser command mode.

In the Configuration command mode, you can perform such tasks as the following:

- Specify the server-level configuration of the LX unit. The server-level configuration includes the Superuser password and settings for ppciboot, RADIUS, TACACS+, SecurID, and all other server-level features.

- Access the Asynchronous command mode.
- Access the Ethernet command mode.
- Access the Interface command mode.
- Access the Menu command mode.
- Access the Notification command mode.
- Access the SNMP command mode.
- Access the Subscriber command mode.
- Access the Broadcast Group command mode.

Refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Configuration Command Mode.

Asynchronous Command Mode

The Asynchronous command prompt (e.g., `Async 4-4:0 >>`) is displayed when you are in the Asynchronous command mode. For example, the prompt `Async 4-4:0 >>` indicates that you are in the Asynchronous command mode for port 4. You can access the Asynchronous command mode by executing the `port async` command in the Configuration command mode with an LX port number as the command argument; for example:

```
Config:0 >>port async 4
```

In the Asynchronous command mode, you can do the followng:

- Configure asynchronous port settings such as access methods, APD settings, autobaud, autodial, flow control, and inbound and outbound authentication.
- Access the PPP command mode.
- Access the Modem command mode.

Refer to the "Asynchronous Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Asynchronous Command Mode.

PPP Command Mode

The PPP command prompt (e.g., `PPP 4-4:0 >>`) is displayed when you are in the PPP command mode. You can access the PPP command mode by executing the `ppp` command in the Asynchronous command mode.

In the PPP command mode, you can configure the Point-to-Point Protocol (PPP) for asynchronous ports. Some of the settings that you can configure include accounting, authentication, IPCP parameters, and LCP parameters.

Refer to the "PPP Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the PPP Command Mode.

Modem Command Mode

The Modem command prompt (e.g., `Modem 4-4:0 >>`) is displayed when you are in the Modem command mode. You can access the Modem command mode by executing the `modem` command in the Asynchronous command mode.

In the Modem command mode, you can configure external modems for asynchronous ports. Some of the settings that you can configure include type, dialout number, modem retries, and the modem initialization string.

Refer to the "Modem Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Modem Command Mode.

Ethernet Command Mode

The Ethernet command prompt (e.g., `Ether 1-1:0 >>`) is displayed when you are in the Ethernet command mode. You can access the Ethernet command mode by executing the `port ethernet` command in the Configuration command mode with an LX port number as the command argument; for example:

Config:0 >>`port ethernet 1`

In the Ethernet command mode, you can configure Ethernet port descriptions and the duplex mode and speed of Ethernet ports.

Refer to the "Ethernet Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Ethernet Command Mode.

Subscriber Command Mode

The Subscriber command prompt (e.g., `Subs_mark >>`) is displayed when you are in the Subscriber command mode. You can access the Subscriber command mode by executing the `subscriber` command in the Configuration command mode.

In the Subscriber command mode, you can provision subscribers of the LX unit. Some of the subscriber settings include function keys, Telnet settings, and security settings.

Refer to the "Subscriber Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Subscriber Command Mode.

SNMP Command Mode

The SNMP command prompt (e.g., `Snmp:0 >>`) is displayed when you are in the SNMP command mode. You can access the SNMP command mode by executing the `snmp` command in the Configuration command mode.

In the SNMP command mode, you can configure the SNMP settings for an LX unit.

Refer to the "SNMP Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the SNMP Command Mode.

Interface Command Mode

The Interface command prompt (e.g., `Intf 1-1:0 >>`) is displayed when you are in the Interface command mode. You can access the Interface command mode by executing the `interface` command in the Configuration command mode.

In the Interface command mode, you can configure interfaces for the LX unit. Some of the settings that you can configure include the IP settings, MTU, and IP Rotaries for the interface, as well as SSH and Telnet settings.

Refer to the "Interface Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Interface Command Mode.

Menu Command Mode

The Menu command prompt (e.g., `Menu :0 >>`) is displayed when you are in the Menu command mode. You can access the Menu command mode by executing the `menu` command in the Configuration command mode.

In the Menu command mode, you can create, delete, import, and display menus and access the Menu Editing command mode by executing the `open` command.

Refer to the "Menu Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Menu Command Mode.

Menu Editing Command Mode

The Menu Editing command prompt (e.g., `mark-1:0 >>`) is displayed when you are in the Menu Editing command mode. For example, the prompt `mark-1:0 >>` indicates that the menu `mark` is open in the Menu Editing command mode. You can access the Menu Editing command mode by executing the `open` command in the Menu command mode.

In the Menu Editing command mode, you can create and modify menus.

Refer to the "Menu Editing Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Menu Editing Command Mode.

Notification Command Mode

The Notification command prompt (e.g., `Notification:0 >>`) is displayed when you are in the Notification command mode. You can access the Notification command mode by executing the `notification` command in the Configuration command mode.

In the Notification command mode, you can configure the sending of accounting log messages to pagers, email addresses, SNMP trap clients, local files, remote hosts, syslogd, and asynchronous ports.

Refer to the "Notification Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Notification Command Mode.

Broadcast Group Command Mode

The Broadcast Group command prompt (e.g., `BrGroups 6:0 >>`) is displayed when you are in the Broadcast Group command mode. You can access the Broadcast Group command mode by executing the `broadcast group` command in the Configuration command mode.

In the Broadcast Group command mode, you can configure a Broadcast Group. A Broadcast Group consists of Slave Ports and Master Ports. The Slave Ports receive data broadcasts from the Master Ports.

Refer to the "Broadcast Group Commands" chapter of the *LX-Series Commands Reference Guide* for detailed information on the commands that you can execute in the Broadcast Group Command Mode.

Disabling (Negating) Features and Settings

In order to disable a feature or setting, you must execute the `no` command with one or more modifiers. The `no` command must be executed in the same Command Mode in which the feature or setting was specified. For example, you can disable Autobaud by executing the `no` command with the `autobaud` modifier in the Asynchronous command mode. The full command syntax would look like this:

```
Async 6-6:0 >>no autobaud
```

To display the features and settings that can be disabled or negated in any command mode, enter `no?`; for example:

```
Async 6-6:0 >>no?
apd
authentication
autobaud
autodial
```

The above example shows that you can disable the Autodial feature by executing the `no autodial` command in the Asynchronous command mode.

In some instances, the `no` command may require more than one modifier. For example, to reset the dialout number in the Modem command mode, you need to execute the `no` command with the `dialout` modifier *and* the `number` modifier.

Type the question mark (?) after the first modifier to determine if the `no` command requires additional modifiers to disable a feature or negate a setting; for example:

```
Modem 6-6:0 >>no dialout?
number
Modem 6-6:0 >>no dialout number?
<cr>
```

Related Documents

For detailed information on the LX commands, refer to the *LX-Series Commands Reference Guide* (P/N 451-0310E).

For more information on the LX hardware, refer to *Getting Started with the LX Series* (P/N 451-0308E).

The *LX Quick Start Instructions* (P/N 451-0312F) describes how to get the LX unit up and running.

Chapter 1

Initial Setup of the LX Unit

This section describes how to do the initial setup of the LX unit. Before you use the LX unit for network management, you must perform the tasks described in this chapter. You can do the tasks described in this chapter after you have installed and powered on the LX unit as described in Chapter 1 of *Getting Started with the LX Series*.

Configuring TCP/IP

You can allow the LX unit to obtain its TCP/IP parameters from the network, or you can explicitly configure TCP/IP parameters for the LX unit with the Quick Start Configurator or the IP Configuration Menu. (You can access the IP Configuration Menu from the ppciboot Main Menu.)

Obtaining TCP/IP Parameters from the Network

If the TCP/IP parameters for the LX unit have not been explicitly configured, the LX unit will attempt to load its TCP/IP parameters from the network when the LX unit boots. The LX unit can load its TCP/IP parameters from any LAN that runs DHCP, BOOTP, or RARP.

Configuring TCP/IP Parameters with the Quick Start Configurator

Do the following to configure TCP/IP parameters with the Quick Start Configurator:

1. Plug in the terminal at the DIAG port (port 0) on the LX unit. (The port values are 9600 bps, eight bits, one stop bit, no parity, and Xon/Xoff flow control.) The `Run Initial Connectivity Setup? y/n` message appears (when the LX first boots up on default parameters).
2. Press `y` (yes) and press <Enter>. The Superuser Password prompt appears.

3. Enter the password `system`. The Quick Configuration menu appears:

```
                  Quick Configuration menu
              1 Unit IP address
              2 Subnet mask
              3 Default Gateway
              4 Domain Name Server
              5 Domain Name Suffix
              6 Superuser Password
              7 Exit and Save
    Enter your choice:
```

4. Press the number corresponding to the parameter you want to set.
5. Enter the appropriate information and press <Enter> to return to the Quick Configuration menu. Once you enter a parameter value, a data entry line specific to that parameter appears on the Quick Configuration menu.
6. Continue in this way through the menu, configuring as many parameters as you want. You are not required to configure all parameters.

   NOTE: You should change the Superuser Password, since this is the first time you are configuring the LX unit (the default password is `system`).

7. Press `7` (`Exit and Save`) to save your changes. The `Is this information correct?` message appears.

```
                  CONFIGURATION SUMMARY
          1 Unit IP address                    10.80.1.5
          2 Subnet mask                        255.0.0.0
          3 Default Gateway
          4 Domain Name Server
          5 Domain Name Suffix
          6 Superuser Password                 Changed
          7 Exit and Save
 Is this information correct?  (y/n) :
```

8. Press `y` (yes) and press <Enter>. The `Save this information to flash?` message appears.
9. Press `y` (yes) and press <Enter>. The information is saved to flash.
10. Press <Enter> several times to display the `Login:` prompt.
11. Enter your login name. The default is `InReach`.
12. Enter your password. The default is `access`. You can now use the LX unit.

    NOTE: The login username and password are case-sensitive.

Setting the TCP/IP Parameters in the IP Configuration Menu

You can use the IP Configuration Menu to set the TCP/IP parameters for the LX unit. For more information, refer to "Using the IP Configuration Menu" in *Getting Started with the LX Series*.

Creating and Loading a Default Configuration File

This section explains how to create a default configuration file with which you can load multiple units.

Creating a Default Configuration File

After your first LX unit is up and running, you can save the unit configuration to the network. For further information, refer to "Saving the Configuration to the Network" on page 30. You must rename this `.zip` file to `lx` *`last six digits of the mac address`*`.prm` (e.g. `lx12ab9f.prm`). Once this is complete, you can use this `.prm` file as a template to configure multiple units at one time by changing the last six digits of the mac address to reflect that of the specific unit.

Loading a Default Configuration File

If loading via BOOTP and DHCP, you can load a default configuration file from a TFTP server that is located on the same server from which you obtained your IP address. If you are not loading via one of these, the unit looks on the TFTP server specified in ppciboot. If the configuration is defaulted, it is detected at startup and the unit checks that a TFTP server was passed by ppciboot. If a TFTP server is accessible, the LX unit connects to it and tries to download a default file named `lx` *`last six digits of the mac address`*`.prm` (e.g., `lx12ab9f.prm`).

If this file exists, the LX unit loads it into its configuration table. If the default file does not exist, the Quick Start menu is displayed.

You can use the `.prm` file as a template to configure multiple units at one time. After copying the `.prm` file, you would rename it to `lx` *`last six digits of the mac address`*`.prm` (e.g., `lx12ab9f.prm`). For more information, refer to "Saving the Configuration to the Network" on page 62.

Saving the Configuration to the Network

The TFTP protocol is used to perform the operation of saving the LX configuration to a network host. If the network host is a UNIX host, a configuration file must already exist on the TFTP server.

The configuration file is a `.zip` file that contains everything previously described except for the SSH keys, since they belong to the unit itself and cannot be used on a different unit.

Since the format is a `.zip` file, it is usable by WinZip or UNIX Unzip.

To save the configuration to the network, execute the following command in the Superuser Command Mode:

```
save configuration network filename tftp_server_address
```

NOTE: The filename that you specify in the `save configuration network` command must not include the `.zip` extension.

Setting Up Local (Onboard) Security for the LX Unit

Local security is the default security method for the LX unit. Under Local security, the user is authenticated against a username/password file that resides on the LX unit.

NOTE: The LX unit also supports RADIUS, TACACS+, and SecurID security. Under RADIUS, TACACS+, and SecurID, the user is authenticated against a username/password file that resides on the authentication server. For more information, refer to "Setting Up RADIUS, SecurID, and TACACS+ for the LX Unit" on page 33.

IMPORTANT!

MRV Communications recommends that you change the default password for the user **InReach** *before* you put the LX unit on a network. For more information, refer to "Changing the Password Defaults" (below).

Changing the Password Defaults

It is widely known that the default password for the **InReach** user is **access**. If an unauthorized user knew this username/password combination, he/she could log on to your LX unit. For this reason, you should change the InReach user's password to something other than **access**.

It is also widely known that the default Superuser password is **system**. To reduce the risk of an unauthorized user gaining access to the Superuser Command Mode, MRV recommends that you change this password to something other than **system**.

Changing the Default Password for the InReach User

Do the following to change the User-level password of the **InReach** User:

1. Access the Configuration Command Mode. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)

2. Access the Subscriber Command Mode for the **InReach** subscriber. You do this by entering the `subscriber` command with **InReach** as the command argument; for example:

   Config:0 >>`subscriber InReach`

3. Enter the `password` command at the Subs_InReach >> prompt; for example:

   Subs_InReach >>`password`

4. Enter a new User password at the `Enter your NEW password:` prompt. The password will be displayed as asterisks, as in the following example:

   Enter your NEW password : `**********`

5. Re-enter the new User password at the `Re-Enter your NEW password:` prompt. The password will be displayed as asterisks, as in the following example:

   Re-Enter your NEW password: `**********`

Changing the Default Superuser Password

To change the Superuser password for the LX unit, do the following:

1. Access the Configuration Command Mode. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)

2. Enter the `password` command at the `Config:0 >>` prompt; for example:

   Config:0 >>`password`

3. Enter a new Superuser password at the `Enter your NEW password:` prompt. The password will be displayed as asterisks, as in the following example:

   Enter your NEW password : `**********`

4. Re-enter the new Superuser password at the `Re-Enter your NEW password:` prompt. The password will be displayed as asterisks, as in the following example:

   Re-Enter your NEW password: **********

Setting Up RADIUS, SecurID, and TACACS+ for the LX Unit

You can implement SecurID, RADIUS, or TACACS+ authentication on the LX unit. For more information, refer to the following:

- "Setting Up RADIUS" (below)
- "Setting Up TACACS+" on page 38
- "Setting Up SecurID" on page 43

Setting Up RADIUS

The LX can implement RADIUS authentication and RADIUS accounting at the server level and for specific interfaces and asynchronous ports. You must configure RADIUS accounting and/or authentication at the server level before you can implement it on specific interfaces and asynchronous ports on the LX unit.

The basic steps for configuring RADIUS authentication on the LX unit are:

1. Installing and configuring the RADIUS server on a Network-based Host (see page 34).
2. Specifying the RADIUS server settings on the LX (see page 34).
3. Specifying the RADIUS period on the LX (see page 38).

For more information on RADIUS authentication, refer to "Overview of RADIUS Authentication" on page 157.

For more information on RADIUS accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 161.

Installing and Configuring the RADIUS Server on a Network-based Host

Before you can authenticate with RADIUS on your LX unit, you must configure a RADIUS server on your network.

In general, RADIUS server implementations are available on the Internet. These implementations generally use a daemon process that interacts with RADIUS clients (located on LX units and on other remote access devices).

The daemon uses a list of clients and associated secrets that it shares with these clients. The per-client secret is used to encrypt and validate communications between the RADIUS server and the client. The file used to keep the client list and secrets is the "clients" file.

Another file used by the daemon to store the users that are authenticated is the "users" file. The "users" file contains the RADIUS attributes associated with a particular user. As a minimum, this file must contain the user's username, password (depending on the RADIUS server used), and Service-type.

To configure the RADIUS server, refer to your RADIUS host documentation. MRV recommends that you use the Merit RADIUS server implementation. Information for the Merit RADIUS server can be found at http://www.merit.edu. Refer to the GOPHER SERVER and the MERIT Network Information Center for new releases.

Specifying the RADIUS Server Settings on the LX

Do the following to specify the RADIUS server settings on the LX unit:

1. Check the primary RADIUS Server host to ensure that the RADIUS server client database has been configured.
2. Access the Configuration Command Mode on the LX. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)

3. Use the `radius primary authentication server address` command to specify the IP address of the RADIUS primary authentication server; for example:

   Config:0 >>`radius primary authentication server address 146.32.87.93`

4. Use the `radius primary authentication server secret` command to specify the secret that will be shared between LX unit and the RADIUS primary authentication server; for example:

   Config:0 >>`radius primary authentication server secret BfrureG`

5. Use the `radius primary authentication server port` command to specify the socket your RADIUS server is listening to; for example:

   Config:0 >>`radius primary authentication server port 1645`

   NOTE: The LX listens to port 1812 by default.

6. To verify the LX RADIUS configuration, exit from the Configuration command mode and execute the `show radius characteristics` command at the Superuser command prompt; for example:

   InReach:0 >>`show radius characteristics`

   Refer to Table 1 on page 36 for descriptions of all of the settings that you can specify for a RADIUS server.

   In order to use a RADIUS primary accounting server, or a RADIUS secondary server, you must specify an IP address and a secret for the respective RADIUS server. For examples of the commands that you would use, refer to the following sections:

   - "RADIUS Primary Accounting Server Commands" on page 37
   - "RADIUS Secondary Authentication Server Commands" on page 37

- "RADIUS Secondary Accounting Server Commands" on page 37

NOTE: The use of a RADIUS primary accounting server, and the use of RADIUS secondary servers, is optional.

After you have specified the RADIUS settings for the RADIUS primary authentication server, you can configure the RADIUS primary accounting server and the RADIUS secondary authentication and accounting servers.

Table 1 - RADIUS Settings

RADIUS Settings	Description
`address`	IP address of the RADIUS server
[1]`port`	UDP port of the RADIUS server
[1]`retransmit`	The maximum number of times that the LX unit will attempt to retransmit a message to the RADIUS server
`secret`	The RADIUS secret shared between the LX unit and the RADIUS server
[1]`timeout`	The length of time that the LX unit will wait for the RADIUS server to respond before retransmitting packets to it

1. If you do not specify a UDP port, retransmit value, or timeout value for the RADIUS server, the LX unit will use the default values for these settings. For more information, refer to the applicable commands in the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide*.

RADIUS Command Examples

This section provides examples of all of the commands that are used to specify settings for the RADIUS servers. Refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide* for detailed descriptions of the commands in this chapter.

RADIUS Primary Authentication Server Commands

```
Config:0 >>radius primary authentication server address 152.34.65.33
```

Config:0 >>radius primary authentication server port 1645

Config:0 >>radius primary authentication server retransmit 3

Config:0 >>radius primary authentication server secret AaBbCc

Config:0 >>radius primary authentication server timeout 7

RADIUS Primary Accounting Server Commands

Config:0 >>radius primary accounting server address 181.28.68.56

Config:0 >>radius primary accounting server port 1646

Config:0 >>radius primary accounting server retransmit 3

Config:0 >>radius primary accounting server secret reuyyurew

Config:0 >>radius primary accounting server timeout 7

RADIUS Secondary Authentication Server Commands

Config:0 >>radius secondary authentication server address 178.67.82.78

Config:0 >>radius secondary authentication server port 1812

Config:0 >>radius secondary authentication server retransmit 3

Config:0 >>radius secondary authentication server secret AsJkirbg

Config:0 >>radius secondary authentication server timeout 7

RADIUS Secondary Accounting Server Commands

Config:0 >>radius secondary accounting server address 198.20.84.77

Config:0 >>radius secondary accounting server port 1813

Config:0 >>radius secondary accounting server retransmit 3

Config:0 >>radius secondary accounting server secret GgJjoreou

Config:0 >>radius secondary accounting server timeout 7

Specifying the RADIUS Period on the LX

The RADIUS period is the interval at which the LX unit will update the RADIUS accounting server with the status of each RADIUS user. The RADIUS period is specified in minutes. Do the following to specify the RADIUS period:

1. Access the Configuration Command Mode. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)
2. Use the `radius period` command to specify the RADIUS period; for example:

```
Config:0 >>radius period 10
```

Setting Up TACACS+

You can implement TACACS+ authentication and TACACS+ accounting at the server level and for specific interfaces and asynchronous ports on the LX unit. You must implement TACACS+ accounting and/or authentication at the server level before you can implement it on specific interfaces and asynchronous ports on the LX unit.

The basic steps for configuring TACACS+ authentication on the LX unit are:

1. Installing and configuring the TACACS+ server on a Network-based Host (see page 38).
2. Specifying the TACACS+ server settings on the LX (see page 39).
3. Specifying the TACACS+ period on the LX (see page 42).

For more information on TACACS+ authentication, refer to "Overview of TACACS+ Authentication" on page 167.

For more information on TACACS+ accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 161.

Installing and Configuring the TACACS+ Server on a Network-based Host

Before you can configure TACACS+ on your LX unit, you must configure a TACACS+ server on your network.

In general, TACACS+ server implementations are available on the Internet. These implementations generally use a daemon process that interacts with TACACS+ clients (located on LX units and on other remote access devices).

The daemon uses a list of clients and associated secrets that it shares with these clients. The per-client secret is used to encrypt and validate communications between the TACACS+ server and the client. The file used to keep the client list and secrets is the "clients" file.

Another file used by the daemon to store the users that are authenticated is the "users" file. The "users" file contains the TACACS+ attributes associated with a particular user. As a minimum, this file must contain the user's username, password (depending on the TACACS+ server used), and Service-type.

To configure the TACACS+ server, refer to your TACACS+ host documentation.

Specifying the TACACS+ Server Settings on the LX

Do the following to specify the TACACS+ server settings on the LX unit:

1. Check the primary TACACS+ Server host to ensure that the TACACS+ server client database has been configured.
2. Access the Configuration Command Mode on the LX. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)
3. Use the `tacacs+ primary authentication server address` command to specify the IP address of the TACACS+ primary authentication server; for example:

   ```
   Config:0 >>tacacs+ primary authentication server
   address 149.19.87.89
   ```

4. Use the `tacacs+ primary authentication server secret` command to specify the secret that will be shared between LX unit and the TACACS+ primary authentication server; for example:

```
Config:0 >>tacacs+ primary authentication server
secret Goitji
```

5. Use the `tacacs+ primary authentication server port` command to specify the socket your TACACS+ server is listening to; for example:

   ```
   Config:0 >>tacacs+ primary authentication server
   port 1687
   ```

   NOTE: The LX listens to port 1812 by default.

6. To verify the LX TACACS+ configuration, exit from the Configuration command mode and execute the `show tacacs+ characteristics` command at the Superuser command prompt; for example:

   ```
   InReach:0 >>show tacacs+ characteristics
   ```

   Refer to Table 1 on page 36 for descriptions of all of the settings that you can specify for a TACACS+ server.

   In order to use a TACACS+ primary accounting server, or a TACACS+ secondary server, you must specify an IP address and a secret for the respective TACACS+ server. For examples of the commands that you would use, refer to the following sections:

   - "TACACS+ Primary Authentication Server Commands" on page 41
   - "TACACS+ Secondary Authentication Server Commands" on page 42
   - "TACACS+ Secondary Accounting Server Commands" on page 42

   NOTE: The use of a TACACS+ primary accounting server, and the use of TACACS+ secondary servers, is optional.

After you have specified the TACACS+ settings for the TACACS+ primary authentication server, you can configure the TACACS+ primary accounting server and the TACACS+ secondary authentication and accounting servers.

Table 2 - TACACS+ Settings

TACACS+ Settings	Description
`address`	IP address of the TACACS+ server
[1]`port`	UDP port of the TACACS+ server
[1]`retransmit`	The maximum number of times that the LX unit will attempt to retransmit a message to the TACACS+ server
`secret`	The TACACS+ secret shared between the LX unit and the TACACS+ server
[1]`timeout`	The length of time that the LX unit will wait for the TACACS+ server to respond before retransmitting packets to it

1. If you do not specify a UDP port, retransmit value, or timeout value for the TACACS+ server, the LX unit will use the default values for these settings. For more information, refer to the applicable commands in the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide*.

TACACS+ Command Examples

This section provides examples of all of the commands that are used to specify settings for the TACACS+ servers. Refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide* for detailed descriptions of the commands in this chapter.

TACACS+ Primary Authentication Server Commands

```
Config:0 >>tacacs+ primary authentication server address
182.36.98.33
Config:0 >>tacacs+ primary authentication server port 1687
Config:0 >>tacacs+ primary authentication server retransmit 3
Config:0 >>tacacs+ primary authentication server secret Gfsufsa
Config:0 >>tacacs+ primary authentication server timeout 7
```

TACACS+ Primary Accounting Server Commands

```
Config:0 >>tacacs+ primary accounting server address 182.28.86.56
Config:0 >>tacacs+ primary accounting server port 1664
Config:0 >>tacacs+ primary accounting server retransmit 3
Config:0 >>tacacs+ primary accounting server secret iuhgeuer
Config:0 >>tacacs+ primary accounting server timeout 7
```

TACACS+ Secondary Authentication Server Commands

```
Config:0 >>tacacs+ secondary authentication server address
182.57.32.58
Config:0 >>tacacs+ secondary authentication server port 1842
Config:0 >>tacacs+ secondary authentication server retransmit 3
Config:0 >>tacacs+ secondary authentication server secret L3498reiu
Config:0 >>tacacs+ secondary authentication server timeout 7
```

TACACS+ Secondary Accounting Server Commands

```
Config:0 >>tacacs+ secondary accounting server address 182.20.56.18
Config:0 >>tacacs+ secondary accounting server port 1819
Config:0 >>tacacs+ secondary accounting server retransmit 3
Config:0 >>tacacs+ secondary accounting server secret Geihuige2
Config:0 >>tacacs+ secondary accounting server timeout 7
```

Specifying the TACACS+ Period on the LX

The TACACS+ period is the interval at which the LX unit will update the TACACS+ accounting server with the status of each TACACS+ user. This value is specified in minutes. Do the following to specify the TACACS+ period:

1. Access the Configuration Command Mode. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)
2. Use the `tacacs+ period` command to specify the TACACS+ period; for example:

```
Config:0 >>tacacs+ period 10
```

Setting Up SecurID

You can implement SecurID authentication at the server level and for specific interfaces and asynchronous ports on the LX unit. You must implement SecurID authentication at the server level before you can implement it on specific interfaces and asynchronous ports on the LX unit.

Under SecurID authentication, the user is required to enter a user name and a PIN number plus the current token code from his or her SecurID server. The LX unit transmits the information to the RSA ACE/Server, which approves access when the information is validated.

SecurID supports both DES and SDI encryption.

The basic steps for configuring SecurID authentication on the LX unit are:

1. Installing and configuring the SecurID server on a Network-based Host (see page 38).
2. Specifying the SecurID server settings on the LX (see page 39).

For more information on SecurID authentication, go to the RSA SecurID website (http://www.rsasecurity.com/products/securid/index.html).

Installing and Configuring the SecurID Server on a Network-based Host

Before you can configure SecurID on your LX unit, you must configure a SecurID server on your network. To configure the SecurID server, refer to your SecurID host documentation.

Specifying the SecurID Server Settings on the LX

Do the following to specify the SecurID server settings on the LX unit:

1. Check the primary SecurID Server host to ensure that the SecurID application is running.
2. Access the Configuration Command Mode on the LX. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)
3. Use the `securid authentication version` command to specify the SecurID authentication version for the LX unit. You can specify the authentication version as Version 5, or pre-Version 5 (legacy); for example:

   ```
   Config:0 >>securid authentication version version_5
   Config:0 >>securid authentication version legacy
   ```

4. Use the `securid authentication port` command to specify the socket your SecurID server is listening to; for example:

   ```
   Config:0 >>securid authentication port 1687
   ```

   NOTE: The LX listens to port 1812 by default.

5. Use the `securid primary authentication server address` command to specify the IP address of the SecurID primary authentication server; for example:

   Config:0 >>`securid primary authentication server address 149.19.87.89`

   NOTE: If the SecurID authentication version is "legacy", you must specify a Master authentication server instead of a Primary authentication server. For more information, refer to the `securid master authentication server address` command in the *LX-Series Commands Reference Guide*.

6. Use the `securid authentication encryption` command to specify the SecurID encryption method for the LX unit. You can specify DES or SDI as the encryption method; for example:

   Config:0 >>`securid authentication encryption des`

   Config:0 >>`securid authentication encryption sdi`

7. To verify the LX SecurID configuration, exit from the Configuration command mode and execute the `show securid characteristics` command at the Superuser command prompt; for example:

   InReach:0 >>`show securid characteristics`

SecurID Command Examples

This section provides examples of all of the commands that are used to specify settings for the SecurID servers. Refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide* for detailed descriptions of the commands in this chapter.

Config:0 >>`securid primary authentication server address 138.30.65.34`

Config:0 >>`securid authentication port 4500`

Config:0 >>`securid primary authentication server name bigsky1.com`

Config:0 >>`securid authentication encryption des`

```
Config:0 >>securid authentication retransmit 7
Config:0 >>securid authentication timeout 3
Config:0 >>securid authentication version version_5
```

Refer to Table 3 (below) for descriptions of all of the settings that you can specify for a SecurID server.

Table 3 - SecurID Settings

SecurID Settings	Description
`address`	IP address of the SecurID server
[1]`port`	UDP port of the SecurID server
[1]`retransmit`	The maximum number of times that the LX unit will attempt to retransmit a message to the SecurID server
[1]`encryption`	The encryption method for SecurID authentication on the LX unit
[1]`version`	The SecurID authentication version that will be used on the LX unit
[1]`name`	The host name of the SecurID authentication server for the LX unit
[1]`timeout`	The length of time that the LX unit will wait for the SecurID server to respond before retransmitting packets to it

1. If you do not specify a UDP port, retransmit value, timeout, version, encryption, or name for the SecurID server, the LX unit will use the default values for these settings. For more information, refer to the applicable commands in the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide*.

NOTE: If the SecurID secret on the LX unit does not match the SecurID secret on the SecurID server, you will need to clear the secret from the LX unit. To clear the SecurID secret from the LX unit, refer to the `zero securid secret` command in the *LX-Series Commands Reference Guide*.

Resetting the Unit to Factory Defaults

If you believe you have misconfigured the unit, or you believe the configuration is somehow corrupt, you may wish to reset the unit to it's factory defaults. This may be done in one of several ways:

From an LX asynchronous port:

1. Access the Configuration Command Mode. (Refer to "Configuration Command Mode" on page 18 for information on accessing the Configuration Command Mode.)
2. Enter the default Configuration command to reset the LX unit to the factory defaults; for example:

   Config:0 >>`default configuration`

   NOTE: After you enter the above command, the LX will display a confirmation prompt warning you that the unit will be rebooted. The LX unit will be defaulted, and rebooted, if you answer "yes" to the confirmation prompt.

From a web browser:

1. Browse to the LX unit's IP address, log in to the LX unit, and bring up the console.
2. Click on the 'Admin' button on the menu bar of the client and entering the Superuser password. This activates a 'Default' button on the menu bar.
3. Click on the 'Default' button to display the options to default the unit or certain other parameters.
4. Select the option to default the unit.

   NOTE: After you select a default option, the LX will display a confirmation prompt warning you that the unit will be rebooted. The LX unit will be defaulted, and rebooted, if you answer "yes" to the confirmation prompt.

From the LX DIAG port:

NOTE: This method is recommended if you no longer have network access, or if you are unable to make a serial connection to an LX asynchronous port.

1. Connect a terminal to the DIAG port of the LX unit.
2. Power-cycle the LX unit. When the unit is powered on, the ppciboot Main Menu is displayed.
3. Select the asterisk (*) from the menu to display the following options:

   ```
   [1] Reset ppciboot Configuration

   [2] Reset Linux System Configuration
   ```

4. Select `[1]` to reset the ppciboot configuration to system defaults. (**Note:** Although the ppciboot configuration will be reset to defaults, it will not be saved to flash. To save the configuration to flash, execute the `save configuration flash` command in the Superuser command mode.)
5. Select `[2]` to reset the Linux system configuration. You are prompted for the password, which is **access**. If you enter the password, the command erases all of the configurations you have saved, except for the ppciboot configuration.
6. Press `B` to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration.

Refer to “Booting from Defaults” on page 76 for further information on defaulting from ppciboot and defaulting from the CLI.

Chapter 2

Setting Up Remote Console Management

Network Elements can be managed via Telnet connections, or via SSH connections, to the LX asynchronous ports on which the network elements are attached. This method of managing network elements is known as **remote console management**. This chapter describes how to set up remote console management on an LX unit.

Setting up remote console management involves doing the following:

- Connecting the LX asynchronous port to the Network Element (see below).
- Configuring the LX asynchronous port for the remote management of the connected Network Element (see page 51).
- Setting up security for the LX asynchronous port to which the network element is connected (see page 54).
- Creating the subscriber(s) that have remote access to the asynchronous port where the Network Element is connected (see page 58).

Connecting the Console Port to the Network Element

Network elements can be connected to LX asynchronous ports by a modem or by a direct serial line. The LX asynchronous-port connectors are female RJ-45 connectors. Use a crossover cable to connect a direct serial line from an LX console port to the serial management port on a network element. Use a straight-through cable to connect a console port to a modem.

MRV Communications provides RJ-45 crossover cables. You can make the MRV-supplied RJ-45 crossover cables into straight-through cables. For more information, refer to “Making Straight-through Cables” on page 50.

Making Straight-through Cables

To make an MRV-supplied crossover cable into a straight-through cable, do the following:

- Lay the modular cable on a table or on some other flat surface. (The modular cable should lie flat with no rolls or twists in it.)
- Crimp the RJ-45 connector in opposite directions at both ends (see Figure 2).

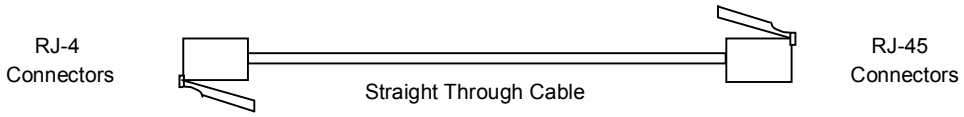

Figure 2 - Straight-through Wiring Scheme

Recommendations for Making Cables

Keep the following in mind when you make your own cables:

- **Before crimping the cables,** make sure that the RJ-45 connector is fully inserted into the die-set cavity and that the wire is fully inserted into the RJ-45 connector. (The die set might be fragile, and it could break if the RJ-45 connector is not properly seated before you squeeze the handle.)
- In order to keep track of the cable type, you should use different colored wires for straight-through and crossover cable. For example, MRV Communications recommends silver wire for making crossover cables and black wire for making straight-through cables.

NOTE: MRV Communications recommends that you not use Ethernet Xbase-T crossover or straight-through cable for serial communications.

Modular Adapters (RJ-45 to DB-25 and RJ-45 to DB-9)

You can obtain adapters with male and female DB-25 and female connectors from MRV Communications. These adapters direct signals from the RJ-45 connectors on the cable to the correct pin on the DB-25, or DB-9, connector. For more information, refer to *Getting Started with the LX Series*.

Configuring Ports for Remote Console Management

This section describes how to configure LX asynchronous ports for remote console management.

Configuring Asynchronous Ports for Direct Serial Connections

The default settings for LX asynchronous ports will support direct serial connections to most Network Elements. However, when conditions warrant, you can explicitly set an asynchronous port to non-default values.

NOTE: Autobaud must be disabled on ports that are used for remote console management. To disable autobaud on a port, execute the `no autobaud` command in the Asynchronous command mode.

Explicitly Setting LX Asynchronous Port Characteristics

It is recommended that you explicitly set the characteristics of an LX asynchronous port to match those of a directly connected Network Element. To explicitly set the characteristics of an LX asynchronous port, do the following:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to configure. (Refer to “Asynchronous Command Mode” on page 19 for information on accessing the Asynchronous Command Mode.)
2. Use the `access remote` command in to set the access for the asynchronous port to Remote; for example:

   Async 6-6:0 >>`access remote`

3. In the Asynchronous Command Mode, enter the appropriate command to set the speed, parity, data bits, stop bits, flow control, or autohangup setting for the asynchronous port.

   Table 4 lists the commands that you can use to set the port characteristics that pertain to remote console management of directly connected Network Elements. For the full syntax of each command listed in Table 4, refer to the *LX-Series Commands Reference Guide*.

Table 4 - Commands for Setting Asynchronous Port Characteristics

Port Characteristics	Allowable Values	Command Examples
autohangup	enabled or disabled	autohangup enable no autohangup
data bits	5, 6, 7, or 8	bits 6
flow control	xon or cts	flowcontrol cts flowcontrol xon
parity	even, odd, or none	parity even parity odd parity none
speed	134, 200, 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200, or 230400	speed 115200
stop bits	1 or 2	stop bits 1 stop bits 2

NOTE: MRV Communications recommends that you enable Autohangup on an LX asynchronous port that will be used to do remote console management. This ensures that the port will drop the connection, when the network element resets DTR at subscriber logout.

Setting Up Modem Ports for Remote Console Management

Do the following to set up a Modem Port for remote console management:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to set up for remote console management. (Refer to "Asynchronous Command Mode" on page 19 for information on accessing the Asynchronous Command Mode.)
2. Execute the `access remote` command to set the port access to REMOTE; for example:

   Async 5-5:0 >>`access remote`
3. Execute the `modem enable` command to enable modem control on the port; for example:

   Async 5-5:0 >>`modem enable`
4. Execute the `flow control` command to set the port flow control to CTS; for example:

   Async 5-5:0 >>`flowcontrol cts`
5. Ensure that the port is set to the same speed as the modem to which the port is attached. To set the port speed, use the `speed` command; for example:

   Async 5-5:0 >>`speed 57600`
6. Execute the `modem` command to access the Modem Command Mode for the port under configuration; for example:

   Async 5-5:0 >>`modem`
7. In the Modem Command Mode, execute the `type` command to set the Modem Type to DIALOUT; for example:

   Modem 5-5:0 >>`type dialout`

8. In the Modem Command Mode, execute the `dialout number` command to specify the number that the modem will dial to connect with the Network Element on the Public Network; for example:

   Modem 5-5:0 >>`dialout number 19785558371`

9. In the Modem Command Mode, execute the `initstring` command to specify the initialization string for the modem; for example:

   Modem 5-5:0 >>`initstring AT S7=45 S0=1 L1 V1 X4 &C1 &1 Q0 &S1`

   NOTE: The initialization string may vary between modem types.

10. In the Modem Command Mode, execute the `retry` command to specify the Retry value for the modem; for example:

    Modem 5-5:0 >>`retry 6`

11. In the Modem Command Mode, execute the `timeout` command to specify the Timeout value for the modem; for example:

    Modem 5-5:0 >>`timeout 30`

Setting Up Security for a Console Port

You can use LOCAL authentication, RADIUS authentication, SecurID authentication, or TACACS+ authentication to protect a console port from unauthorized access. These methods of authentication require a user to enter a valid username/password combination to access the console port.

Setting Up Local Authentication

Under LOCAL authentication, a username/password combination is validated against the local security database. LOCAL authentication is enabled by default on console ports. (Other authentication options on console ports are NONE, RADIUS, TACACS+, and SecurID.)

You can enable LOCAL authentication on a console port by doing the following:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to configure. (Refer to “Asynchronous Command Mode” on page 19 for information on accessing the Asynchronous Command Mode.)

2. Execute the following command to enable LOCAL authentication on the port:

```
Async 5-5:0 >>authentication outbound local enable
```

Setting Up RADIUS Authentication

Under RADIUS authentication, a username/password combination is validated against the RADIUS user and client database. The RADIUS security database is stored on the RADIUS server for the LX unit. In order to use RADIUS authentication on a port, you must have RADIUS set up for the LX unit. Refer to "Setting Up RADIUS" on page 33 for information on setting up RADIUS for the LX unit.

RADIUS authentication is disabled by default on console ports. You can enable RADIUS authentication on a console port by doing the following:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to configure. (Refer to "Asynchronous Command Mode" on page 19 for information on accessing the Asynchronous Command Mode.)
2. Execute the following command to enable RADIUS authentication on the port:

```
Async 5-5:0 >>authentication outbound radius enable
```

NOTE: If RADIUS authentication is enabled, you may want to implement a backup method (Fallback), which will be used if the RADIUS server is unreachable. Fallback switches to Local Authentication when there is no reply from the RADIUS server(s) after 3 attempts. For more information, refer to "Setting Up Fallback" on page 57.

Setting Up TACACS+ Authentication

Under TACACS+ authentication, a username/password combination is validated against the TACACS+ user and client database. The TACACS+ security database is stored on the TACACS+ server for the LX unit. In order to use TACACS+ authentication on a port, you must have TACACS+ set up for the LX unit. Refer to "Setting Up TACACS+" on page 38 for information on setting up TACACS+ on the LX unit.

TACACS+ authentication is disabled by default on console ports. You can enable TACACS+ authentication on a console port by doing the following:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to configure. (Refer to "Asynchronous Command Mode" on page 19 for information on accessing the Asynchronous Command Mode.)
2. Execute the following command to enable TACACS+ authentication on the port:

   Async 5-5:0 >>`authentication outbound tacacs+ enable`

NOTE: If TACACS+ authentication is enabled, you may want to implement a backup method (Fallback), which will be used if the TACACS+ server is unreachable. Fallback switches to Local Authentication when there is no reply from the TACACS+ server(s) after 3 attempts. For more information, refer to "Setting Up Fallback" (below).

Setting Up SecurID Authentication

Under SecurID authentication, a username/password combination is validated against the SecurID user and client database. The SecurID security database is stored on the SecurID server for the LX unit. In order to use SecurID authentication on a port, you must have SecurID set up for the LX unit. Refer to "Setting Up SecurID" on page 43 for information on setting up SecurID on the LX unit.

SecurID authentication is disabled by default on console ports. You can enable SecurID authentication on a console port by doing the following:

1. Access the Asynchronous Command Mode for the asynchronous port that you want to configure. (Refer to "Asynchronous Command Mode" on page 19 for information on accessing the Asynchronous Command Mode.)
2. Execute the following command to enable SecurID authentication on the port:

```
Async 5-5:0 >>authentication outbound securid enable
```

NOTE: If SecurID authentication is enabled, you may want to implement a backup method (Fallback), which will be used if the SecurID server is unreachable. Fallback switches to Local Authentication when there is no reply from the SecurID server(s) after 3 attempts. For more information, refer to "Setting Up Fallback" (below).

Setting Up Fallback

Fallback Authentication can be used as a mechanism for authenticating users when the configured authentication method (i.e., RADIUS, TACACS+, or SecurID) fails because the authentication server is unreachable. When a user logs in via Fallback, his or her username/password combination is validated against the LOCAL security database for the LX unit.

The LX unit will make three attempts to log in the user via RADIUS, TACACS+, or SecurID before it implements Fallback. After the third attempt at logging in via the configured authentication method (RADIUS, TACACS+, or SecurID), the username/password combination will be validated against the LOCAL security database for the LX unit.

RADIUS, TACACS+, or SecurID must be enabled on a port in order for Fallback to function on the port. When all three methods (i.e., RADIUS, TACACS+, or SecurID) are disabled on the port, Fallback is ignored by the port.

Do the following to enable Fallback on a port:

1. Access the Asynchronous Command Mode for the asynchronous port on which you want to enable Fallback. (Refer to "Asynchronous Command Mode" on page 19 for information on accessing the Asynchronous Command Mode.)
2. Execute the following command to enable Fallback authentication on the port:

```
Async 5-5:0 >>authentication fallback enable
```

Creating Subscribers for Remote Console Management

In order for a subscriber to do remote console management, he/she must have specific access rights. If RADIUS is the outbound authentication method, configure a Service-type of Outbound-User for the subscriber on the RADIUS server.

If local authentication is used, do the following to set up the neccessary access rights for the subscriber:

1. Create, or access, the subscriber record of the subscriber that you want to configure for console-port access. (Refer to "Subscriber Command Mode" on page 21 for information on creating or accessing a subscriber record.)
2. In the Subscriber Command Mode, specify one or more access methods for the subscriber to use in connecting to the LX unit. For more information, refer to "Specifying Access Methods" on page 59.
3. Execute the `access console enable` command to specify that the subscriber will have console access to the LX unit; for example:

```
Subs_mark >>access console enable
```

4. Execute the `access port` command to specify the console ports that the subscriber can access. In the following example, the `access port` command specifies that the subscriber `mark` can log on to ports 2, 3, 5, and 6:

```
Subs_mark >>access port 2 3 5 6
```

5. **If you want the subscriber to create his or her own login password,** execute the `password enable` command; for example:

   Subs_mark >>`password enable`

   When the subscriber logs in to the LX unit for the first time, he/she will be asked to enter, and confirm, his or her new password.

6. **If you want to create a login password the subscriber,** execute the `password` command; for example:

   Subs_mark >>`password`

   The following prompts are displayed:

   ```
   Enter your NEW password   :
   Re-enter your NEW password:
   ```

7. Enter the new password at the `Enter` prompt, and re-enter it at the `Re-enter` prompt. (This is the password that the subscriber will be required to enter when he/she logs on to a console port.)

Specifying Access Methods

You can specify SSH, Telnet, or the Web (or any combination of SSH, Telnet, and the Web) as the method(s) that the subscriber can use to access LX asynchronous ports for remote console management.

Because SSH includes data encryption capabilities, it is recommended as the access method for subscribers who will be sending sensitive data to the LX asynchronous ports.

Specifying Telnet As an Access Method

1. Execute the `access telnet enable` command; for example:

   Subs_mark >>`access telnet enable`

2. Execute the `telnet mode` command to set the Telnet Mode. In the following example, the Telnet Mode is set to character:

   Subs_mark >>`telnet mode character`

In the following example, the Telnet Mode is set to line:

```
Subs_mark >>telnet mode line
```

Specifying SSH As an Access Method

1. Execute the `access ssh enable` command; for example:

   ```
   Subs_mark >>access ssh enable
   ```

2. Execute the `ssh cipher` command to specify the SSH encryption type for the subscriber. In the following examples, the SSH encryption type is set to Triple-DES, ANY, and BLOWFISH respectively:

   ```
   Subs_mark >>ssh cipher triple-des
   Subs_mark >>ssh cipher any
   Subs_mark >>ssh cipher blowfish
   ```

   Refer to the `ssh cipher` command in the *LX-Series Commands Reference Guide* for more information on the Triple-DES, ANY, and BLOWFISH encryption types.

Specifying the Web As an Access Method

Execute the `access web enable` command; for example:

```
Subs_mark >>access web enable
```

Chapter 3

System Administration

This chapter explains how to upgrade the software, as well as some basic maintenance functions.

Backup and Recovery

This section explains how to save, edit, and load the configuration file.

Saving the Configuration File

The configuration file (`Config.prm`) is saved in a format that is readable in WordPad and the vi editor in UNIX. Because anyone can easily modify it, the file is signed with a digest using the SHA encryption algorithm. The SHA encryption lets the administrator know if a modified file is being loaded by issuing an alert message when a file not matching the original algorithm is being loaded. This way the administrator knows the file was modified and can take the appropriate action.

The `Config.prm` file is created when you configure the LX unit. After the `Config.prm` file has been created on one unit, it can be copied to other units. When the `Config.prm` file resides on a new unit, you can copy its contents as appropriate for the new unit. For example, you can change the IP settings (i.e., IP Address, Subnet Mask, etc.) to the IP settings of the new unit. All other settings will be imported when the LX unit is rebooted.

Where the Configuration is Stored

All files related to the unit configuration are located in the directory `/config`. This directory contains the SSH keys, Menus, Configuration, a file to tell from where the configuration is to be taken (the `ConfToBootFrom` file), and the zone information directory (time and date).

Saving the Configuration Into the Flash

To save the configuration into the flash, execute the `save configuration flash` command in the Superuser command mode; for example:

```
InReach:0 >>save configuration flash
```

Saving the Configuration to the Network

The TFTP protocol is used to save the LX configuration to a network host. Consequently, if you are saving to a UNIX host, a configuration file must already exist on the TFTP server. Use the touch command to create the configuration file as a `.zip` file. Windows-based workstations will automatically create the `.zip` file once the LX unit attempts the TFTP put process.

The configuration format differs slightly from that described in "How the Configuration is Organized." The `.zip` file contains everything previously described except for the SSH keys, since they belong to the unit itself and cannot be used on a different unit.

Since the format is a `.zip` file, it is usable by WinZip or UNIX Unzip.

Use the following command to save the configuration to the network:

```
save configuration network filename tftp_server_address
```

NOTE: The filename that you specify in the `save configuration network` command must not include a `.zip` extension.

Editing the Files on a Unix Host

You can edit the `Config.prm` file so that you can bring multiple units online at one time.

To edit the files:

1. Open the .`zip` file into the directory by entering the following command:

   `unzip filename.zip`

   The `Config.prm` file appears. If you have configured menus, the Menu file also appears.

2. Open the `Config.prm` file with any text editor (e.g., vi or emacs).
3. Select and copy the section of the `Config.prm` file that you want to modify:
   - Users that have access to all new LX units
   - PPP configurations
   - Broadcast Groups
   - Interface configurations
   - RADIUS, SecurID, or TACACS+ configurations
   - Specific Async Port configurations
4. If you are adding a new user to the `Config.prm` file, copy an existing user, paste it into the section directly below the last user, and make the necessary modifications to the copy.
5. Follow the same steps for any other changes you make to the `Config.prm` file.

Editing the Files in Windows

You can edit the `Config.prm` file so that you can bring multiple units online at one time.

To edit the files:

1. Open the `.zip` file into the directory using winzip.

The `Config.prm` file appears. If you have configured menus, the Menu file also appears.

2. Open the `Config.prm` file with the WordPad editor.
3. Select and copy the section of the `Config.prm` file that you want to modify:
   - Users that have access to all new LX units
   - PPP configurations

- Broadcast Groups
- Interface configurations
- RADIUS, SecurID, or TACACS+ configurations
- Specific Async Port configurations

4. If you are adding a new user to the `Config.prm` file, copy an existing user, paste it into the section directly below the last user, and make the necessary modifications to the copy.
5. Follow the same steps for any other changes you make to the `Config.prm` file.

Recreating the Zip File in Order to Upload It Onto the LX

NOTE: To perform this procedure, you must be in the directory in which the files to be zipped reside.

1. To recreate the zip file, type the following command in UNIX:

   ```
   zip -o filename.zip file1 file2 file3
   ```

   where `filename.zip` (you can name this whatever you want) is the archive you are writing the files to, and `file1`, `file2`, and `file3` are the files you are adding to the archive.
2. In Windows, select the files you want to add to the zip file by clicking on them while holding down the **Ctrl** key.
3. Right click on the selected files and select **Add to Zip**.

Loading the Configuration

At the `Config` prompt, load the configuration as follows:

```
Config:0:>>boot configuration from network tftp_server_address filename

Config:0:>>end

InReach:0:>>save configuration flash

InReach:0:>>reload
```

After the LX has reloaded, check the system status screen to make sure that the LX loaded from the proper place. Enter the following command:

```
InReach:0:>>show system status
```

Applying Default Configurations to Other Units

This section explains how to create a default configuration file with which you can load multiple units.

Creating a Default Configuration File

After your first LX unit is up and running, you can save the unit configuration to the network. For further information, refer to "Saving the Configuration to the Network" on page 62. You must rename this `.zip` file to `lx` *`last six digits of the mac address`*`.prm` (e.g. `lx12ab9f.prm`). Once this is complete, you can use this `.prm` file as a template to configure multiple units at one time by changing the last six digits of the mac address to reflect that of the specific unit.

Restoring the Default Configuration File to a New Unit

The unit looks on the TFTP server specified in ppciboot. If the configuration is defaulted, it is detected at startup and the unit checks that a TFTP server was passed by ppciboot. If a TFTP server is accessible, the LX unit connects to it and tries to download a default file named `lx` *`last six digits of the mac address`*`.prm` (e.g., `lx12ab9f.prm`).

If this file exists, the LX unit loads it into its configuration table. If the default file does not exist, the Quick Start menu is displayed.

Scripting On External Units

The LX unit supports Expect scripting. Expect is a common, simple, command line scripting language. You can use it to write simple scripts to automate interactive applications.

For example, you can write an Expect script that can automatically log you in, modify the IP configuration, set up the configuration for any port, make the LX unit dial out, and establish a PPP configuration to a remote site, etc. For information on the LX commands, refer to the *LX-Series Commands Reference Guide*.

How to Upgrade the Software

You can upgrade the software and enter the IP information on your LX unit via two methods, depending upon your specific needs:

- To upgrade software via the Command Line Interface, refer to "Upgrading Software with the Command Line Interface" for further instructions.
- To upgrade software via the ppciboot Menu, refer to "Upgrading Software with the ppciboot Main Menu" and "Using the IP Configuration Menu" for further instructions.

Upgrading Software and ppciboot with the Command Line Interface

NOTE: The default filename for the software is `linuxito.img`. The ppciboot filename is `ppciboot.img`.

NOTE: In superuser mode a check is performed to determine how much space is available before updating the software or ppciboot. Eight MB must be available to update software. One MB must be available to update ppciboot.

Make sure you have a TFTP server up and running, containing the software image and the ppciboot image.

To download the ppciboot from the command line interface (you must be in superuser mode), do the following:

1. Type the following and press <Enter>:

   `InReach:0>>update ppciboot` *`tftp_server_ip_address/name`*

   NOTE: If the LX unit has a TFTP server address configured, you do not need to include the TFTP server IP Address or the TFTP server name in the `update ppciboot` command.

   By default, the software stores in memory the IP address of the TFTP server from which it has booted. If this occurs, this argument becomes optional. The "`TFTP Download complete, verifying file integrity`" message appears. The loaded file is checked for integrity. If the check is successful, the "`File OK, copying boot image to flash`" message appears (if the check finds a problem, the "`Verify failed, Bad ppciboot file`" message appears). You have upgraded ppciboot. You must reboot the unit for the new ppciboot to take effect. Now you must upgrade the software.

2. Type the following and press <Enter>:

   `InReach:0>>update software` *`tftp_server_ip_address/name`*

3. Type the following and press <Enter> to save your configuration locally:

   `InReach:0>>save config flash`

   This stores the parameters.

4. Type the following and press <Enter> to save your configuration locally:

   `InReach:0>>reload`

When the reload is complete, log in again. The new software is activated.

NOTE: You can load a default configuration file from a TFTP server while the unit is at its default setting.

ppciboot Factory Default Settings

The following table lists the factory default settings.

Main Menu Configuration	Factory Default Setting
Boot from Network	yes
Save boot image to flash	no
Boot from flash	yes
Time Out, in seconds	8
IP Configuration Menu Configuration	**Factory Default Setting**
IP Assignment method #1	DHCP
IP Assignment method #2	BOOTP
IP Assignment method #3	RARP
IP Assignment method #4	User Defined

NOTE: For defaults on specific commands, refer to the *LX-Series Commands Reference Guide*.

Each LX Series unit is configured at the factory to use a default set of initialization parameters that sets all ports to operate with asynchronous ASCII terminal devices.

Upgrading Software with the ppciboot Main Menu

NOTE: At boot, the DIAG port (port 0) is used to configure the loading method (network or flash) of the Software image, ppciboot image, and the IP address assignment preferences.

This section explains how to use the ppciboot Main menu to set up the boot configuration. Use it as a reference for how to use specific menu entries. You can access the ppciboot commands through the DIAG port (port 0), the graphic user interface (GUI), or in the Configuration Command Mode of the CLI. When you set ppciboot parameters, the software is not loaded on the unit yet. Use the ppciboot menu to set load parameters that allow you to get up and running.

To access the menu, you need only connect a terminal using a console port cable to the DIAG port (port 0) and press <Enter> one or two times. The Main Menu appears:

```
Welcome to In-Reach ppciboot Version x.x
          Main Menu
[1] Boot from network:                yes
[2] Save software image to flash:     no
[3] Boot from flash:                  yes
[4] Time Out, in seconds (0=disabled): 8
[5] IP Configuration Menu
[6] Update ppciboot Firmware
[7] Ethernet Network Link
[*] Reset to System Defaults
[S] Save Configuration
[B] Boot System
Make a choice:
__
```

If you want to accept the defaults, press `B` or wait eight seconds.

At the "`Make a choice`" prompt of the Main Menu, type the number corresponding to the configuration action you want to perform. The sections that follow describe each option in detail.

Booting from the Network

The `Boot from network` option lets you boot your software image file from the network. To boot from the network:

1. Press `1` to toggle between yes and no. To boot from the network, choose `yes`.
2. Press `B` to Boot the system. Do this only after you have made all configuration changes to the LX and saved the configuration.

NOTE: MRV recommends that you leave `Boot from flash` on if you are booting from the network. By doing so, you provide a fallback method of booting in the event the network becomes unreachable.

Saving the Boot Image to Flash

The `Saving the software image to Flash` option lets you save the software image from the network to flash. To save the software image to flash:

1. Press `2` to toggle between yes and no. To save the software image to flash, choose `yes`.
2. Press `B` to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration. Booting the system can take five or more minutes.

Booting from Flash

The `Booting from Flash` option lets you boot your software image from the flash. To boot from the flash:

1. Press `3` to toggle between yes and no. To boot from flash, choose `yes`.
2. Press `B` to Boot the system. Do this only after you have configured the LX and saved the configuration.

Setting the Timeout in Seconds

The `Time Out, in seconds` option lets you set the amount of time the system waits for you to press `Boot` before booting automatically. To set the timeout (the default is eight seconds):

1. Press the number `4 (Time Out, in seconds)`.
2. An `Enter Time Out` prompt appears.
3. Add a time in seconds and press <Enter>. (**Note:** Entering 0 will disable the timeout. You should not enter 0, and thus disable the timeout, for remotely located units.)
4. **Press `S` to save the configuration**.

IP Configuration Menu

The `IP Configuration Menu` option lets you change addresses and settings if you do not want to accept the defaults. Refer to the "Using the IP Configuration Menu" section for details.

Updating the ppciboot Firmware

NOTE: Updating ppciboot firmware from the Main menu works only if you have already set up an ip address, ip mask, and TFTP server.

The `Update ppciboot Firmware` option lets you update the firmware via the Main Menu. To update ppciboot firmware:

1. Press the number `6 (Update ppciboot Firmware)`. The ppciboot firmware begins loading from the TFTP server.
2. If the firmware loads successfully (taking only a few seconds), the Main menu reappears. A verification check of the firmware is performed. If an error message appears, the ppciboot image may be corrupt.
3. **Press `S` to save the configuration**.
4. **Press `B` to boot the system**.

Setting the Speed and Duplex Mode of the Ethernet Network Link

The `Ethernet Network Link` option lets you set the speed and duplex mode of the Ethernet Network Link. To set the speed or duplex mode of your Ethernet Network Link:

1. Press the number `7 (Ethernet Network Link)`. The following speed/duplex options are displayed:

```
Auto, 100 half -for 100TX half duplex
      100 full -for 100TX full duplex
      10 half -for 10TX half duplex
      10 full -for 10TX full duplex
```

2. Select one of the speed/duplex options from the above display.
3. **Press `S` to save the configuration**.

Resetting to System Defaults

The `Reset to System Defaults` option lets you reset the unit to system defaults. To reset to the system defaults:

1. Press the asterisk (*) `(Reset to System Defaults)`. The following options appear:

```
[1] Reset ppciboot Configuration

[2] Reset Linux System Configuration
```

2. Select `1` or `2`. If you select `[1] Reset ppciboot Configuration,` the command sets the ppciboot configuration to system defaults, but it does not save the configuration to flash. If you select `[2] Reset Linux System Configuration,` you are prompted for the password, which is `access`. If you enter the password, the command erases all of the configurations you have saved, except for the ppciboot configuration.
3. Press `B` to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration.

Refer to “Booting from Defaults” on page 76 for further information on defaulting from ppciboot and defaulting from the CLI.

Saving the Configuration

The `Saving Configuration` option lets you save the ppciboot configuration. When you are finished configuring the Main menu, press `S` to save the configuration.

Booting the System

The `Boot System` option lets you boot the system. Be sure to save the configuration and choose a boot method before you boot the system. Press `B` to boot the system. Do this only after you have configured all necessary ppciboot options and saved the configuration.

Using the IP Configuration Menu

The `IP Configuration Menu` option lets you change addresses and settings if you do not want to accept the defaults. To configure the IP settings:

1. At the Main menu, enter `5` to open the IP Configuration menu.

```
          Welcome to In-Reach ppciboot Version x.x
                IP Configuration Menu

        [1] IP Assignment method #1:        DHCP
        [2] IP Assignment method #2:        BOOTP
        [3] IP Assignment method #3:        RARP
        [4] IP Assignment method #4:        User Defined
        [5] Unit IP Address:
        [6] Network mask:
        [7] Gateway:
        [8] TFTP Server IP Address:
        [S] Save Configuration
        [R] Return to Main menu
        Make a choice:
```

2. Choose the number of the field you want to change. See the following sections for specific details.

Choosing an IP Assignment Method

The `IP Assignment Method` option lets you set the method by which you want to assign IPs. To configure an IP Assignment method:

1. Press `1, 2, 3, or 4` to see the options for `IP Assignment method #1-4`:. Select the IP Assignment method you want to change, and toggle the options (DHCP, BOOTP, RARP, User Defined, and None) by repeatedly pressing the option number.
2. When you reach the option you want, stop toggling the options for that `IP Assignment method` and go on to press the numbers corresponding (2 for `IP Assignment method #2:, etc)` to the other IP Assignment methods and make the changes you want in the same way.
3. If you are finished configuring the IP settings, **press `S` to save the configuration**. The IP Configuration menu reappears. Press `R` to return to the Main Menu.

NOTE: If any of the four IP Assignment methods are set to "User Defined", you will need to complete additional configuration.

Changing the Unit IP Address

The `Unit IP Address` option lets you change the unit IP address (this applies only to the user-defined IP method). To change an IP Address:

1. Press the number `5 (Unit IP Address)`. A `Unit IP Address` prompt appears.
2. Type the new address and press <Enter>.
3. If you are finished configuring the IP settings, press `S` to save the configuration. The IP Configuration menu reappears. Press `R` to return to the Main Menu.

Changing the Network Mask

The `Network Mask` option lets you change the Network Mask (this applies only to the user-defined IP method). To change a Network Mask:

1. Press the number `6 (Network Mask)`. A `Network Mask` prompt appears.
2. Type the new network mask and press <Enter>.
3. If you are finished configuring the IP settings, press `S` to save the configuration. The IP Configuration menu reappears. Press `R` to return to the Main Menu.

Changing the Gateway Address

The `Gateway` option lets you change the Gateway address (this applies only to the user-defined IP method). To change a Gateway address:

1. Press the number `7 (Gateway)`. A `Gateway` prompt appears.
2. Type the new Gateway address and press <Enter>.
3. If you are finished configuring the IP settings, press `S` to save the configuration. The IP Configuration menu reappears. Press `R` to return to the Main Menu.

Changing the TFTP Server IP Address

The `TFTP Server IP Address` option lets you change the TFTP Server IP address (the address from where you load the boot image). This applies only to the user-defined IP method. To change the TFTP Server IP address:

1. Press the number `8 (TFTP Server IP address)`. A `TFTP Server IP address` prompt appears.
2. Type the new TFTP Server IP address and press <Enter>.
3. If you are finished configuring the IP settings, press `S` to save the configuration. The IP Configuration menu reappears. Press `R` to return to the Main Menu.

Saving the Configuration

The `Saving Configuration` option lets you save the ppciboot configuration. To save the configuration:

1. When you are finished configuring using the IP Configuration menu, press `S` to save the configuration.
2. Press `R` to return to the Main Menu.

NOTE: The `IP Assignment method #1-4` has precedence over user defined assignment, but the user defined settings are used as soon as the User Defined method comes up.

Booting from Defaults

The first time you boot a unit takes longer because the system computes the SSH keys server and client. The process takes a few minutes. The keys are saved into the flash.

You can default the configuration in two ways:

- From the Main Menu.
- From the Command Line Interface.

Depending on where you default the configuration from, the effect is not the same.

Defaulting from CLI

When you default from the CLI, only the configuration (Config.prm) is erased. The SSH keys are preserved. To default from the CLI, enter the `default configuration` command in the Configuration command mode.

Defaulting from the Main Menu

When you default from the Main Menu the entire configuration, including the SSH keys, is erased. The next reboot must take the extra time needed to recompute the SSH keys.

1. Choose the (*) Reset to System Defaults option from the ppci-boot menu.
2. Choose [2] Reset Linux System Configuration. The following display appears:

```
[2] Reset Linux system configuration
WARNING: This will erase all configuration data in
the system. Do not use unless the configuration is
unusable.
```

3. Enter the password, which is access. The Main Menu appears.
4. Press B to boot the unit. Various lines of data are displayed on the screen while the default ppciboot loads. This may take a few minutes.

NOTE: This display is generated by the operational software. The system must be booted before this occurs.

The default from ppciboot completes.

Acquiring the IP Configuration

The LX software gets its IP configuration from ppciboot or from the configuration. If the configuration is not loaded yet, the LX unit uses the IP configuration from ppciboot. Once the configuration file is found and loaded, the IP is modified according to the configuration. Therefore, if the configuration is already set, it always overrules the ppciboot configuration.

You can use two commands to display interface information. The show interface 1 status command displays the actual setting of the interface. The show interface 1 characteristics command displays the configuration for the interface. Refer to the *LX-Series Commands Reference Guide* for details on how to use these commands.

Chapter 4

Setting Up the Notification Feature

The Notification Feature is used to send syslog messages of LX system events to pagers, email addresses, cell phones, SNMP trap clients, outbound asynchronous ports, and local or remote syslogd files.

Overview of the Notification Feature

The Notification Feature uses the syslog daemon (syslogd) to generate event messages. Event Messages can be generated for events that occur in any of the Linux facilities listed in Table 5.

Table 5 - Sources of Event Messages

Facility	Description
`all`	Generate messages for all system events.
`authpriv`	The Superuser authentication process.
`daemon`	A system daemon, such as `in.ftpd`.
`kern`	The Linux kernel.
`syslog`	The syslog daemon (`syslogd`).
`user`	User processes; This is the default facility.

The event messages that are sent to any given destination can be filtered according to the facility and priority (severity level) of the message. For example, a destination could be configured to receive only those messages that originate in a daemon and have a priority of `crit`.

Table 6 lists the priorities that can be specified as filters for the Notification Feature.

Table 6 - Supported Priorities

Priority	Description
`none`	No messages will be logged. This setting effectively disables syslog for this User Profile.
`info`	Normal, informational messages
`notice`	Conditions that are not errors, but which might require specific procedures to adjust them
`warning`	A warning message
`err`	A software error condition. This is the default priority.
`crit`	A critical condition, such as a hard device error
`alert`	A condition that the system administrator needs to correct immediately, such as a corrupted system database.
`emerg`	A severe condition. This is the kind of condition that can immediately affect the users' ability to work on the LX.
`sigsnotice`	Indicates a state transition of the serial input signals CTS or DCD/DSR. **Note:** When this priority is specified, the facility for the User Profile must be set to `kern`. To set the facility for a User Profile to `kern`, refer to the `userprofile facility` command in the *LX-Series Commands Reference Guide*.

Configuring the Notification Feature

In order to use the Notification Feature, you must do the following:

- Create a **Service Profile**. A Service Profile defines a method for sending event messages to a destination. This method is typically a protocol (e.g., SMTP) or an on-board feature (e.g., outbound asynchronous ports). For most event notification processes, the Service Profile also defines the destination to which event messages will be sent. For more information, refer to "Creating Service Profiles" on page 82.
- Create a **User Profile**. A User Profile specifies a facility/priority filter for a destination. A User Profile also specifies the destinations (i.e., addresses and telephone numbers) for event notification processes that send event messages by email, cell phones, and pagers. For more information on User Profiles, refer to "Overview of User Profiles" on page 88.

Service Profiles

A Service Profile must be created for each desired method of sending event messages to a destination. For example, to send event messages to pagers via the Telocator Alphanumeric Protocol (TAP), a Service Profile of the TAP type must first be created. A Service Profile must be fully configured, as described in "Creating Service Profiles" on page 82, before a User Profile can be associated with it.

You can create more than one Service Profile for each method of sending event messages. For example, you can create several Service Profiles of the TAP type, with each Service Profile specifying a different Short Message Service Center (SMSC) for sending messages.

In the Notification Command Mode, you can create Service Profiles of the following types:

- **SNPP** – Used to send event messages to pagers with the Simple Network Pager Protocol (SNPP) (see "Configuring SNPP Service Profiles" on page 84).

- **WEB** – Used to send event messages to pagers or cell phones via a Web Driver (see "Configuring WEB Service Profiles" on page 86).
- **TAP** – Used to send event messages to pagers via TAP (see "Configuring TAP Service Profiles" on page 84).
- **SNMP** – Used to send event messages to SNMP trap clients (see "Creating Service Profiles" on page 82).
- **LOCALSYSLOG** – Used to send event messages to a local file on the LX unit (see "Configuring LOCALSYSLOG Service Profiles" on page 83).
- **REMOTESYSLOG** – Used to send event messages to syslogd on a remote host (see "Configuring REMOTESYSLOG Service Profiles" on page 86).
- **ASYNC** – Used to send event messages to outbound asynchronous ports on the LX unit (see "Configuring ASYNC Service Profiles" on page 85). Users can receive the event messages by logging in to the outbound asynchronous port. Under this method, syslog messages will be sent out the specified asynchronous port(s) as they occur.
- **SMTP** – Used to send event messages to email addresses (see "Configuring SMTP Service Profiles" on page 87).

Creating Service Profiles

To create a Service Profile, do the following:

1. Access the Notification Command Mode. (Refer to "Notification Command Mode" on page 23 for information on accessing the Notification Command Mode.)
2. Use the `serviceprofile protocol` command to create a Service Profile. For example, the following command creates a Service Profile called `Skytel`, using the SNPP protocol:

   Notification:0 >>`serviceprofile Skytel protocol snpp`

   You can use the `serviceprofile protocol` command to create a Service Profile of any of the following types: SNPP, WEB, TAP, SNMP, LOCALSYSLOG, REMOTESYSLOG, ASYNC, or SMTP.

3. Configure the Service Profile. This step will vary, depending on the type of the Service Profile. For more information, refer to the following sections:
   - "Configuring LOCALSYSLOG Service Profiles" on page 83
   - "Configuring SNPP Service Profiles" on page 84
   - "Configuring TAP Service Profiles" on page 84
   - "Configuring ASYNC Service Profiles" on page 85
   - "Configuring REMOTESYSLOG Service Profiles" on page 86
   - "Configuring WEB Service Profiles" on page 86
   - "Configuring SMTP Service Profiles" on page 87

NOTE: SNMP Service Profiles do not require any configuration after they are created with the `serviceprofile protocol` command. However, in order for an SNMP trap client to receive event messages from an LX unit, it must be a Version 1 trap client with a community name of `public`. For more information, refer to the `trap client version` command, and the `trap client community` command, in the *LX-Series Commands Reference Guide*.

Configuring LOCALSYSLOG Service Profiles

After you have created a LOCALSYSLOG Service Profile, you can use the `serviceprofile file` command to specify the local file to which the event messages will be sent; for example:

```
Notification:0 >>serviceprofile local file Build5
```

The local syslog writes event messages to the default directory `/var/log`. To read the contents of the file, go to `/var/log/<filename>` in the shell. For example, you would go to `/var/log/Build5` to read the contents of the local file specified in the above `serviceprofile file` command.

You can create User Profiles to filter, by facility and priority, the event messages that will be sent to the local file. For more information, refer to "Creating a User Profile" on page 88.

Configuring SNPP Service Profiles

After you have created an SNPP Service Profile, you can configure it by doing the following:

1. Use the `serviceprofile server` command to specify the SNPP server to which syslogd will send the log messages. (The pager messages will be forwarded to the user by the service provider's server.) The service provider's server can be specified as an IP Address or as any symbolic name that can be resolved by DNS; for example:

   Notification:0 >>`serviceprofile Skytel server snpp.Skytel.com`

NOTE: If you specify a symbolic name (e.g., `snpp.Skytel.com`) as the SNPP server, you must have a primary DNS server, and a domain name suffix, configured for the LX unit. For more information, refer to the `primary dns` command, and the `domain name` command, in the *LX-Series Commands Reference Guide*.

2. Use the `serviceprofile port` command to specify the LX TCP port that will be used to send messages to the SNPP server; for example:

   Notification:0 >>`serviceprofile Skytel port 7777`

In order to send messages to a pager, you must create a User Profile that specifies the pager pin number as its contact field. For more information, refer to "Creating a User Profile" on page 88.

Configuring TAP Service Profiles

After you have created a TAP Service Profile, you can configure it by doing the following:

1. Use the `serviceprofile smsc` command to specify the SMSC that will be used to send the event messages to the pager; for example:

   Notification:0 >>`serviceprofile verizon smsc 18668230501`

2. Use the `serviceprofile parity` command to specify the bit parity setting for the Service Profile; for example:

   Notification:0 >>`serviceprofile verizon parity even`

3. Use the `serviceprofile bits` command to specify the bits-per-byte setting for the Service Profile; for example:

   Notification:0 >>`serviceprofile verizon bits 7`

4. Use the `serviceprofile stopbits` command to specify the stop bits setting for the Service Profile; for example:

   Notification:0 >>`serviceprofile verizon stopbits 2`

   NOTE: The bits-per-byte setting, and the stop bits setting, that you specify for a Service Profile, must match the bits-per-byte setting of any modem port specified in a User Profile based on this Service Profile. Refer to "Creating a User Profile" on page 88 for more information on specifying a modem port for a User Profile.

In order to send event messages to a pager or cell phone via TAP, you must create a User Profile that specifies the cell phone number to which event messages will be sent, as well as the LX modem port that will be used to send the event messages to the SMSC. For more information, refer to "Creating a User Profile" on page 88.

Configuring ASYNC Service Profiles

After you have created an ASYNC Service Profile, you can use the `serviceprofile async port` command to specify the outbound asynchronous ports to which event messages will be sent; for example:

Notification:0 >>`serviceprofile serialport async port 5 7`

You can create User Profiles to filter, by facility and priority, the event messages that will be sent to the outbound asynchronous ports. For more information, refer to "Creating a User Profile" on page 88.

Configuring REMOTESYSLOG Service Profiles

After you have created a REMOTESYSLOG Service Profile, you can use the `serviceprofile host` command to specify the remote UNIX host to which the event messages will be sent; for example:

```
Notification:0 >>serviceprofile syslogvenus host 10.179.170.253
```

Do the following on the UNIX host that you specify in the `serviceprofile host` command:

1. Edit the file `/etc/syslog.conf` and add the following entry for `user.warning`:

   ```
   user.warning /tftpboot/test/user.warning.log
   ```

2. Create an empty log file as follows:

   ```
   #touch /tftpboot/test/user.warning.log
   #chmod 777 /tftpboot/test/user.warning.log
   ```

3. Restart the syslog daemon to make changes to the `syslog.conf` file take effect:

   ```
   # ps –ef|grep syslog
   # kill –HUP pid#
   ```

You can create User Profiles to filter, by facility and priority, the event messages that will be sent to the remote host. For more information, refer to “Creating a User Profile” on page 88.

Configuring WEB Service Profiles

After you have created a WEB Service Profile, you can use the `serviceprofile driver` command to specify the web driver that will be used to send the event messages to the pager or cell phone; for example:

```
Notification:0 >>serviceprofile freds driver VERIZON_WEB
```

The supported web drivers are ATT_WEB, CELLNET_WEB, CINGULAR_WEB, ORANGE_WEB, PAGENET_WEB, PROXIMUS_WEB, and VERIZON_WEB.

NOTE: You must set the date and time for the LX unit, or some wireless providers will reject event messages that are sent from it. To set the date and time for the LX unit, refer to the date command and the clock command in the *LX-Series Commands Reference Guide*.

In order to send event messages to a pager or cell phone via a Web Driver, you must create a User Profile that specifies the pager number or cell phone number as its contact field. For more information, refer to "Creating a User Profile" on page 88.

Configuring SMTP Service Profiles

After you have created an SMTP Service Profile, you can use the `serviceprofile server` command to specify the SMTP server to which syslogd will send the log messages. (The messages will be forwarded by the server to a specific email address.) The server can be specified as an IP Address or as any symbolic name that can be resolved by DNS; for example:

```
Notification:0 >>serviceprofile mrvemail server 10.179.176.21
```

NOTE: If you specify a symbolic name (e.g., `mrv.com`) as the SMTP server, you must have a DNS server configured for the LX unit. Refer to the `primary dns` command in the *LX-Series Commands Reference Guide* for more information on configuring a DNS server for the LX unit. (In addition, the LX unit will need to have a fully qualified domain name suffix.)

In order to send messages to an email address, you must create a User Profile that specifies the email address as its contact field. For more information, refer to "Creating a User Profile" on page 88.

Overview of User Profiles

A User Profile filters event messages by the type (facility) and severity level (priority) of the event message. A User Profile also specifies the destinations (i.e., addresses and telephone numbers) for event notification processes that send event messages by email, cell phones, and pagers. The LX unit supports a maximum of 20 User Profiles.

Creating a User Profile

Do the following to create a User Profile:

1. Access the Notification Command Mode. (Refer to "Notification Command Mode" on page 23 for information on accessing the Notification Command Mode.)

2. Use the `userprofile serviceprofile` command to create a User Profile; for example:

   ```
   Notification:0 >>userprofile adminscell serviceprofile
   verizon
   ```

   NOTE: You must create, and link, a User Profile to an existing Service Profile. In the above example, the User Profile `adminscell` is created, and linked to, the Service Profile `verizon`.

3. If the User Profile is for a Service Profile of the SNPP, SMTP, TAP, or WEB type, you must use the `userprofile contact` command to specify the contact field for the User Profile; for example:

   ```
   Notification:0 >>userprofile adminscell contact 9785552222
   ```

   The contact field specifies the destination (e.g., pager, cell phone, etc.) for User Profiles that are created for Service Profiles of the SNPP, SMTP, TAP, or WEB type. The allowable values for this field are the following:

   - **Pager Pin Number** (e.g., `8875551212`) for User Profiles that are based on Service Profiles of the SNPP type.
   - **Email Address** (e.g., `jstraw@mrv.com`) for User Profiles that are based on Service Profiles of the SMTP type.

- **Pager Number or Telephone Number** (e.g., `9785552222`) for User Profiles that are based on Service Profiles of the TAP or WEB type.

4. Use the `userprofile priority` command to specify a priority characteristic for the User Profile; for example:

   Notification:0 >>`userprofile adminscell priority warning`

   The allowable values for the priority characteristic are info, notice, warning, err, crit, alert, emerg, and none.

5. Use the `userprofile facility` command to specify a facility characteristic for the User Profile; for example:

   Notification:0 >>`userprofile adminscell facility user`

   Event messages that originate from the specified facility, and have the specified priority (see step 4), will be sent to the destination. The allowable values for the facility characteristic are authpriv, daemon, kern, syslog, user, and all.

6. If the User Profile is for a Service Profile of the TAP type, you must use the `userprofile modem port` command to specify the modem port that the LX unit will use to send event messages to the SMSC; for example:

   Notification:0 >>`userprofile adminscell modem port 17`

Displaying Information on the Notification Feature

This section describes how to display information about the Notification feature. The information that can be displayed includes the characteristics of Service Profiles and the characteristics of User Profiles.

Displaying Characteristics of Service Profiles

Use the `show notification serviceprofile` command, in the Superuser Command Mode, to display the characteristics of Service Profiles; for example:

InReach:0 >>`show notification serviceprofile jacklocal`

In the above example, the characteristics are displayed for the Service Profile `jacklocal`. Use the following syntax to display the characteristics of *all* Service Profiles on the LX unit:

```
InReach:0 >>show notification serviceprofile all
```

Figure 3 shows an example of the Service Profile display.

```
ServiceProfile: syslog Protocol: localsyslog
File: syslog

ServiceProfile: messages Protocol: localsyslog
File: messages

ServiceProfile: jackremote Protocol: remotesyslog
Remote Host:

ServiceProfile: jackasync Protocol: async
Async Port: 5

ServiceProfile: jack Protocol: tap
SMSC: 18668230501 Bits/Parity/StopBits:8N1
Modem Port(s): 33

ServiceProfile: webjack Protocol: web
Driver: verizon_web
```

Figure 3 - Service Profile Display

Displaying Characteristics of User Profiles

Use the `show notification userprofile` command, in the Superuser Command Mode, to display the characteristics of User Profiles; for example:

```
InReach:0 >>show notification userprofile grogers
```

In the above example, the characteristics are displayed for the User Profile `grogers@mrv`. Use the following syntax to display the characteristics of *all* User Profiles on the LX unit:

```
InReach:0 >>show notification userprofile all
```

Figure 4 shows an example of the User Profile display.

```
UserProfile: messages ServiceProfile: messages
Contact:
Facility: all Priority: notice

UserProfile: debug ServiceProfile: debug
Contact:
Facility: all Priority: debug

UserProfile: grogers@mrv ServiceProfile: N/A
Contact:
Facility: kern Priority: emerg

UserProfile: mark ServiceProfile: N/A
Contact:
Facility: kern Priority: emerg
```

Figure 4 - User Profile Display

Configuration Examples

This section contains examples of each type of Service Profile. Each example includes the commands for creating the Service Profile, along with the commands for creating a User Profile based on the Service Profile.

Localsyslog Example

The following commands configure the logging of events to the local syslogd:

Notification:0 >>`serviceprofile local protocol localsyslog`
Notification:0 >>`serviceprofile local file Build5`
Notification:0 >>`userprofile locallog service local`
Notification:0 >>`userprofile locallog facility user`
Notification:0 >>`userprofile locallog priority warning`

NOTE: In the above example, the `locallog` home directory is `/var/log/Build5`.

Outbound Asynchronous Port Example

The following commands forwards the logging of events to ports 5, 6, and 7:

```
Notification:0 >>serviceprofile 3serialport protocol async
Notification:0 >>serviceprofile 3serialport async port 5 6 7
Notification:0 >>userprofile serialport service 3serialport
Notification:0 >>userprofile serialport facility user
Notification:0 >>userprofile serialport priority warning
```

Remotesyslog Example

The following commands configure the logging of events to syslogd on a remote host:

```
Notification:0 >>serviceprofile Rlogvenus protocol
remotesyslog
Notification:0 >>serviceprofile Rlogvenus host
10.179.170.253
Notification:0 >>userprofile venus service Rlogvenus
Notification:0 >>userprofile venus facility user
Notification:0 >>userprofile venus priority warning
```

After you executed the above commands, you would do the following ***on the remote host***:

1. Add the following entry to the `/etc/syslog.conf` file:

   ```
   user.warning     /tftpboot/log/user.warning.log
   ```

2. Create an empty log file as follows:

   ```
   #touch /tftpboot/log/user.warning.log
   #chmod 777 /tftpboot/log/user.warning.log
   ```

3. Restart the syslog daemon, using the following commands, to make changes to the syslog.conf take effect.

   ```
   # ps –ef|grep syslog
   # kill –HUP pid#
   ```

SNPP Example

The following commands configure the logging of events to a text pager:

```
Notification:0 >>serviceprofile Skytel protocol snpp
Notification:0 >>serviceprofile Skytel server snpp.Skytel.com
Notification:0 >>serviceprofile Skytel port 7777
Notification:0 >>userprofile johnpager service Skytel
Notification:0 >>userprofile johnpager contact 8875551212
Notification:0 >>userprofile johnpager facility user
Notification:0 >>userprofile johnpager priority warning
```

NOTE: In order to resolve the provider's address, DNS must be configured on the LX unit.

TAP Example

The following sequence of commands could be used to configure the logging of events via a wireless provider such as Verizon, Sprint, or AT&T:

```
Notification:0 >>serviceprofile verizon protocol tap
Notification:0 >>serviceprofile verizon  SMSC 18668230501
```
(provider's service phone #)
```
Notification:0 >>serviceprofile  verizon bits 7
Notification:0 >>serviceprofile verizon  stopbit 1
Notification:0 >>serviceprofile verizon  parity even
Notification:0 >>userprofile gina'scell service verizon
Notification:0 >>userprofile gina'scell contact 785551212
Notification:0 >>userprofile gina'scell facility user
Notification:0 >>userprofile gina'scell priority warning
Notification:0 >>userprofile gina'scell modem port 17
Notification:0 >>exit
```

Now configure the modem port that will be used for sending messages:

```
Config>>port async 17
Async 17-17:0 >>no apd
```

```
Async 17-17:0 >>access remote
Async 17-17:0 >>modem
Modem>>modem enable
Modem>>type dialout
```

A list of wireless SMSC phone numbers is provided here for your convenience:

Carrier	SMSC Number	Email Address SMSC Phone#@
AT&T 7, 1, e	800-841-8837	@mobile.att.net
Cingular 7, 1, e	800-909-4602	@Cingular.com
Nextel 7, 1, e	801-301-6683	@messaging.nextel.com
Sprint 7, 1, e	888-656-1727	@sprintpcs.com
Verizon 7, 1, e, 8, 1, n	866-823-0501	@vtext.com
Skytel 8, 1, n	800-679-2778	pin@skytel.com

NOTE: MRV Communications is not responsible for these SMSC phone numbers and cannot guarantee their service. Please contact your provider for a number near you.

SNMP Example

The following commands configure the logging of events to an SNMP trap client (the LX unit must first have a trap client configured):

```
Snmp:0 >>trap client 0 10.179.170.57
Snmp:0 >>trap client 0 community public
Snmp:0 >>trap client 0 version 1
```

The Service Profile and the User Profile can then be created in the Notification Command Mode:

```
Notification:0 >>serviceprofile ricksnmp protocol snmp
Notification:0 >>userprofile ricksnmp service ricksnmp
```

Notification:0 >>`userprofile ricksnmp facility user`
Notification:0 >>`userprofile ricksnmp priority warning`

Email Example

The following commands configure the logging of events to an email address:

Notification:0 >>`serviceprofile youremail protocol smtp`
Notification:0 >>`serviceprofile youremail server 10.10.10.21`
Notification:0 >>`userprofile jsmith service youremail`
Notification:0 >>`userprofile jsmith contact 785551111@vtext.com` (verizon text phone)
Notification:0 >>`userprofile jsmith facility user`
Notification:0 >>`userprofile jsmith priority warning`

NOTE: You may need to configure the LX with a Domain suffix, a DNS server address, and a primary gateway address.

Web Example

The following commands configure the logging of events to a web driver:

Notification:0 >>`serviceprofile cingular protocol web`
Notification:0 >>`serviceprofile cingular driver cingular_web`
Notification:0 >>`userprofile kevin service cingular`
Notification:0 >>`userprofile kevin contact 9785551313`
Notification:0 >>`userprofile kevin facility user`
Notification:0 >>`userprofile kevin priority warning`

NOTE: The date and time must be set for the LX unit. (If the date and the time are *not* set, some wireless providers will reject the message.) The date and time are set with the `date` and `clock` commands in the Configuration Command Mode. The supported web drivers can be retrieved from the CLI help.

Chapter 5

Configuring the Data Broadcast Feature

The Data Broadcast Feature allows you to specify ports as Slave Ports that receive data broadcasts from, and send data broadcasts to, Master Ports on the same LX unit. Any asynchronous port, or TCP port, on the LX unit can be configured as a Slave Port or a Master Port. The source of the data broadcast can be a direct serial connection, or a Telnet connection, to a Master Port. Users can receive data broadcasts by Telneting to a TCP port that is configured as a Slave Port.

All Slave Ports and Master Ports belong to a **Broadcast Group**. The Slave Ports in a Broadcast Group can only receive data broadcasts from a Master Port in the same Broadcast Group.

When a port is configured as a Slave Port, it can still receive data from sources other than the Master Ports in its Broadcast Group. By default, any data that a Slave Port receives is forwarded to the Master Ports in the Broadcast Group. The Master Ports then broadcast the data to the Slave Ports in the Broadcast Group.

Setting Up Broadcast Groups

Do the following to set up a Broadcast Group:

1. Access the Configuration Command Mode in the LX CLI. (For more information, refer to "Configuration Command Mode" on page 18.)
2. Use the `broadcast group` command to create a Broadcast Group; for example:

```
Config:0 >>broadcast group 4
BrGroups 4:0 >>
```

This enters the Broadcast Group Command Mode. In the above example, the Broadcast Group Command prompt (**BrGroups 4:0 >>**) indicates that you are in the Broadcast Group Command Mode for Broadcast Group 4.

3. Use the `master port` command to specify the Master Ports for the Broadcast Group; for example:

```
BrGroups 4:0 >>master port async 5
BrGroups 4:0 >>master port tcp 1500
```

In the above example, asynchronous port 5, and TCP port 1500, are specified as Master Ports for Broadcast Group 4.

4. Use the `slave port` command to specify the Slave Ports for the Broadcast Group; for example:

```
BrGroups 4:0 >>slave port async 4 6 7
BrGroups 4:0 >>slave port tcp 2500
```

In the above example, asynchronous port 4, 6, and 7, and TCP port 2500, are specified as Slave Ports for Broadcast Group 4.

5. Use the `mode` command to specify the Telnet mode for the Broadcast Group; for example:

```
BrGroups 4:0 >>mode line
```

In the above example, the Telnet mode is specified as `line`; the Telnet mode can also be specified as `character`.

6. Use the `exit` command to return to the Configuration Command Mode; for example:

```
BrGroups 4:0 >>exit
Config:0 >>
```

7. Use the `broadcast group enable` command to enable the Broadcast Group that you just created; for example:

```
Config:0 >>broadcast group 4 enable
```

NOTE: In order to enable a Broadcast Group, the Broadcast Group must contain at least one Master Port and one Slave Port.

Usage Guidelines

Keep the following in mind as you add Slave Ports and Master Ports to a Broadcast Group:

- You cannot specify a the DIAG port (port 0) as a Slave Port or a Master Port.
- A maximum of 20 ports, including Masters and Slaves, can be configured for a Broadcast Group.
- You cannot add a port to a Broadcast Group if it is already a member of another Broadcast Group.
- A TCP port that is already in use cannot be added to a Broadcast Group.
- No more than one TCP socket may be open on a single TCP port.
- A maximum of 16 TCP ports can be configured for a Broadcast Group.
- To prevent data overruns, it is recommended that the Master Port(s) and Slave Port(s) in a Broadcast Group be set to the same port speed.

Specifying Port Options

You can specify that a timestamp will be appended to each line of data that is broadcast from a Master Port. You can also specify that non-broadcast data will be discarded by Slave Ports and that Slave Ports will echo any data that comes into them. This section describes how to configure these features.

Appending a Timestamp

Use the `timestamp` option of the `master port` command to specify that a timestamp will be appended to each line of data that is broadcast from a Master Port; for example:

```
BrGroups 4:0 >>master port async 4 6 7 timestamp
```

Discarding Non-Broadcast Data

By default, any data that a Slave Port receives is forwarded to the Master Port(s) in the Broadcast Group. This data is then broadcast to all of the Slave Ports in the Broadcast Group.

However, you can configure Slave Port(s) to discard data without forwarding it to the Master Port(s). To do this, specify the `discard` option in the `slave port` command; for example:

```
BrGroups 4:0 >>slave port async 5 7 discard
BrGroups 4:0 >>slave port tcp 2500 discard
```

In the above example, the `discard` option is specified for the asynchronous ports 5 and 7 and the TCP port 2500, in the Broadcast Group 4.

Echoing Incoming Data at Slave Ports

Use the `localecho` option in the `slave port` command to specify that Slave Ports will echo any data that comes into them; for example:

```
BrGroups 4:0 >>slave port async 5 7 localecho
```

Removing Ports from Broadcast Groups

To remove Master Ports from a Broadcast Group, execute the `no master port` command in the Broadcast Group Command Mode; for example:

```
BrGroups 4:0 >>no master port async 5
BrGroups 4:0 >>no master port tcp 1500
```

In the above examples, asynchronous port 5 and TCP port 1500 are removed from Broadcast Group 4.

To remove Slave Ports from a Broadcast Group, execute the `no slave port` command in the Broadcast Group Command Mode; for example:

```
BrGroups 4:0 >>no slave port async 7
BrGroups 4:0 >>no slave port tcp 2500
```

In the above examples, asynchronous port 7 and TCP port 2500 are removed from Broadcast Group 4.

To verify that Master Ports or Slave Ports have been deleted from a Broadcast Group, execute the `show broadcast group characteristics` command. (The deleted ports will not be listed in the Broadcast Group Characteristics Display.) For more information on the `show broadcast group characteristics` command, refer to "Displaying Broadcast Group Characteristics" on page 101.

NOTE: You can not delete a Broadcast Group. In lieu of deleting a Broadcast Group, you can remove all of the ports from the Broadcast Group and then disable the broadcast Group.

Disabling Broadcast Groups

To disable a Broadcast Group, execute the `no broadcast group` command in the Configuration Command Mode; for example:

```
Config:0 >>no broadcast group 4
```

In the above example, Broadcast Group 4 is disabled.

Displaying Broadcast Group Characteristics

This section describes how to display information about Broadcast Groups. The information includes Broadcast Group characteristics and Broadcast Group Summaries.

Displaying Broadcast Group Characteristics

Use the `show broadcast group characteristics` command to display the characteristics of Broadcast Groups; for example:

```
InReach:0 >>show broadcast group 1 characteristics
```

In the above example, the Broadcast Group characteristics are displayed for Broadcast Group 1. Use the following syntax to display the Broadcast Group characteristics of *all* Broadcast Groups on the LX unit:

```
InReach:0 >>show broadcast group all characteristics
```

Figure 5 shows an example of the Broadcast Group Characteristics Display.

```
  Time: 08 Nov 2002 16:29:26 US/EASTERN
  Broadcast Group Number:            1  Mode:
 Line Mode
  State:                       Disabled
  Async Master port(s) with Timestamp:

  Async Master port(s) without Timestamp:
   1,4
  TCP Master port(s) with Timestamp:

  TCP Master port(s) without Timestamp:

  Async Slave port(s) with Discard:

  Async Slave port(s) without Discard:
   2-3,5-7
  Async Slave port(s) with Local Echo:

  Async Slave port(s) without Local Echo:
   2-3,5-7
  TCP Slave port(s) with Discard:

  TCP Slave port(s) without Discard:

  TCP Slave port(s) with Local Echo:

  TCP Slave port(s) without Local Echo:
```

Figure 5 - Broadcast Group Characteristics Display

Displaying Broadcast Group Summaries

Use the `show broadcast group summary` command, in the Superuser Command Mode, to display summary information for all Broadcast Groups on the LX unit; for example:

InReach:0 >>`show broadcast group summary`

Figure 6 shows an example of the Broadcast Group Summary Display.

```
Broadcast group number:                    State:

                        1                  Enabled
                        2                  Disabled
                        3                  Disabled
                        4                  Disabled
                        5                  Disabled
```

Figure 6 - Broadcast Group Summary Display

Chapter 6

Configuring IP Interfaces

An IP interface is a logical interface for accessing the LX unit from a network. You can configure up to 4 IP interfaces on an LX unit. Each IP interface has its own IP characteristics.

You can access an LX unit via the Address of the IP interface, or by the ppciboot (server) Address of the LX unit. The network treats an IP interface as a network element that is no different from an actual server.

For example, you could have an LX unit with an IP address of 117.19.23.5, a Broadcast address of 117.255.255.255, and the subnet mask of 255.0.0.0 in ppciboot. You could then create the IP interfaces shown in Table 7 for the LX unit.

Table 7 - IP Interface Examples

Interface Number	IP Address	Broadcast Address	Subnet Mask
1	119.20.112.3	119.255.255.255	255.0.0.0
2	124.45.65.23	119.255.255.255	255.0.0.0
3	178.123.87.123	119.255.255.255	255.0.0.0

This would enable you to include the LX unit in three different networks (i.e., 119.20.112.0, 124.45.65.0, and 178.123.87.0).

IP interfaces can be configured as rotaries. For more information, refer to “Configuring Rotaries” on page 113.

An IP interface has the same subscriber database as the LX unit on which it was created. A subscriber can connect to asynchronous ports, or virtual ports, on the LX unit via an IP interface. IP interfaces support SSH and Telnet as methods for connecting subscribers to the LX unit. Refer to "Specifying the Subscriber Access Methods" on page 123 for more information.

You can authenticate connections via IP interfaces with the same authentication methods that are configured for the LX unit (LOCAL, RADIUS, TACACS+, or SecurID). However, you must enable the authentication method on the IP interface before you can use it on the IP interface. (For more information, refer to "Configuring Local Authentication on an IP Interface" on page 110 and "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface" on page 110.)

Setting Up IP Interfaces

IP interfaces are created and configured in the Interface Command Mode. You can enter the Interface Command Mode by executing the `interface` command in the Configuration Command Mode. When you are in the Interface Command Mode, the Interface Command prompt (e.g., `Intf 1-1:0 >>`) is displayed.

To configure an IP interface, do the following:

1. Execute the `interface` command in the Configuration Command Mode; for example:

   ```
   Config:0 >>interface 1
   ```

   This enters the Interface command mode for the specified IP interface (IP interface 1 in the above example).

2. Use the `address` command to specify an IP Address, and Subnet Mask, for the interface; for example:

   ```
   Intf 1-1:0 >>address 119.20.112.3 mask 255.0.0.0
   ```

   In the above example, the IP Address is specified as 119.20.112.3 and the subnet Mask is specified as 255.0.0.0.

3. Use the broadcast command to specify the Broadcast Address for the IP interface; for example:

   Intf 1-1:0 >>`broadcast 119.255.255.255`

4. Configure an authentication method (LOCAL, RADIUS, TACACS+, or SecurID) for the IP interface. For more information, refer to the following sections:

   - "Configuring Local Authentication on an IP Interface" on page 110
   - "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface" on page 110

   Refer to the following sections to configure optional parameters for an IP interface:

   - "Specifying SSH Keepalive Parameters" on page 107
   - "Specifying Socket Numbers" on page 108
   - "Specifying Maximum Transmission Units (MTU)" on page 109

Specifying SSH Keepalive Parameters

The SSH Keepalive Count is the number of times that an SSH client will attempt to make an SSH connection to an IP interface. The SSH Keepalive Interval is the length of time, in seconds, between attempts at making an SSH connection to the IP interface.

Specifying the SSH Keepalive Count

To specify the SSH Keepalive Count, execute the `ssh keepalive count` command; for example:

Intf 1-1:0 >>`ssh keepalive count 8`

Specifying the SSH Keepalive Interval

To specify the SSH Keepalive Count, execute the `ssh keepalive interval` command; for example:

Intf 1-1:0 >>`ssh keepalive interval 30`

Specifying Socket Numbers

IP interfaces have a default SSH Socket Number of 22 and a default Telnet Socket Number of 23. Table 8 lists the default SSH and Telnet Socket Numbers for LX serial ports.

Table 8 - Default Socket Numbers for Serial Ports

LX Serial Port	Default Telnet Port	Default SSH Port
0	0	0
1	2100	2122
2	2200	2222
3	2300	2322
4	2400	2422
5	2500	2522
6	2600	2622
7	2700	2722
8	2800	2822

This section describes how to specify SSH Socket Numbers and Telnet socket Numbers for IP interfaces and LX (asynchronous) ports. This is typically done to prevent hackers from accessing LX ports via default SSH Socket Numbers or default Telnet Socket Numbers.

Specifying a Telnet Socket Number for a Serial Port

To specify a Telnet Socket Number for a serial port, execute the `serial` command with the `telnet` modifier; for example:

```
Intf 1-1:0 >>serial 6 ssh 1297
```

In the above example, the Telnet Socket Number for serial port `6` is set to `1297`.

Specifying an SSH Socket Number for a Serial Port

To specify an SSH Socket Number for a serial port, execute the `serial` command with the `ssh` modifier; for example:

```
Intf 1-1:0 >>serial 4 ssh 983
```

In the above example, the SSH Socket Number for serial port `4` is set to `983`.

Specifying a Virtual Port Socket Number for SSH

To specify the Virtual Port Socket Number for making an SSH connection to the IP interface, execute the `ssh port` command; for example:

```
Intf 1-1:0 >>ssh port 988
```

In the above example, the Virtual Port Socket Number for making an SSH connection to the IP interface is set to `988`.

Specifying a Virtual Port Socket Number for Telnet

To specify the Virtual Port Socket Number for making a Telnet connection to the IP interface, execute the `telnet port` command; for example:

```
Intf 1-1:0 >>telnet port 1743
```

In the above example, the Virtual Port Socket Number for making a Telnet connection to the IP interface is set to `1743`.

Specifying Maximum Transmission Units (MTU)

The Maximum Transmission Units (MTU) is the maximum size (in bytes) of frames that can be transmitted on the IP interface. Frames that are larger than the designated MTU size are fragmented before transmission. (Note that the software fragments frames on the transmit side only.)

Use the `mtu` command to specify the MTU for an IP interface; for example:

```
Intf 1-1:0 >>mtu 1200
```

You can specify any number from 1000 through 1500 as the MTU size. The default MTU size is 1500.

Configuring Local Authentication on an IP Interface

Local authentication can be used when a subscriber logs in to a specific asynchronous port via an IP interface. In order to use local authentication, it must be enabled as the method of inbound authentication for the asynchronous port. Then it must be enabled for the IP interface.

Execute the `authentication enable` command, with the `inbound` and `local` modifiers, to enable local authentication for inbound asynchronous ports. The `authentication enable` command is executed in the Asynchronous Command Mode; for example:

```
Async 4-4:0 >>authentication inbound local enable
```

In the above example, local authentication is enabled as the method of inbound authentication for asynchronous port 4.

Execute the `authentication local enable` command, in the Interface Command Mode, to enable local authentication on the IP interface; for example:

```
Intf 1-1:0 >>authentication local enable
```

Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface

Server-based authentication methods (i.e., RADIUS, TACACS+, or SecurID) can be used when a subscriber logs in to an asynchronous port via an IP interface. In order to enable server-based authentication for an IP interface, the authentication method must be configured for the LX unit and enabled as the method of inbound authentication for the asynchronous port. For more information, refer to "Setting Up RADIUS, SecurID, and TACACS+ for the LX Unit" on page 33 and the `authentication enable` command in the *LX-Series Commands Reference Guide*.

To enable RADIUS authentication on the IP interface, execute the `authentication radius enable` command, in the Interface Command Mode; for example:

```
Intf 1-1:0 >>authentication radius enable
```

To enable SecurID authentication on the IP interface, execute the `authentication securid enable` command, in the Interface Command Mode; for example:

```
Intf 1-1:0 >>authentication securid enable
```

To enable TACACS+ authentication on the IP interface, execute the `authentication tacacs+ enable` command, in the Interface Command Mode; for example:

```
Intf 1-1:0 >>authentication tacacs+ enable
```

Configuring RADIUS Accounting on an Interface

RADIUS Accounting allows you to log user account information to a remote server in a per-client file. The file or record can contain information such as the user who logged in, the duration of the session, port number, Client IP address, and the number of bytes/packets that were processed by the LX unit. For more information on RADIUS accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 161.

RADIUS accounting can be used when a subscriber logs in to an asynchronous port via an IP interface. In order to enable RADIUS accounting for an IP interface, RADIUS accounting must be configured for the LX unit. For more information, refer to "Setting Up RADIUS" on page 33.

Execute the `radius accounting enable` command, in the Interface Command Mode, to enable RADIUS accounting on the IP interface; for example:

```
Intf 1-1:0 >>radius accounting enable
```

Configuring TACACS+ Accounting on an Interface

TACACS+ Accounting allows you to log user account information to a remote server in a per-client file. For more information on TACACS+ accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 161.

Execute the `tacacs+ accounting enable` command, in the Interface Command Mode, to enable TACACS+ accounting on the IP interface; for example:

```
Intf 1-1:0 >>tacacs+ accounting enable
```

Configuring Fallback on an IP Interface

Fallback Authentication can be used as a mechanism for authenticating users when the configured authentication method (i.e., RADIUS, TACACS+, or SecurID) fails because the authentication server is unreachable. When a user logs in via Fallback, his or her username/password combination is validated against the LOCAL security database for the LX unit.

The LX unit will make three attempts to log in the user via RADIUS, TACACS+, or SecurID before it implements Fallback. After the third login attempt, the username/password combination will be validated against the LOCAL security database for the LX unit.

RADIUS, TACACS+, or SecurID must be enabled on an IP interface in order for Fallback to function on the interface. (Refer to "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface" on page 110 for information on enabling RADIUS, TACACS+, or SecurID.) When all three methods (i.e., RADIUS, TACACS+, or SecurID) are disabled on the interface, Fallback is ignored by the interface.

Execute the `authentication fallback enable` command, in the Interface Command Mode, to enable Fallback on the IP interface; for example:

```
Intf 1-1:0 >>authentication fallback enable
```

Configuring Rotaries

The term "rotary" refers to the assignment of an IP address to multiple destinations that offer the same type of service. On an LX unit, an IP interface can be configured as a rotary, with LX asynchronous ports as the multiple destinations of the rotary. A user can attempt to connect to an IP interface that is configured as a rotary. When a user attempts such a connection, he/she is connected to an available port that has been configured as one of the destinations of the rotary.

Figure 7 illustrates a rotary on an LX unit.

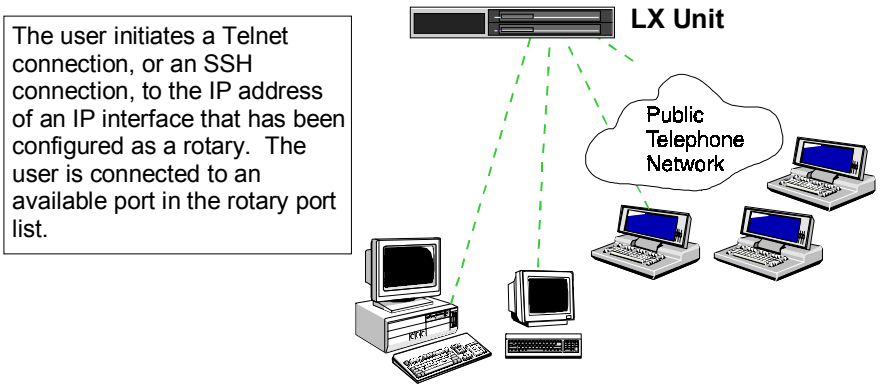

Figure 7 - Rotary Connections on an IP Interface

The rotary is transparent to users. A user simply requests a connection to an IP address, and the LX unit sets up the connection with one of the available ports in the rotary group.

Do the following to configure an IP interface as a rotary:

1. Create a new IP interface, or access an existing one, by executing the `interface` command in the Configuration Command Mode; for example:

   Config:0 >>`interface 1`

   This enters the Interface Command Mode for the specified interface (i.e., Interface `1`). The Interface Command prompt (e.g., `Intf 1-1:0 >>`) is displayed.

2. Use the `address` command to configure a server IP address for the IP interface; for example:

   Intf 1-1:0 >>`address 10.240.10.100`

3. Use the `rotary type` command to specify the rotary type (Round Robin or First Available); for example:

   Intf 1-1:0 >>`rotary type round robin`

   The rotary type is identifies the port search method for the rotary. The allowable values are:

`first available`	An incoming call is connected to the First Available (non-busy) port in the rotary.
`round robin`	The LX unit will search the rotary for an available port, starting with the lowest-numbered port in the rotary.

4. Use the `rotary port` command to configure the IP interface as a rotary, and to assign LX asynchronous ports to the rotary; for example:

   Intf 1-1:0 >>`rotary port 1 2 3`

   In the above example, the LX asynchronous ports `1`, `2`, and `3` are assigned to the rotary.

5. Use the `rotary tcp port` command to assign a TCP socket number to the rotary; for example:

   Intf 1-1:0 >>`rotary tcp port 3000`

   In the above example, the TCP socket number for the rotary is specified as `3000`. This identifies the socket that will be used to make Telnet connections to the rotary.

   NOTE: The default TCP socket is 1500.

6. Use the `rotary ssh port` command to assign an SSH socket number to the rotary; for example:

   Intf 1-1:0 >>`rotary ssh port 3022`

   In the above example, the SSH socket number for the rotary is specified as `3022`. This identifies the socket that will be used to make SSH connections to the rotary.

   NOTE: The default SSH socket is 1522.

7. Use the `rotary enable` command to enable the rotary; for example:

   Intf 1-1:0 >>`rotary enable`

Disabling Rotaries

Execute the `no rotary` command in the Interface Command Mode to disable a rotary; for example:

Intf 1-1:0 >>`no rotary`

When a rotary is disabled, it no longer functions as a rotary.

NOTE: Disabling a rotary does not *delete* the rotary; the configuration of the rotary still exists, and you can re-enable it by executing the `rotary enable` command in the Interface Command Mode.

To verify that a rotary has been disabled, execute the `show interface rotary` command. If the rotary is in fact disabled, it will say "Disabled" in the "Rotary State" column of the display. For more information on the `show interface rotary` command, refer to "Displaying Rotary Information" on page 118.

Removing Ports from a Rotary

To remove asynchronous ports from a rotary, execute the `no rotary port` command in the Interface Command Mode; for example:

Intf 1-1:0 >>`no rotary port`

In the above example, the asynchronous ports are removed from the rotary on Interface 1.

To verify that asynchronous ports have been removed from a rotary, execute the `show interface rotary` command. If the asynchronous ports have in fact been removed, they will not appear in the "Serial Ports" column of the display. For more information on the `show interface rotary` command, refer to "Displaying Rotary Information" on page 118.

Displaying Interface Information

This section describes how to display information about IP interfaces and rotaries. The IP interface information includes characteristics, port mapping, statuses, and summaries. The rotary information includes the Rotary IP Address, the Rotary ports, the Rotary type, and the Rotary State.

Displaying Interface Characteristics

Use the `show interface characteristics` command, in the Superuser Command Mode, to display the characteristics of an IP interface; for example:

```
InReach:0 >>show interface 1 characteristics
```

In the above example, the interface characteristics are displayed for IP interface 1. Use the following syntax to display the interface characteristics of *all* IP interfaces on the LX unit:

```
InReach:0 >>show interface all characteristics
```

Figure 8 shows an example of the Interface Characteristics display.

```
Time:                                          Mon, 22 Dec 1969 16:14:27
Interface Name:          Interface_1  Bound to :                     eth0
IP MTU Size:                    1500
IP Address   :             0.0.0.0  Learned IP Address  :  102.19.169.191
IP Mask      :             0.0.0.0  Learned IP Mask     :   255.255.255.0
IP Broadcast :             0.0.0.0  Learned IP Broadcast:  102.19.169.255
Interface Status:            In Use  Learned IP Gateway  :    102.19.169.1
Rotary Feature:            Disabled  Learned IP DNS      :         0.0.0.0
Authentication:               Local  Radius Accounting:           Disabled
Authentication FallBack:     Disabled  Tacacs+ Accounting:           Disabled
SSH    port:                     22  Telnet port:                      23
SSH Keepalive Interval:           0  SSH Keepalive Count:               3
```

Figure 8 - Interface Characteristics Display

Displaying Interface Port Mapping

Use the `show interface characteristics` command, in the Superuser Command Mode, to display the Telnet Socket Number, and the SSH Socket Number, associated with each serial port on the LX unit; for example:

InReach:0 >>`show interface 1 port mapping`

In the above example, the port mapping for IP interface 1 is displayed. Use the following syntax to display the port mapping for *all* IP interfaces on the LX unit:

InReach:0 >>`show interface all port mapping`

Figure 9 shows an example of the Interface Port Mapping display.

```
Serial Port    Telnet Port   SSH Port
      0              0            0
      1           2100         2122
      2           2200         2222
      3           2300         2322
      4           2400         2422
      5           2500         2522
      6           2600         2622
      7           2700         2722
      8           2800         2822
```

Figure 9 - Interface Port Mapping Display

Displaying Interface Statuses

Use the `show interface characteristics` command, in the Superuser Command Mode, to display the status information for IP interfaces; for example:

InReach:0 >>`show interface 1 status`

In the above example, the status information for IP interface 1 is displayed. Use the following syntax to display the status information for *all* IP interfaces on the LX unit:

InReach:0 >>`show interface all status`

Figure 10 shows an example of the Interface Status display.

```
Time:                                        Mon, 22 Dec 1969 16:19:34
Interface Name:          Interface_1     Bound to :                eth0
IP Address:           102.19.169.191     IP Mask:          255.255.255.0
IP Broadcast Addr:     102.19.169.255
```

Figure 10 - Interface Status Display

Displaying Interface Summaries

Use the `show interface summary` command, in the Superuser Command Mode, to display summary information for all of the IP interfaces on the LX unit; for example:

InReach:0 >>`show interface summary`

Figure 11 shows an example of the Interface Summary display.

```
       Name          Address        Broadcast       Addr. Mask    Bound to
 Interface_1          0.0.0.0          0.0.0.0          0.0.0.0        eth0
 Interface_2          0.0.0.0          0.0.0.0          0.0.0.0     eth0:1
```

Figure 11 - Interface Summary Display

Displaying Rotary Information

Use the `show interface rotary` command, in the Superuser Command Mode, to display information on rotaries; for example:

InReach:0 >>`show interface 1 rotary`

In the above example, the rotary information for IP interface 1 is displayed. Use the following syntax to display the rotary information for *all* IP interfaces on the LX unit:

InReach:0 >>`show interface all rotary`

Figure 12 shows an example of the Rotary display.

```
Rotary Ip Address      TCP/SSH Port    Rotary Type      Rotary State     Serial Ports
  147.132.145.16        1500/1522      First Available    Disabled         2,3,4,7
```

Figure 12 - Rotary Display

Chapter 7

Configuring Subscriber Accounts for the LX Unit

In order for a user (subscriber) to use the LX unit, he/she must log in to the unit under a **subscriber account**. The subscriber account defines a **User Profile** that includes the subscriber's username and password. The User Profile also defines the subscriber's Security Level (User or Superuser) and contains all of the settings that affect the subscriber's use of the LX unit.

This chapter describes how to create and delete subscriber accounts, how to modify subscriber accounts, and how to display information on subscriber accounts.

The *LX-Series Commands Reference Guide* provides a detailed syntax, and description, for each command mentioned in this chapter.

Creating Subscriber Accounts and Entering Subscriber Command Mode

To create a subscriber account, or to access an existing subscriber account, use the `subscriber` command in the Configuration Command Mode; for example:

Config:0 >>`subscriber jack`

where `jack` is an example of a subscriber name (user name).

The subscriber name must contain at least 2 characters, and no more than 15 characters. The reserved words `super` and `subscriber`, and any variation of `super` and `subscriber`, cannot be used as subscriber names. (Variations of `super` and `subscriber` include `su`, `sup`, `sub`, `subs`, etc.)

The maximum number of subscribers on an LX unit is equal to double the number of ports on the unit. For example, the maximum number of subscribers is 16 on an 8-port unit, 32 on a 16-port unit, 64 on a 32-port unit, and 96 on a 48-port unit.

Executing the `subscriber` command puts you into the Subscriber Command Mode for the subscriber. The Subscriber Command prompt (e.g., **Subs_jack >>**) is displayed.

Creating Subscriber Accounts by Copying

You can also create subscriber accounts by executing the `copy subscriber` command in the Configuration Command Mode. The `copy subscriber` command creates new subscriber accounts by copying the configuration of an existing subscriber account; for example:

Config:0 >>`copy subscriber benw to jimk billj edw`

In the above example, the subscriber account configuration of `benw` is copied to `jimk`, `billj`, and `edw`.

Deleting Subscriber Accounts

Use the `no subscriber` command, in the Configuration Command Mode, to delete a subscriber account; for example:

Config:0 >>`no subscriber jack`

In the above example, the subscriber account `jack` is deleted.

NOTE: You can not delete the subscriber `InReach`.

The User Profile

When you create a new subscriber account with the `subscriber` command, its User Profile is based on the default User Profile of the `InReach` subscriber. (The `InReach` subscriber is the default subscriber for the LX unit.)

Refer to the following sections to specify new settings in a User Profile:

- "Specifying the Subscriber Access Methods" on page 123
- "Setting Up the Session and Terminal Parameters" on page 128
- "Configuring the Subscriber Password" on page 132
- "Specifying a Preferred Service" on page 133
- "Specifying a Dedicated Service" on page 133
- "Enabling Login Menus" on page 134
- "Adding Superuser Privileges to a Subscriber Account" on page 133
- "Configuring the Subscriber Password" on page 132
- "Enabling Audit Logging" on page 134
- "Enabling Command Logging" on page 134

Specifying the Subscriber Access Methods

You can specify up to four methods for the subscriber to access the LX unit. The methods include Telnet, SSH, Web Browser, and Console. For information on specifying each method, refer to the following:

- "Telnet Access" (see below)
- "SSH Access" (see page 124)
- "Web Browser Access" (see page 126)
- "Console Access" (see page 127)

You can also provide subscribers with access via Dialback. For more information, refer to "Dialback Access" on page 127.

Telnet Access

In order to specify Telnet access for a subscriber, do the following:

1. Set the `telnet access` parameter to `enabled`; for example:

   ```
   Subs_jack >>access telnet enable
   ```

2. Set the `telnet mode` parameter to `line` or `character`; for example:

   ```
   Subs_jack >>telnet mode line
   Subs_jack >>telnet mode character
   ```

After you have executed the above commands, the subscriber will have Telnet access to virtual ports on the LX unit. Refer to "Console Access" on page 127 to give the user access to asynchronous ports on the LX unit.

SSH Access

In order to specify SSH access for a subscriber, do the following:

1. Set the `ssh access` parameter to `enabled`; for example:

   ```
   Subs_jack >>access ssh enable
   ```

2. Set the `ssh log level` parameter to the class of SSH messages that will be logged to syslogd; for example:

   ```
   Subs_jack >>ssh log level debug
   ```

   The above example of the `ssh log level` command specifies that SSH messages of the debug class will be logged to syslogd for the subscriber. You can also specify SSH log levels of error, fatal, info, quiet, verbose.

3. Set the `ssh cipher` parameter to `triple-des`, `any`, or `blowfish`; for example:

   ```
   Subs_jack >>ssh cipher triple-des
   Subs_jack >>ssh cipher any
   Subs_jack >>ssh cipher blowfish
   ```

Description of the Three Encryption Types

`triple-des`	Specifies that the Triple Data Encryption Standard (Triple-DES) is the only SSH encryption type supported for this subscriber.
`any`	Specifies that any SSH encryption type is supported for this subscriber.
`blowfish`	Specifies that BLOWFISH is the only SSH encryption type supported for this subscriber. See "Usage Guidelines" (below) for more information on the BLOWFISH encryption type.

After you have executed the above commands, the subscriber will have SSH access to virtual ports on the LX unit. Refer to "Console Access" on page 127 to give the subscriber access to asynchronous ports on the LX unit. You can specify a unique SSH key for the subscriber. Refer to "Specifying a Unique SSH Key for the Subscriber" on page 126 for more information.

Overview of Triple-DES

DES is a block cipher (i.e., it acts on a fixed-length block of plaintext and converts it into a block of ciphertext of the same size by using the secret key). In DES, the block size for plaintext is 64 bits. The length of the key is also 64 bits but 8 bits are used for parity. Hence the effective key length is only 56 bits.

In Triple-DES, we apply 3 stages of DES with a separate key for each stage. The key length in Triple-DES is 168 bits.

Decryption is done by applying the reverse transformation to the block of ciphertext using the same key. Since the same key is used both in encryption and decryption, DES is a symmetric key cipher. This method differs from algorithms like the RSA encryption which use different keys to encrypt and decrypt a message.

Overview of Blowfish

Blowfish is a variable-length key block cipher. It is only suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than DES when implemented on 32-bit microprocessors with large data caches, such as the Pentium and the PowerPC. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use.

Specifying a Unique SSH Key for the Subscriber

You can specify a unique SSH key for the subscriber by executing the `ssh key` command; for example:

```
Subs_jack >>ssh key
```

When you execute the `ssh key` command, the following prompt is displayed:

```
Please enter your key:
```

Type an SSH key at the above prompt. The SSH key can be any random string of characters.

As an alternative to typing the SSH key, you can paste a generated SSH key at the above prompt. (The SSH key must be generated on the host from which the subscriber will make SSH connections to the LX unit. Refer to your Linux documentation for more information on generating an SSH key.)

When a subscriber has a unique SSH key, he/she can log on to the LX unit, via SSH, without entering a password. (The only requirement is that the user must log on from the host on which his or her SSH key was generated.)

Web Browser Access

In order to specify Web Browser access for the subscriber, set the `access web` parameter to `enabled`; for example:

```
Subs_jack >>access web enable
```

In order for the subscriber to have access to virtual ports on the LX, you must configure Telnet or SSH for the subscriber. For more information, refer to "Telnet Access" on page 124 and "SSH Access" on page 124.

Refer to "Console Access" on page 127 to give the user access to asynchronous ports on the LX.

Console Access

By default, a user can only access virtual ports on the LX when his or her subscriber account has been configured for Telnet, SSH, or Web Browser access. In order for a subscriber to access asynchronous ports, the access to those ports must be configured in the subscriber account.

To configure a subscriber account for access to asynchronous ports, do the following:

1. Execute the `access console enable` command to enable asynchronous port access for the subscriber; for example:

   ```
   Subs_jack >>access console enable
   ```

2. Execute the `access port enable` command to specify the asynchronous ports that the subscriber can access; for example:

   ```
   Subs_jack >>access port 2 4 6 enable
   ```

   In the above example, the subscriber is given access to asynchronous ports 2, 4, and 6.

Dialback Access

The LX unit supports Dialback as an access method for LX subscribers. Under Dialback, the subscriber dials in to the LX unit and logs in as he/she would if he/she were a dialin subscriber. The LX unit then validates the login and terminates the call. If the subscriber login is valid, the LX unit calls the subscriber back. The subscriber is then logged in to the LX unit.

Dialback is used for security (the destination is recorded by the Telco for billing, and calls can be restricted to specific destinations) and to manage connection costs (central site billing).

In order to specify Dialback access for a subscriber, do the following:

1. Set the `dialback access` parameter to `enabled`; for example:

   Subs_jack >>`dialback enable`

2. Specify a `dialback number` for the subscriber; for example:

   Subs_jack >>`dialback number 19785551978`

   The `dialback number` is the telephone number that the LX modem will dial to call back the subscriber.

3. Specify the `dialback retry` parameter for the subscriber; for example:

   Subs_jack >>`dialback retry 7`

   The `dialback retry` parameter is the number of times that the modem on the LX unit can attempt to answer a dialback call

Setting Up the Session and Terminal Parameters

The session and terminal parameters include all settings that affect the subscriber session and the operation of the subscriber terminal during a subscriber session. These settings include the session timeouts and limits, screen pause, user prompts, terminal type, Subscriber session mode, and function keys for switching between sessions.

For more information, refer to the following:

- **Function Keys for Switching Between Sessions** – Used to switch between subscriber sessions, including the Local Command Mode (see "Setting Up the Session Switch Characters" on page 131).
- **Terminal Type** – Use the `terminal` command to set the terminal type for the subscriber. You can set the terminal type to ANSI or VT100; for example:

  Subs_jack >>`terminal ansi`
  Subs_jack >>`terminal vt100`

- **Maximum Length of a Subscriber Session** – Use the `session timeout` command to set the maximum length (in seconds) of a subscriber session. The syntax of the `session timeout` command is as follows:

  Subs_jack >>`session timeout 36000`

  The allowable values are 0 through 65535. A value of 0 means that there is no limit to the length of a subscriber session.

- **User Prompts** – You can specify a custom user prompt of up to 8 ASCII characters to replace the *username* field of the default login prompt for a subscriber. To specify a custom user prompt, execute the `prompt` command; for example:

  Subs_jack >>`prompt mxxxx9`

  In the above example, the subscriber's default login prompt (e.g., `jack:0 >`) is changed to `mxxxx9:0 >`.

- **Subscriber Session Mode** – When the Subscriber session mode is `CLI`, the subscriber is logged into the CLI when he/she accesses the LX unit; when the Subscriber session mode is `Shell`, the subscriber is logged into the Linux shell when he/she accesses the LX unit. Use the `shell enable` command to change the Subscriber session mode from `CLI` to `Shell`; for example:

  Subs_jack >>`shell enable`

  When the `shell enable` command is executed, the Maximum Subscriber Sessions is automatically set to 1. The Maximum Subscriber Sessions cannot be changed from 1 until the Subscriber Session Mode is disabled with the `no shell` command (see below).

  When the Subscriber session mode is `Shell`, the subscriber can only access the Linux shell and the GUI; the subscriber cannot access the CLI.

  Use the `no shell` command to change the Subscriber session mode from `Shell` to `CLI`; for example:

  Subs_jack >>`no shell`

When the `no shell` command is executed, the Maximum Subscriber Sessions is automatically set to 4.

- **Screen Pause** – When this feature is enabled, the screen will pause after displaying the number of lines specified in the "lines/screen" value for the terminal. To enable this feature for a subscriber, use the `pause enable` command; for example:

  Subs_jack >>`pause enable`

- **Inactivity Timeout** – The Inactivity Timeout is the length of time (in seconds) that the subscriber has to enter keyboard data. If the subscriber does not enter keyboard data before the expiration of the Inactivity Timeout, he/she is logged out. You can use the `idletime` command to set the Inactivity Timeout to any value from 0 through 65535; for example:

  Subs_jack >>`idletime 1200`

  A value of 0 means that the Inactivity Timer is effectively disabled.

- **Maximum Simultaneous Connections** – You can configure 1 through 255 simultaneous connections for a subscriber. Use the `maxsubscriber` command to set the maximum simultaneous connections for the subscriber; for example:

  Subs_jack >>`maxsubscriber 10`

- **Maximum Subscriber Sessions** – Use the `session` command to specify the maximum number of sessions for a subscriber. The allowable values are 0 through 4, where a value of 0 disables the subscriber's access to the LX unit; for example:

  Subs_jack >>`session 3`

Setting Up the Session Switch Characters

The LX unit supports up to 4 sessions per subscriber. (Refer to "Setting Up the Session and Terminal Parameters" on page 128 to configure the number of sessions for a subscriber.) You can configure Control characters as function keys for switching to the previous, or next, session. You can also configure a Control character as a function key for switching to the Local Command Mode.)

To configure Session Switch characters for a subscriber, use the following commands:

- `backward_switch` – to specify the Function Key for switching (backwards) to the previous session; for example:

  Subs_jack >>`backward_switch ^I`

- `forward_switch` – to specify the Forward Switch (i.e., Control-character sequence for switching to the next session); for example:

  Subs_jack >>`forward_switch ^J`

- `local_switch` – to specify the Local Switch (i.e., Control-character sequence for switching to the Local Command Mode); for example:

  Subs_jack >>`local_switch ^K`

The Session Switch character can be specified as an uppercase alphabetical character with, or without, a caret (^) before it. When the Session Switch character is preceded by a caret, the LX command parser interprets it as a Control-character sequence. For example, `^I` is interpreted as `CTRL/I`; `^J` as `CTRL/J`; and `^M` as `CTRL/M`.

Be sure that there are no conflicting uses for the character you select (particularly with control characters that are used by applications programs, or with the character you set for the FORWARD SWITCH, the LOCAL SWITCH, or any Telnet command characters). If you specify a CTRL character, when the user types the character, it will be displayed as ^<Key> (e.g., if the user types CTRL/I, the terminal will echo the characters: ^I).

Configuring the Subscriber Password

The default password for an LX subscriber account is `access`. It is recommended that you, or the subscriber, change the password from this default *before* the subscriber uses it to log in to the LX unit. This prevents unauthorized users (who might know the default password) from logging on to the LX unit.

Changing the Subscriber Password

To change the subscriber password, execute the `password` command; for example:

```
Subs_jack >>password
```

When the `password` command is executed, the following prompts are displayed:

```
Enter your NEW password   :
Re-enter your NEW password:
```

Enter the new password at the `Enter` prompt, and re-enter it at the `Re-enter` prompt. The password string can be up to 16 characters in length, and it will be masked when you enter it at the above prompts.

Enabling the Subscriber to Change His or Her Own Password

To enable the subscriber to change his or her own password, execute the `password enable` command; for example:

```
Subs_jack >>password enable
```

The subscriber will be prompted to enter, and verify, his or her new password the next time he/she logs in to the LX unit.

Adding Superuser Privileges to a Subscriber Account

By default, a subscriber password has **user** privileges on the LX unit. A subscriber with **user** privileges can only access the User Command Mode, or his or her assigned Login menu, when he/she logs in to the LX unit.

You can add Superuser privileges to a subscriber account. With Superuser privileges, the subscriber can use the `enable` command in the User Command Mode to enter the Superuser Command Mode.

Use the `security level superuser` command to add Superuser privileges to the subscriber account; for example:

```
Subs_jack >>security level superuser
```

Specifying a Dedicated Service

If a dedicated service is specified for a subscriber, the subscriber will begin running the dedicated service whenever he/she logs in to the LX unit. Telnet must be enabled for the subscriber in order for him to run a dedicated service. Refer to “Specifying the Subscriber Access Methods” on page 123 to enable Telnet for a subscriber.

Use the `dedicated service` command to specify a dedicated service for the subscriber; for example:

```
Subs_jack >>dedicated service 192.173.56.10
```

Specifying a Preferred Service

Use the `preferred service` command to assign a service to which the subscriber will be connected whenever he/she makes a connect request without specifying a service; for example:

```
Subs_jack >>preferred service 178.87.42.19
```

Telnet must be enabled for the subscriber in order for him to run a preferred service. Refer to “Specifying the Subscriber Access Methods” on page 123 to enable Telnet for a subscriber.

Enabling Audit Logging

An audit log records all of the port activity for a subscriber. This includes the commands that the subscriber enters as well as the data that is output on the port for the subscriber. To enable audit logging for a subscriber, execute the `audit log enable` command; for example:

```
Subs_jack >>audit log enable
```

To display the contents of the audit log, execute the `show audit log` command in the Superuser Command Mode. For more information, refer to "Displaying the Audit Log for a Subscriber" on page 138.

Enabling Login Menus

A Subscriber Menu is a menu that displays for a subscriber when he/she logs in to the LX unit. In order for a menu to display for a subscriber, you must enable the Login Menu feature and specify a menu for the subscriber.

Use the `menu enable` command to enable the Login Menu feature and to specify a menu that will be displayed for a subscriber when he/she logs in to the LX unit; for example:

```
Subs_jack >>menu financegroup enable
```

In the above example, the subscriber `jack` is enabled for the Login Menu feature, and the menu `financegroup` is specified for him. The `financegroup` menu will be displayed for the subscriber `jack` when he/she logs on to the LX unit.

Enabling Command Logging

Command logging creates an audit trail of subscriber input in a subscriber session. The audit trail is sent to the accounting log and to syslogd. To enable command logging for a subscriber, execute the `command log enable` command; for example:

```
Subs_jack >>command log enable
```

To display the contents of the command log, execute the `show command log` command in the Superuser Command Mode. For more information, refer to "Displaying the Command Log for a Subscriber" on page 139.

Displaying Subscriber Information

This section describes how to display subscriber characteristics, subscriber status and TCP information, subscriber summaries, and the audit log and command log for a subscriber.

Displaying Subscriber Characteristics

Use the `show subscriber characteristics` command, in the Superuser Command Mode, to display subscriber characteristics; for example:

```
demo:0 >>show subscriber tim characteristics
```

In the above example, the `show subscriber characteristics` command is used to display the characteristics for the subscriber `tim`. Use the following syntax to display the characteristics for all of the subscribers on the LX unit:

```
demo:0 >>show subscriber all characteristics
```

Figure 13 shows an example of the Subscriber Characteristics display.

```
Subscriber Name:             tim
Security:                  Super  User Prompt:                      Demo
Preferred Service:                Dedicated Service:
Command Logging:         Disabled  User Password:               Disabled
Maximum Connections:           50  Maximum Sessions:                  4
Session Mode:              Normal  Screen Pause:                 Enabled
Debug Feature:           Disabled  Debug File:                /tmp/D_demo
Idle Timeout:                 0    Session Timeout:                   0
Menu Feature:            Disabled  Menu Name:              /config/M_demo
Forward Switch:                ^F  Local Switch:                     ^L
Backward Switch:               ^B  Dialback Feature:            Disabled
Dialback Retry:                 4  Dialback Number:
Dialback Timeout:              45  Audit Feature:                Disabled
Port Access list:                                                   1-8
Remote Access list:                                 Telnet Ssh Web_Server
```

Figure 13 - Subscriber Characteristics Display

Refer to the `show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Characteristics display.

Displaying the Subscriber Status

Use the `show subscriber status` command, in the Superuser Command Mode, to display the status information for a subscriber; for example:

```
demo:0 >>show subscriber tim status
```

In the above command, the `show subscriber status` command is used to display the status information for the subscriber `tim`. Use the following syntax to display the status information for all of the subscribers on the LX unit:

```
demo:0 >>show subscriber all status
```

Figure 14 shows an example of the Subscriber Status display.

```
Time:                                        Fri, 03 Jan 2003 17:44:21
Subs. Name:                    tim  Number of Connections:              0
Configured TermType:          Ansi  Session Mode:                   Normal
```

Figure 14 - Subscriber Status Display

Refer to the `show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Status display.

Displaying the Subscriber TCP Information

Use the `show subscriber tcp` command, in the Superuser Command Mode, to display the subscriber TCP information; for example:

```
demo:0 >>show subscriber tim tcp
```

In the above command, the `show subscriber tcp` command is used to display the TCP information for the subscriber `tim`. Use the following syntax to display the TCP information for all of the subscribers on the LX unit:

```
demo:0 >>show subscriber all tcp
```

Figure 15 shows an example of the Subscriber TCP display.

```
Time:                                        Fri, 03 Jan 2003 17:46:32
Subscriber Name:              mark  Telnet Line Mode:      Character Mode
SSH Name:                     mark  SSH Encryption:                  Any
SSH Port:                       22  SSH Log Level:                INFO
```

Figure 15 - Subscriber TCP Display

Refer to the `show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber TCP display.

Displaying the Subscriber Summary Information

Use the `show subscriber summary` command, in the Superuser Command Mode, to display a Subscriber Summary; for example:

```
demo:0 >>show subscriber summary
```

Figure 16 shows an example of the Subscriber Summary display.

```
                Name   Connections   Terminal Type
            In-Reach        0             Ansi
                demo        1             Ansi
                jack        0             Ansi
```

Figure 16 - Subscriber Summary Display

Refer to the `show subscriber summary` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Summary display.

Displaying the Audit Log for a Subscriber

An audit log records all of the port activity for a subscriber. This includes the commands that the subscriber enters as well as the data that is output on the port for the subscriber.

Use the `show audit log` command, in the Superuser Command Mode, to display the audit log for a subscriber; for example:

```
demo:0 >>show audit log tim
```

In the above command, the `show audit log` command is used to display the audit log for the subscriber `tim`.

Figure 17 shows an example of the Audit Log.

```
Nov 18 16:08:32 tim ttyGN0 0 Subs_tim >>end
Nov 18 16:08:50 tim ttyGN0 1 tim:0 >>
Nov 18 16:08:50 tim ttyGN0 2 tim:1 >
Nov 18 16:08:50 tim ttyGN0 3 tim:2 >
Nov 18 16:08:55 tim ttyGN0 3 tim:3 >sho session
Nov 18 16:08:55 tim ttyGN0 3 Number    Device       Program       Pid       Time      Status
Nov 18 16:08:55 tim ttyGN0 3   0     /dev/pts/0    Superuser      477        98          -
Nov 18 16:08:55 tim ttyGN0 3   1     /dev/pts/3    User           481         5          -
Nov 18 16:08:55 tim ttyGN0 3   2     /dev/pts/4    User           482         5          -
Nov 18 16:08:55 tim ttyGN0 3   3     /dev/pts/5    User           483         5          *
```

Figure 17 - Audit Log Display

Displaying the Command Log for a Subscriber

A command log is an audit trail of subscriber input in a subscriber session. Use the `show command log` command, in the Superuser Command Mode, to display the command log for a subscriber; for example:

demo:0 >>`show command log tim`

In the above command, the `show command log` command is used to display the command log for the subscriber `tim`.

Figure 18 shows an example of the Command Log.

```
Nov 11 12:47:30 tim 0 end
Nov 11 12:47:33 tim 0 sho command log
Nov 11 12:49:21 tim 23 modem
Nov 11 12:49:29 tim 23 end
Nov 11 12:49:39 tim 23 show command log tim
```

Figure 18 - Command Log Display

Chapter 8

Configuring Ports for Temperature/Humidity Sensors

You can configure ports to act as temperature and humidity monitors when connected to an In-Reach Temperature/Humidity Sensor. The Temperature/Humidity Sensor provides an accurate measurement of the temperature and humidity in the area in which your LX Series unit is placed.

Refer to *Getting Started with the LX Series* to connect a Temperature/Humidity Sensor to an LX port.

Configuring Sensor Access for an LX Port

You must configure an LX port's access as `sensor` before you can perform any temperature/humidity monitoring on the port. Use the `access` command, in the Asynchronous Command Mode, to do this; for example:

```
Async 4-4:0>>access sensor
```

NOTE: The DIAG port (port 0) cannot be configured as a Sensor port.

Displaying the Temperature and Humidity

Use the `show device status` command, in the Superuser Command Mode, to display the current temperature and humidity readings on a Sensor port; for example:

```
InReach:0 >>show device 4 status
```

In the above example, the temperature and humidity readings of the Sensor attached to port 4 are displayed. Use the following syntax to display the temperature and humidity readings for *all* Temperature/Humidity Sensors on the LX unit:

```
InReach:0 >>show device all status
```

Figure 19 shows an example of the Device Status display for a Sensor port.

```
Time: 29 Aug 2002 17:35:17 US/EASTERN  Device Number:              4
Device Type:                                                  Sensor
Humidity Level(%):                                             39.00
Temperature (Celsius):                                         26.00
Temperature (Fahrenheit):                                      78.80
```

Figure 19 - Device Status Display for a Sensor Port

Displaying Sensor Summaries

Use the `show device summary` command, in the Superuser Command Mode, to display summary information for all of the Temperature/Humidity Sensors that are currently connected to the LX unit; for example:

InReach:0 >>`show device summary`

Figure 20 shows an example of the Device Summary display.

Device Number	Device Type	Model Name
1	Sensor	N/A

Figure 20 - Device Summary Display for Sensors

NOTE: If any of the ports on the LX unit are configured as Power outlets, the Device Summary Display will display information for the attached Power Management Device (IR-5100 or IR-5150).

Chapter 9

Configuring Power Control Units

The In-Reach Power Control Units (IR-5100 and IR-5150) can be managed remotely from asynchronous ports on an LX unit. The management tasks that can be performed remotely include rebooting Power Control Relays and turning Power Control Relays on and off. (For information on performing these tasks, refer to the `outlet` command, and the `outlet group` command in the "Superuser Commands" chapter of the *LX-Series Commands Reference Guide*.)

NOTE: You can access the on-board CLI of an IR-5150 unit that is connected to a console port. To do this, Telnet to its LX console port, and log on to the IR-5150 unit.

Power Control units are remotely managed from LX asynchronous ports that are configured as **Power Masters**. This chapter describes how to configure ports as Power Masters, how to configure Power Control units via Power Masters, and how to display information on Power Control units.

Configuring an LX Asynchronous Port as a Power Master

Use the `access power model` command, in the Asynchronous Command Mode, to configure an LX asynchronous port as a Power Master; for example:

```
Async 5-5:0>>access power model ir5100
```

In the above example, port 5 is configured as a Power Master for an IR-5100 unit. Use the following syntax to configure an asynchronous port as a Power Master for an IR-5150 unit:

```
Async 5-5:0>>access power model ir5150
```

When a port has been configured as a Power Master, you can connect a Power Control unit to it. The connection to the Power Master port is made using the RJ-45 crossover cable that is supplied with the Power Control unit.

You must power on the Power Control unit before you can configure it from the LX unit. For more information, refer to the *Getting Started* guide for the Power Control unit.

Default Name for a Power Control Relay

The default name for a Power Control Relay is derived from its Alarm Master and the number of the relay on the Power Control unit. For example, `5:7` is the default name of the 7th Power Control Relay on the Power Control Unit that is managed from Alarm Master port 5.

You can specify a descriptive name for a Power Control Relay or a Power Control Relay group. A descriptive name is a unique text name of up to 15 alphanumeric characters. For more information, refer to "Naming a Power Control Relay" on page 146 and "Naming a Group of Power Control Relays" on page 147.

You must specify the default name, or the descriptive name, of a Power Control Relay, in the `outlet group` command in the Configuration Command Mode.

However, you only need to specify the number, or descriptive name, of the Power Control Relay in the `outlet name` command in the Asynchronous Command Mode. This is because the LX software "knows" that the Alarm Master is the current asynchronous port.

Refer to the *LX-Series Commands Reference Guide* for more information on the `outlet group` command and the `outlet name` command.

Configuring Power Control Units

Power Control Relays can be assigned to a group and managed and configured as a group. The Off Time for Power Control Relays can be specified using the LX CLI. This section describes how to assign Power Control Relays to a group and how to specify the Off Time for Power Control Relays.

Assigning Power Control Relays to a Group

When Power Control Relays are assigned to a group, they can be configured and managed as a group. This can be more efficient than configuring and managing Power Control Relays individually.

Use the `outlet group` command to assign Power Control Relays to a group; for example:

```
Config:0 >>outlet group 2 2:5 3:7 4:2 4:3 4:5
```

In the above example, the Power Control Relays `2:5 3:7 4:2 4:3 4:5` are assigned to Group `2`.

Specifying the Off Time

The Off Time is the length of time, in seconds, that Power Control Relays must remain off before they can be turned back on. This section describes how to specify the Off Time for a Power Control unit or for a group of Power Control Relays.

Specifying the Off Time for a Group of Power Control Relays

Use the `outlet group off time` command, in the Configuration Command Mode, to specify the Off Time for a group of Power Control Relays; for example:

```
Config:0 >>outlet group 14 off time 20
```

In the above example, the Off Time for Outlet Group 14 is set to 20 seconds.

Specifying the Off Time for a Power Control Unit

Use the `power off time` command, in the Asynchronous Command Mode, to specify the Off Time for all of the Power Control Relays that are managed from an Alarm Master port; for example:

```
Async 5-5:0>>power off time 15
```

In the above example, an Off Time of 15 seconds is specified for all of the Power Control Relays that are managed from asynchronous port 5.

NOTE: The `power off time` command can only be executed on a port that is configured as a Master Alarm port and has a Power Control unit attached to it.

Naming a Power Control Relay

You can assign a descriptive name of up to 15 alphanumeric characters to a Power Control Relay.

Use the `outlet name` command, in the Asynchronous Command Mode, to specify a descriptive name for a Power Control Relay; for example:

```
Async 5-5:0>>outlet 2 name Build5NTserver
```

In the above example, the descriptive name `Build5NTserver` is assigned to Power Control Relay `2` on the Power Control unit that is managed from Alarm Master port 5.

NOTE: The Alarm Master number is not specified in the `outlet name` command (e.g., `5:2`) because the Alarm Master port is *implied* to be the current port in the Asynchronous Command Mode. In the above example, the implied Alarm Master is port 5. (The CLI is in the Asynchronous Command Mode for port 5.)

Naming a Group of Power Control Relays

You can assign a descriptive name of up to 15 alphanumeric characters to a group of Power Control Relays.

Use the `outlet group name` command, in the Configuration Command Mode, to specify a descriptive name for a group of Power Control Relays; for example:

```
Config:0 >>outlet group 14 TestEquipment
```

In the above example, the descriptive name `TestEquipment` is assigned to Power Control Relay Group `14`.

Displaying Information on Power Control Units

This section describes how to display information on Power Control units and Power Control Relays. The information that can be displayed includes statuses and summaries for Power Control units, and statuses for groups of Power Control Relays.

Displaying Status Information for Power Control Units

Use the `show device status` command, in the Superuser Command Mode, to display status information for a particular Power Control unit; for example:

```
InReach:0 >>show device 4 status
```

In the above example, the status for the Power Control unit on port 4 is displayed. Use the following syntax to display the status for *all* of the Power Control units that are managed from the LX unit:

```
InReach:0 >>show device all status
```

NOTE: The `show device status` command displays the status of all Power Control units and Temperature/Humidity sensors that are connected to the LX unit. Refer to Figure 19 on page 142 for the status display for a Temperature/Humidity Sensor port.

Figure 21 shows an example of the Device Status display for an Alarm Master port.

```
Time:      Tue, 17 Sep 2002 20:05:47   Device Number:                    4
Device Type:                                                        IR5100
Model Name:                                                      IR-5100-126
Total Outlet Strip Load:                                               0.0
Outlet Minimum Off Time:                                                15
Outlet          Name       State            Load        Assigned Groups
   1            plug1        Off             0.0                   1 4 13
   2            plug2        Off             0.0                   1 6 10
   3            plug3        Off             0.0                      1 7
   4            plug4        Off             0.0                        1
   5            plug5        Off             0.0                      2 4
   6            plug6        Off             0.0                        2
   7            plug7        Off             0.0                        2
   8            plug8        Off             0.0                        2
   9            plug9        Off             0.0                      3 4
  10           plug10        Off             0.0                        3
  11           plug11        Off             0.0                        3
  12           plug12        Off             0.0                        3
  13           plug13        Off             0.0                      4 5
  14           plug14        Off             0.0                      4 5
  15           plug15        Off             0.0                      4 5
  16           plug16        Off             0.0                        5
```

Figure 21 - Device Status Display for an Alarm Master Port

Displaying Status Information for Groups of Power Control Relays

Use the `show device status` command, in the Superuser Command Mode, to display status information for groups of Power Control Relays; for example:

InReach:0 >>`show outlet group TestEquipment status`

In the above example, the status for the group `TestEquipment` is displayed. Use the following syntax to display the status for *all* groups of Power Control Relays that are managed from the LX unit:

InReach:0 >>`show outlet group all status`

Figure 22 shows an example of the Device Status display for a Power Control Relay Group.

```
Time:      Mon, 16 Sep 2002 17:55:19   Group Number:                    2
Group Name:           TestEquipment   Group Off Time:                  4
Port  Outlet    State
  2      1       Not configured
  2      2       Not configured
```

Figure 22 - Device Status Display for a Power Control Relay Group

Displaying Summary Information for Power Control Units

Use the `show device summary` command, in the Superuser Command Mode, to display summary information for all of the Power Control units that are currently connected to the LX unit; for example:

InReach:0 >>`show device summary`

Figure 23 shows an example of the Device Summary display.

```
    Device Number   Device Type       Model Name

             4         IR5100         IR-5100-126
             5         IR5100         IR-5100-255
```

Figure 23 - Device Summary Display

NOTE: The `show device summary` command displays summary information for all Power Control units and Temperature/Humidity sensors that are connected to the LX unit. Refer to Figure 20 on page 142 for the Summary Display for a Temperature/Humidity Sensor port.

Chapter 10

Configuring Packet Filters with the `iptables` Command

Packet Filters are used to allow certain IP packets to pass, or not pass, through an LX unit. Packet Filters can be applied to IP packets that originate from the LAN side of the LX, or from the LX unit itself.

On the LX unit (as on all Linux-based systems), Packet Filters are known as chains. The INPUT chain filters packets coming from the LAN to the LX; the OUTPUT chain filters packets from the LX destined for the LAN.

NOTE: The LX unit also supports the FORWARD chain, which filters packets that are to be forwarded to another network. The FORWARD chain is used primarily in routing environments rather than in console management environments. For this reason, the FORWARD chain is not covered in this chapter.

A chain consists of a series of rules that specify the criteria for accepting, denying, or dropping a packet. The criteria for accepting, denying, or dropping a packet can include the source IP Address, the destination IP Address, and other characteristics.

Adding a Rule to a Chain

Use the `iptables` command to add a rule to a chain. The `iptables` command is executed in Linux shell. To access the Linux shell, execute the `shell` command in the Superuser Command Mode; for example:

```
InReach:0 >>shell
```

When you are in the Linux shell, you can display the chains for the LX unit by executing the `iptables` command with the `-L` option; for example:

```
In-Reach:/# iptables -L
```

The following sections provide examples of how to create rules using various options of the `iptables` command.

For detailed information on the `iptables` command, refer to Appendix D ("Details of the iptables Command") on page 151.

Example: Dropping Packets Based on the Source IP Address

The following `iptables` command creates a rule that will drop any packets coming to the LX from source address 10.240.10.240:

```
In-Reach:/# iptables -A INPUT -s 10.240.10.240 -j DROP
```

The options in the above command are the following:

`-A` Specifies that the rule is to be appended to the specified chain (in this case, the INPUT chain).

Refer to "Notes on the iptables Command Options" on page 154 for alternatives to the `-A` option.

`-s` Specifies that the rule applies to the specified source IP Address (in this case, 10.240.10.240).

`-j` Specifies the action that is to be taken when a packet matching this criteria is received. In this case, the packet is to be dropped.

Refer to "Notes on the iptables Command Options" on page 154 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Example: Accepting Packets Based on the Destination IP Address

The following `iptables` command creates a rule that will allow the LX unit to output packets to the destination IP address 123.146.17.129:

```
In-Reach:/# iptables -A OUTPUT -d 123.146.17.129 -j ACCEPT
```

The options in the above command are the following:

`-A` Specifies that the rule is to be appended to the specified chain (in this case, the OUTPUT chain).

Refer to "Notes on the iptables Command Options" on page 154 for alternatives to the -A option.

`-d` Specifies that the rule applies to the specified destination IP Address (in this case, 123.146.17.129).

`-j` Specifies the action that is to be taken when a packet matching this criteria is received. In this case, the packet is to be accepted.

Refer to "Notes on the iptables Command Options" on page 154 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Example: Ignoring Telnet Requests from a Specific IP Address

The following `iptables` command creates a rule that ignores Telnet requests from the IP address 143.114.56.104:

```
In-Reach:/# iptables -A INPUT -s 143.114.56.104 -p tcp
--destination-port telnet -j DROP
```

The options in the above command are the following:

`-A` Specifies that the rule is to be appended to the specified chain (in this case, the INPUT chain).

Refer to "Notes on the iptables Command Options" on page 154 for alternatives to the -A option.

`-s` Specifies that the rule applies to the specified destination IP Address (in this case, 143.114.56.104).

`-p` Specifies that the rule applies to a particular protocol (in this case, TCP).

Refer to "Notes on the iptables Command Options" on page 154 for a description of the allowable values of the `-p` option.

`--destination-port` Specifies the TCP destination port to which the rule applies. (In this case, the destination port is the Telnet port.)

`-j` Specifies the action that is to be taken when a packet matching this criteria is received. In this case, the packet is to be dropped.

Refer to "Notes on the iptables Command Options" on page 154 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Notes on the `iptables` Command Options

- **Alternatives to the `-A` Option** – You can use the `-I` option or the `-R` option, instead of the `-A` option, to specify how the rule will be added to the chain. The `-I` option specifies that the rule will be inserted at a specified location before the end of the chain. The `-R` option specifies that the rule will replace a specific rule in the chain.

  In the following example, the `-I` option specifies that the rule is to be inserted as the 11th rule in the INPUT chain:

  ```
  iptables -I INPUT 11 -s 10.240.10.240 -j DROP
  ```

  The rules that follow the new rule will be bumped up by 1.

  In the following example, the `-R` option specifies that the rule is to replace the 8th rule in the OUTPUT chain:

  ```
  iptables -R OUTPUT 8 -s 89.247.112.93 -j DROP
  ```

- **Allowable Values of the `-j` Option** – You can specify the following values for the `-j` option:

  ACCEPT – The packet is allowed to pass through the specified chain (i.e., INPUT or OUTPUT).

  DENY – The packet is *not* allowed to pass through the specified chain (i.e., INPUT or OUTPUT). A message indicating that the LX is not accepting connections is sent back to the source IP Address.

  DROP – The packet is *not* allowed to pass through the specified chain (i.e., INPUT or OUTPUT). A message is *not* sent back to the source IP Address.

- **Allowable Values of the `-p` Option** – You can specify TCP, UDP, or ICMP as the value of the `-p` option.

Saving Changes in Rules

The configuration is kept in the file `/config/iptables.conf`. This file is generated by the utility iptables-save upon reading the filter tables located in the Kernel.

The configuration is dynamically applied when an `iptables` command is entered.

The command `iptables-save` creates the new configuration file in `/config/iptables.conf`.

To make this configuration persistent through the reboot, it is necessary to save the configuration to the flash or the network from the Superuser command line.

Do the following to save the iptables configuration:

1. Execute the `shell` command, in the Superuser Command Mode, to access the Linux shell; for example:

   InReach:0 >>`shell`

2. Verify the Iptables configuration with the `iptables -L` command; for example:

   In-Reach:/# `iptables -L`

3. Save the Iptables changes to the `/config/iptables.conf` file; for example:

   ```
   In-Reach:/# iptables-save -f /config/iptables.conf
   ```

4. Execute the `exit` command to return to the Superuser Command Mode; for example:

   ```
   In-Reach:/# exit
   ```

5. Execute the `save configuration` command, in the Superuser Command Mode, to save the `iptables.conf` file to flash or the network; for example:

   ```
   InReach:0 >>save configuration flash
   ```

   NOTE: You can use the `network` option of the `save configuration` command to save the configuration to a network server. For more information, refer to the `save configuration` command in the *LX-Series Commands Reference Guide*.

Appendix A

Overview of RADIUS Authentication

RADIUS authentication occurs through a series of communications between the LX unit and the RADIUS server. Once RADIUS has authenticated a user, the LX unit provides that user with access to the appropriate network services. The RADIUS server maintains a database that contains user authentication and network service access information.

The following example describes the steps in the RADIUS authentication process. In this example, the user attempts to gain access to an LX asynchronous port.

1. The LX unit prompts the user for a username and password.
2. The LX unit takes the username and password and creates an access-request packet identifying the LX unit making the request, the username and password, and the port being used. The LX unit then sends the access-request packet to the designated RADIUS server for authentication.

NOTE: The user password is encrypted to prevent it from being intercepted and reused by an unwanted user. This is done by generating a random vector and placing it in the request header. A copy of the random vector is MD5 encoded using the configured secret. The user's password is then encrypted by XORing it with the encoded copy of the random vector.

3. The RADIUS server validates the request and then decrypts the password.
4. The username and password are authenticated by the RADIUS server.

5. Upon successful authentication, the RADIUS server sends an access-accept packet containing any specific configuration information associated with that user.
6. The LX unit then grants the user the services requested.

If at any point in the authentication process conditions are not met, the RADIUS server sends an authentication rejection to the LX unit and the user is denied access to the network. Figure 24 shows an example of the RADIUS authentication process.

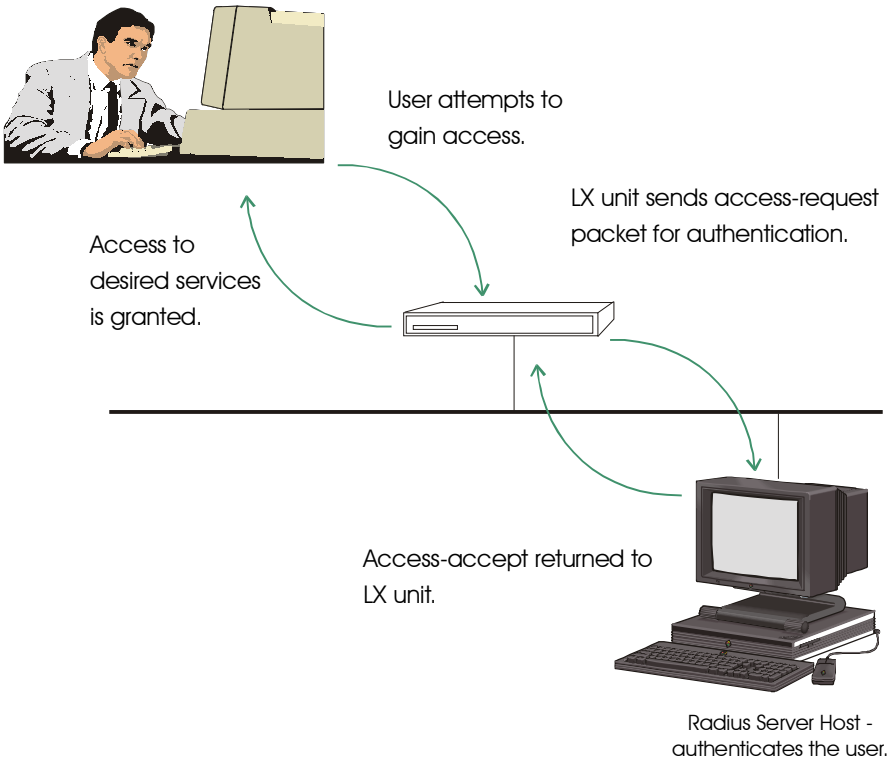

Figure 24 - RADIUS Authentication Process

The LX implementation of RADIUS supports the use of RADIUS secondary servers. The RADIUS secondary server is used when the RADIUS primary server cannot be accessed.

RADIUS Authentication Attributes

Table 9 lists the RADIUS Authentication Attributes that are supported on the LX unit.

NOTE: Some attributes appear in start records, but the majority of attributes appear in stop records (a few also appear in acct-on and acct-off records). RADIUS allows most authentication and configuration attributes to be logged.

Table 9 - Supported RADIUS Authentication Attributes

	Attribute Name	Description
01	User-Name	Name of the user to authenticate.
02	User-Password	The password for the user to authenticate.
03	CHAP-Password	Indicates the CHAP challenge value found in the CHAP-Challenge attribute.
06	Service-Type	Type of service allowed for the connection. The supported types are the following:
	NAS-Prompt	Allows local port access for interactive sessions. The user is prohibited from accessing the Superuser Command Mode. This is true for local port access, Interface virtual port access and access using the GUI.
	Authenticate-Only	Allows local port access for interactive sessions, user is prohibited from accessing the Superuser Command Mode. This Service Type is allowed for local port access, Interface virtual port access and access using the GUI. In each case, the user is prohibited from Superuser access.
	No-Service-Type	Allows local port access for interactive sessions, user is prohibited from accessing the Superuser Command Mode.

	Administrative-User	Allows local port access for interactive sessions. The user is allowed access to Superuser and Configuration Command Modes. This is true for local port access, Interface virtual port access and access using the GUI.
	Framed	Allows local port access for a Dial-in PPP user.
	Outbound-User	Allows only remote port access. If the asynchronous remote-accessed port is configured for outbound RADIUS authentication, the LX requires the user's service-type to be Outbound-User; otherwise the user's access is rejected. **NOTE: All remote access ports on the LX require a Service Type of Outbound-User.**
07	Framed-Protocol	Used with a framed service type. Indicates the type of framed access (e.g., PPP).
08	Framed-IP-Address	The address to be configured for the user.
09	Framed-IP-Netmask	The IP Netmask to be configured for the user when the user is a router to the network.
13	Framed-Compression	The compression protocol for the circuit.
24	State (challenge/response)	Sent by the server to the client in an Access-Challenge, and must be sent unmodified from the client to the server in any Access-Request reply.
60	CHAP-Challenge	

Appendix B

Overview of RADIUS and TACACS+ Accounting

RADIUS Accounting, and TACACS+ Accounting, are client/server account logging schemes that allow you to log user account information to a remote server in a per-client file. The file or record can contain information such as the user who logged in, the duration of the session, port number, Client IP address, and the number of bytes/packets that were processed by the LX unit.

The use of RADIUS Accounting, or TACACS+ Accounting, solves the problems associated with local storage of large numbers of records. It also provides a method for billing customers for account usage.

NOTE: RADIUS Accounting is a developing standard that is *vendor extensible by design*, including a provision for vendor-specific extensions. This allows for greater expandability of accounting information in the future.

The following section describes RADIUS Accounting.

Refer to "TACACS+ Accounting Client Operation" on page 163 for information about TACACS+ Accounting.

RADIUS Accounting Client Operation

If a user is validated under RADIUS, an accounting request (a start request) is sent to the RADIUS accounting server. As a result of the start request, a start record containing the following is created for each user session:

- User-name
- NAS-Identifier
- NAS-IP-Address
- NAS-Port

- NAS-Port-Type
- Acct-Status-Type
- Acct-Session-ID
- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Packets (PPP)
- Acct-Output-Packets (PPP)

The majority of the accounting record information appears in the *stop* record. The stop record is created when the port is logged out, provided that a matching start record was previously sent. The information in the stop record includes everything in the start record, and additional information, such as session time and bytes/packets transferred.

There are two special records that are logged for RADIUS Accounting.

- **Accounting-on** – This record is logged when the LX unit is first booted.
- **Accounting-off** – This record is logged, if possible, when the LX unit is shut down.

These records only contain the NAS-IP-Address. Since these accounting requests only relate to the LX unit using the protocol and not to accounting on a specific port, they are only attempted if the RADIUS protocol is enabled.

RADIUS Accounting Attributes

Table 10 lists the RADIUS Accounting Attributes that are supported on the LX unit.

Table 10 - Supported RADIUS Accounting Attributes

	Attribute Name	Description
01	User-Name	Name of the user to authenticate.
04	NAS-IP-Address	IP address associated with the LX unit.

05	NAS-Port	Port or circuit number associated with the request.
32	NAS-Identifier	The ID that identifies the LX unit to the RADIUS server.
40	Acct-Status-Type	Indicates whether the session has started or stopped. The valid values are: 1 - Start 2 - Stop
42	Acct-Input-Octets	A count of the input octets for the session.
43	Acct-Output-Octets	A count of the output octets for the session.
44	Acct-Session-ID	Session Identifier for the user login.
47	Acct-Input-Packets	A count of the input packets for a PPP session.
48	Acct-Output-Packets	A count of the output packets for a PPP session.
61	NAS-Port-Type	The type of port being used. The valid values are: 0 - Asynchronous

TACACS+ Accounting Client Operation

If a user is validated under TACACS+, an accounting request (a start request) is sent to the TACACS+ accounting server. As a result of the start request, a start record containing the following is created for each user session:

- Start-time
- Bytes
- Bytes-in
- Bytes-out
- Paks (for PPP connections)
- Paks-in (for PPP connections)
- Paks-out (for PPP connections)

Depending on the Accounting Period Interval, an *accounting update request* will be sent which will contain the same fields with the newer information.

The majority of the accounting record information appears in the *stop* record. The stop record is created when the port is logged out, provided that a matching start record was previously sent. The information in the stop record includes everything in the start record, and the following:

- Stop-time
- Elapsed-time

TACACS+ Accounting Attributes

Table 11 lists the TACACS+ Accounting Attributes that are supported on the LX unit.

Table 11 - Supported TACACS+ Accounting Attributes

Attribute Name	Description
Service	Either "ppp" for PPP connection, otherwise equals "shell"
Protocol	Equals "ip" in PPP connections only
Task_id	Each set of start, update, and stop entries should have unique IDs.
Start_time	Time (in seconds since epoch) that the accounting started
Stop_time	Time (in seconds since epoch) that the accounting stopped
Elapsed_time	The number of seconds the user was logged on for
Bytes	The total number of bytes transferred
Bytes_in	The number of bytes received
Bytes_out	The number of bytes transmitted

Paks	The total number of packets transferred (for PPP connections)
Paks_in	The number of packets received (for PPP connections)
Paks_out	The number of packets transmitted (for PPP connections)

Appendix C

Overview of TACACS+ Authentication

TACACS+ authentication occurs through a series of communications between the LX unit and the TACACS+ server. Once TACACS+ has authenticated a user, the LX unit provides that user with access to the appropriate network services. The TACACS+ server maintains a database that contains user authentication and network service access information.

TACACS+ uses the Transport Control Protocol (TCP) on port 49 to ensure reliable transfer. The entire body of the packet is encrypted using a series of 16 byte MD5 hashes. The protocol is split up into 3 distinct categories: Authentication, Authorization, and Accounting.

Authentication is the process of determining who the user is. Usually a user is required to enter in a user name and password to be granted access. Authorization is the process of determining what the user is able to do. The profile in the TACACS+ server should have a service of exec and a priv-lvl of 15 in order to access Superuser privileges, otherwise the user will only be able to be in user mode. Accounting records what the user has done and generally occurs after authentication and authorization.

The TACACS+ superuser request attribute is independent from the TACACS+ login. The TACACS+ superuser request attribute is used to indicate which database to authenticate the superuser password against after a user is logged in. When a user types the `enable` command, and the TACACS+ superuser request is enabled, the enable password will be authenticated against the TACACS+ server database; otherwise it is checked against the LX database "system".

Example of TACACS+ Authentication

The following example describes the steps in the TACACS+ authentication process. In this example, the user attempts to gain access to an LX asynchronous port.

1. The LX unit prompts the user for a username and password.
2. The username is sent to the TACACS+ authentication start packet.
3. The server responds with an authentication reply packet, which will either allow the user access or require a password.
4. If a password is required, the user is prompted for one and the LX sends it to the server in an authentication continue packet.
5. The server responds with a packet that contains an *authentication status pass* or an *authentication status fail*.
6. If the request is successful, the user will be allowed to log in; otherwise the user will have two more chances to receive an *authentication status pass* back from the server.
7. The LX unit then grants the user the services requested.

TACACS+ Authentication Attributes

Table 12 lists the TACACS+ Authentication Attributes that are supported on the LX unit.

Table 12 - Supported TACACS+ Authentication Attributes

	Attribute Name	Description
01	User-Name	Name of the user to authenticate.
02	User-Password	The password for the user to authenticate.

If at any point in the authentication process conditions are not met, the TACACS+ server denies access to the network. Figure 25 shows an example of the TACACS+ authentication process.

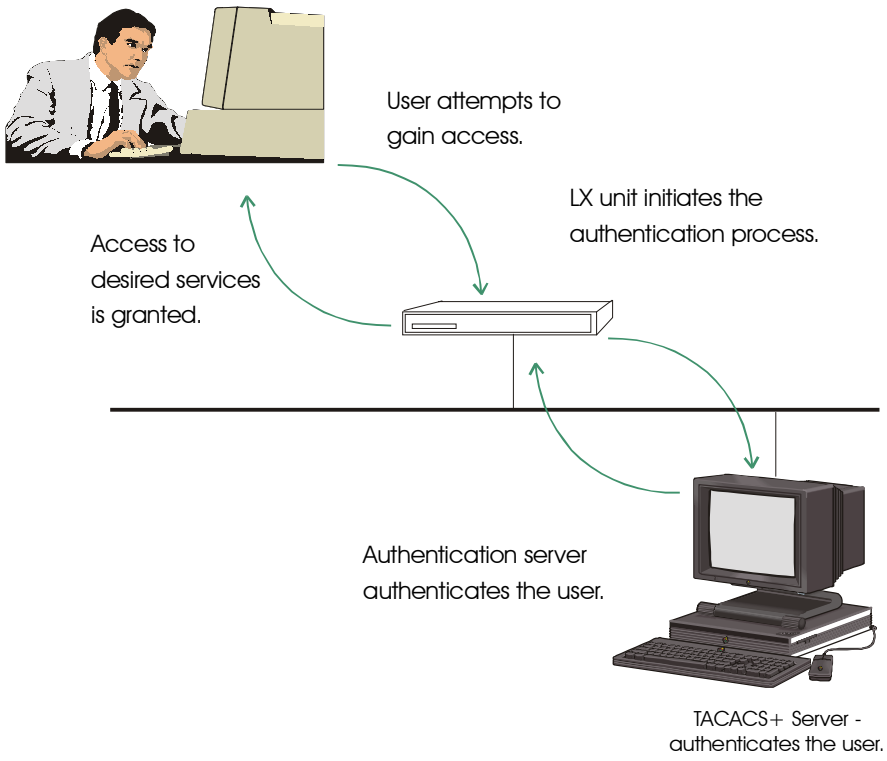

Figure 25 - TACACS+ Authentication Process

The LX implementation of TACACS+ supports the use of TACACS+ secondary servers. The TACACS+ secondary server is used when the TACACS+ primary server cannot be accessed.

Appendix D

Details of the iptables Command

This appendix contains the Linux man pages for the **iptables** command. Refer to the man pages in this appendix for detailed information on the **iptables** command, which is introduced in "Configuring Packet Filters with the iptables Command" on page 151.

iptables man Pages

```
IPTABLES(8)                                                IPTABLES(8)

NAME
       iptables - IP packet filter administration

SYNOPSIS
       iptables -[ADC] chain rule-specification [options]
       iptables -[RI] chain rulenum rule-specification [options]
       iptables -D chain rulenum [options]
       iptables -[LFZ] [chain] [options]
       iptables -[NX] chain
       iptables -P chain target [options]
       iptables -E old-chain-name new-chain-name

DESCRIPTION
       Iptables  is  used  to  set  up, maintain, and inspect the
       tables of IP packet filter  rules  in  the  Linux  kernel.
       Several  different tables may be defined.  Each table con
       tains a number of built-in chains  and  may  also  contain
       user-defined chains.

       Each  chain  is  a  list of rules which can match a set of
       packets.  Each rule specifies what to  do  with  a  packet
```

that matches. This is called a `target', which may be a jump to a user-defined chain in the same table.

TARGETS

A firewall rule specifies criteria for a packet, and a target. If the packet does not match, the next rule in the chain is the examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain or one of the special values ACCEPT, DROP, QUEUE, or RETURN.

ACCEPT means to let the packet through. DROP means to drop the packet on the floor. QUEUE means to pass the packet to userspace (if supported by the kernel). RETURN means stop traversing this chain and resume at the next rule in the previous (calling) chain. If the end of a built-in chain is reached or a rule in a built-in chain with target RETURN is matched, the target specified by the chain policy determines the fate of the packet.

TABLES

There are current three independent tables (which tables are present at any time depends on the kernel configura tion options and which modules are present).

-t, --table

This option specifies the packet matching table which the command should operate on. If the kernel is configured with automatic module loading, an attempt will be made to load the appropriate module for that table if it is not already there.

The tables are as follows: filter This is the default table. It contains the built-in chains INPUT (for packets coming into the box itself), FORWARD (for packets being routed through the box), and OUTPUT (for locally-generated packets). nat This table is consulted when a packet that creates a new connection is encountered. It consists of three built-ins: PREROUTING (for altering packets

as soon as they come in), OUTPUT (for altering locally-generated packets before routing), and POSTROUTING (for altering packets as they are about to go out). mangle This table is used for specialized packet alteration. It has two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing).

OPTIONS

The options that are recognized by iptables can be divided into several different groups.

COMMANDS

These options specify the specific action to perform. Only one of them can be specified on the command line unless otherwise specified below. For all the long versions of the command and option names, you need to use only enough letters to ensure that iptables can differentiate it from all other options.

-A, --append

Append one or more rules to the end of the selected chain. When the source and/or destination names resolve to more than one address, a rule will be added for each possible address combination.

-D, --delete

Delete one or more rules from the selected chain. There are two versions of this command: the rule can be specified as a number in the chain (starting at 1 for the first rule) or a rule to match.

-R, --replace

Replace a rule in the selected chain. If the source and/or destination names resolve to multiple addresses, the command will fail. Rules are numbered starting at 1.

-I, --insert
Insert one or more rules in the selected chain as the given rule number. So, if the rule number is 1, the rule or rules are inserted at the head of the chain. This is also the default if no rule number is specified.

-L, --list
List all rules in the selected chain. If no chain is selected, all chains are listed. It is legal to specify the -Z (zero) option as well, in which case the chain(s) will be atomically listed and zeroed. The exact output is affected by the other arguments given.

-F, --flush
Flush the selected chain. This is equivalent to deleting all the rules one by one.

-Z, --zero
Zero the packet and byte counters in all chains. It is legal to specify the -L, --list (list) option as well, to see the counters immediately before they are cleared. (See above.)

-N, --new-chain
Create a new user-defined chain by the given name. There must be no target of that name already.

-X, --delete-chain
Delete the specified user-defined chain. There must be no references to the chain. If there are, you must delete or replace the referring rules before the chain can be deleted. If no argument is given, it will attempt to delete every non-builtin chain in the table.

-P, --policy
Set the policy for the chain to the given target. See the section TARGETS for the legal targets.

Only non-user-defined chains can have policies, and neither built-in nor user-defined chains can be policy targets.

-E, --rename-chain
Rename the user specified chain to the user sup plied name. This is cosmetic, and has no effect on the structure of the table.

-h Help. Give a (currently very brief) description of the command syntax.

PARAMETERS
The following parameters make up a rule specification (as used in the add, delete, insert, replace and append com mands).

-p, --protocol [!] protocol
The protocol of the rule or of the packet to check. The specified protocol can be one of tcp, udp, icmp, or all, or it can be a numeric value, repre senting one of these protocols or a different one. A protocol name from /etc/protocols is also allowed. A "!" argument before the protocol inverts the test. The number zero is equivalent to all. Protocol all will match with all protocols and is taken as default when this option is omit ted.

-s, --source [!] address[/mask]
Source specification. Address can be either a hostname, a network name, or a plain IP address. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0. A "!" argument before the address specification inverts the sense of the address. The flag --src is a convenient alias for this option.

-d, --destination [!] address[/mask]
Destination specification. See the description of the -s (source) flag for a detailed description of the syntax. The flag --dst is an alias for this option.

-j, --jump target
This specifies the target of the rule; i.e., what to do if the packet matches it. The target can be a user-defined chain (other than the one this rule is in), one of the special builtin targets which decide the fate of the packet immediately, or an extension (see EXTENSIONS below). If this option is omitted in a rule, then matching the rule will have no effect on the packet's fate, but the coun ters on the rule will be incremented.

-i, --in-interface [!] [name]
Optional name of an interface via which a packet is received (for packets entering the INPUT, FORWARD and PREROUTING chains). When the "!" argument is used before the interface name, the sense is inverted. If the interface name ends in a "+", then any interface which begins with this name will match. If this option is omitted, the string "+" is assumed, which will match with any interface name.

-o, --out-interface [!] [name]
Optional name of an interface via which a packet is going to be sent (for packets entering the FORWARD, OUTPUT and POSTROUTING chains). When the "!" argu ment is used before the interface name, the sense is inverted. If the interface name ends in a "+", then any interface which begins with this name will match. If this option is omitted, the string "+" is assumed, which will match with any interface name.

[!] -f, --fragment

This means that the rule only refers to second and further fragments of fragmented packets. Since there is no way to tell the source or destination ports of such a packet (or ICMP type), such a packet will not match any rules which specify them. When the "!" argument precedes the "-f" flag, the rule will only match head fragments, or unfrag mented packets.

-c, --set-counters PKTS BYTES
This enables the administrater to initialize the packet and byte counters of a rule (during INSERT, APPEND, REPLACE operations)

OTHER OPTIONS
The following additional options can be specified:

-v, --verbose
Verbose output. This option makes the list command show the interface address, the rule options (if any), and the TOS masks. The packet and byte coun ters are also listed, with the suffix 'K', 'M' or 'G' for 1000, 1,000,000 and 1,000,000,000 multipli ers respectively (but see the -x flag to change this). For appending, insertion, deletion and replacement, this causes detailed information on the rule or rules to be printed.

-n, --numeric
Numeric output. IP addresses and port numbers will be printed in numeric format. By default, the pro gram will try to display them as host names, net work names, or services (whenever applicable).

-x, --exact
Expand numbers. Display the exact value of the packet and byte counters, instead of only the rounded number in K's (multiples of 1000) M's (mul tiples of 1000K) or G's (multiples of 1000M). This option is only relevant for the -L command.

```
       --line-numbers
              When listing rules, add line numbers to the  begin
              ning  of  each  rule,  corresponding to that rule's
              position in the chain.

       --modprobe=<command>
              When adding or inserting rules into  a  chain,  use
              command  to  load  any  necessary modules (targets,
              match extensions, etc).

MATCH EXTENSIONS
       iptables can use extended packet matching modules.   These
       are  loaded in two ways: implicitly, when -p or --protocol
       is specified, or with the -m or --match options,  followed
       by  the  matching  module name; after these, various extra
       command line options become available,  depending  on  the
       specific  module.  You can specify multiple extended match
       modules in one line, and you can  use  the  -h  or  --help
       options  after  the  module  has been specified to receive
       help specific to that module.

       The following are included in the base package,  and  most
       of  these  can  be preceded by a !  to invert the sense of
       the match.

   tcp
       These extensions are loaded if `--protocol tcp' is  speci
       fied. It provides the following options:

       --source-port [!] [port[:port]]
              Source  port  or port range specification. This can
              either be a service  name  or  a  port  number.  An
              inclusive  range  can  also be specified, using the
              format port:port.  If the first  port  is  omitted,
              "0"  is assumed; if the last is omitted, "65535" is
              assumed.  If the second port greater then the first
              they will be swapped.  The flag --sport is an alias
              for this option.
```

```
    --destination-port [!] [port[:port]]
           Destination port or port range  specification.  The
           flag --dport is an alias for this option.

    --tcp-flags [!] mask comp
           Match  when  the  TCP  flags are as specified.  The
           first argument is the flags which we  should  exam
           ine,  written  as  a  comma-separated list, and the
           second argument is a comma-separated list of  flags
           which  must be set.  Flags are: SYN ACK FIN RST URG
           PSH ALL NONE.  Hence the command
            iptables   -A   FORWARD   -p    tcp    --tcp-flags
           SYN,ACK,FIN,RST SYN
           will  only match packets with the SYN flag set, and
           the ACK, FIN and RST flags unset.

    [!] --syn
           Only match TCP packets with the SYN bit set and the
           ACK and FIN bits cleared.  Such packets are used to
           request TCP  connection  initiation;  for  example,
           blocking  such  packets coming in an interface will
           prevent incoming TCP connections, but outgoing  TCP
           connections  will  be unaffected.  It is equivalent
           to --tcp-flags SYN,RST,ACK SYN.  If  the  "!"  flag
           precedes  the  "--syn",  the sense of the option is
           inverted.

    --tcp-option [!] number
           Match if TCP option set.

udp
    These extensions are loaded if `--protocol udp' is  speci
    fied.  It provides the following options:

    --source-port [!] [port[:port]]
           Source  port  or port range specification.  See the
           description of the --source-port option of the  TCP
           extension for details.
```

```
    --destination-port [!] [port[:port]]
           Destination  port or port range specification.  See
           the description of the --destination-port option of
           the TCP extension for details.

icmp
    This  extension  is  loaded if `--protocol icmp' is speci
    fied.  It provides the following option:

    --icmp-type [!] typename
           This allows specification of the ICMP  type,  which
           can be a numeric ICMP type, or one of the ICMP type
           names shown by the command
            iptables -p icmp -h

mac
    --mac-source [!] address
           Match source MAC address.  It must be of  the  form
           XX:XX:XX:XX:XX:XX.  Note that this only makes sense
           for packets entering  the  PREROUTING,  FORWARD  or
           INPUT  chains  for  packets coming from an ethernet
           device.

limit
    This module matches at a limited rate using a token bucket
    filter:  it can be used in combination with the LOG target
    to give limited logging.  A rule using this extension will
    match  until this limit is reached (unless the `!' flag is
    used).

    --limit rate
           Maximum average matching rate: specified as a  num
           ber,   with   an   optional  `/second',  `/minute',
           `/hour', or `/day' suffix; the default is 3/hour.

    --limit-burst number
           The maximum initial number  of  packets  to  match:
           this  number  gets  recharged by one every time the
           limit specified above is not reached,  up  to  this
           number; the default is 5.
```

multiport
This module matches a set of source or destination ports. Up to 15 ports can be specified. It can only be used in conjunction with -p tcp or -p udp.

--source-port [port[,port]]
Match if the source port is one of the given ports.

--destination-port [port[,port]]
Match if the destination port is one of the given ports.

--port [port[,port]]
Match if the both the source and destination ports are equal to each other and to one of the given ports.

mark
This module matches the netfilter mark field associated with a packet (which can be set using the MARK target below).

--mark value[/mask]
Matches packets with the given unsigned mark value (if a mask is specified, this is logically ANDed with the mark before the comparison).

owner
This module attempts to match various characteristics of the packet creator, for locally-generated packets. It is only valid in the OUTPUT chain, and even this some packets (such as ICMP ping responses) may have no owner, and hence never match.

--uid-owner userid
Matches if the packet was created by a process with the given effective user id.

--gid-owner groupid
Matches if the packet was created by a process with

```
              the given effective group id.

       --pid-owner processid
              Matches if the packet was created by a process with
              the given process id.

       --sid-owner sessionid
              Matches if the packet was created by a  process  in
              the given session group.

   state
       This  module,  when  combined  with  connection  tracking,
       allows access to the connection tracking  state  for  this
       packet.

       --state state
              Where  state  is a comma separated list of the con
              nection  states  to  match.   Possible  states  are
              INVALID  meaning that the packet is associated with
              no known connection, ESTABLISHED meaning  that  the
              packet  is  associated  with a connection which has
              seen packets in both directions, NEW  meaning  that
              the  packet has started a new connection, or other
              wise associated with a  connection  which  has  not
              seen  packets in both directions, and RELATED mean
              ing that the packet is starting a  new  connection,
              but is associated with an existing connection, such
              as an FTP data transfer, or an ICMP error.

   unclean
       This module takes no options, but attempts to match  pack
       ets  which seem malformed or unusual.  This is regarded as
       experimental.

   tos
       This module matches the 8 bits of Type of Service field in
       the IP header (ie. including the precedence bits).

       --tos tos
              The argument is either a standard name, (use
```

```
               iptables -m tos -h
              to see the list), or a numeric value to match.

TARGET EXTENSIONS
       iptables  can  use  extended target modules: the following
       are included in the standard distribution.

   LOG
       Turn on kernel logging of  matching  packets.   When  this
       option is set for a rule, the Linux kernel will print some
       information on all matching packets (like most  IP  header
       fields)  via  the  kernel  log  (where it can be read with
       dmesg or syslogd(8)).

       --log-level level
              Level of logging (numeric or see syslog.conf(5)).

       --log-prefix prefix
              Prefix log messages with the specified  prefix;  up
              to  29  letters long, and useful for distinguishing
              messages in the logs.

       --log-tcp-sequence
              Log TCP sequence numbers. This is a  security  risk
              if the log is readable by users.

       --log-tcp-options
              Log options from the TCP packet header.

       --log-ip-options
              Log options from the IP packet header.

   MARK
       This  is  used  to set the netfilter mark value associated
       with the packet.  It is only valid in the mangle table.

       --set-mark mark
```

REJECT

This is used to send back an error packet in response to the matched packet: otherwise it is equivalent to DROP. This target is only valid in the INPUT, FORWARD and OUTPUT chains, and user-defined chains which are only called from those chains. Several options control the nature of the error packet returned:

--reject-with type

The type given can be icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unreachable, icmp-net-prohibitedor icmp-host-prohibited, which return the appropriate ICMP error message (port-unreachable is the default). The option echo-reply is also allowed; it can only be used for rules which specify an ICMP ping packet, and generates a ping reply. Finally, the option tcp-reset can be used on rules which only match the TCP protocol: this causes a TCP RST packet to be sent back. This is mainly useful for blocking ident probes which frequently occur when sending mail to broken mail hosts (which won't accept your mail otherwise).

TOS

This is used to set the 8-bit Type of Service field in the IP header. It is only valid in the mangle table.

--set-tos tos

You can use a numeric TOS values, or use
iptables -j TOS -h
to see the list of valid TOS names.

MIRROR

This is an experimental demonstration target which inverts the source and destination fields in the IP header and retransmits the packet. It is only valid in the INPUT, FORWARD and PREROUTING chains, and user-defined chains which are only called from those chains. Note that the outgoing packets are NOT seen by any packet filtering

chains, connection tracking or NAT, to avoid loops and other problems.

SNAT

This target is only valid in the nat table, in the POSTROUTING chain. It specifies that the source address of the packet should be modified (and all future packets in this connection will also be mangled), and rules should cease being examined. It takes one option:

--to-source <ipaddr>[-<ipaddr>][:port-port]

which can specify a single new source IP address, an inclusive range of IP addresses, and optionally, a port range (which is only valid if the rule also specifies -p tcp or -p udp). If no port range is specified, then source ports below 512 will be mapped to other ports below 512: those between 512 and 1023 inclusive will be mapped to ports below 1024, and other ports will be mapped to 1024 or above. Where possible, no port alteration will occur.

DNAT

This target is only valid in the nat table, in the PRE ROUTING and OUTPUT chains, and user-defined chains which are only called from those chains. It specifies that the destination address of the packet should be modified (and all future packets in this connection will also be man gled), and rules should cease being examined. It takes one option:

--to-destination <ipaddr>[-<ipaddr>][:port-port]

which can specify a single new destination IP address, an inclusive range of IP addresses, and optionally, a port range (which is only valid if the rule also specifies -p tcp or -p udp). If no port range is specified, then the destination port will never be modified.

MASQUERADE
This target is only valid in the nat table, in the POSTROUTING chain. It should only be used with dynami cally assigned IP (dialup) connections: if you have a static IP address, you should use the SNAT target. Mas querading is equivalent to specifying a mapping to the IP address of the interface the packet is going out, but also has the effect that connections are forgotten when the interface goes down. This is the correct behavior when the next dialup is unlikely to have the same interface address (and hence any established connections are lost anyway). It takes one option:

--to-ports <port>[-<port>]
This specifies a range of source ports to use, overriding the default SNAT source port-selection heuristics (see above). This is only valid with if the rule also specifies -p tcp or -p udp).

REDIRECT
This target is only valid in the nat table, in the PRE ROUTING and OUTPUT chains, and user-defined chains which are only called from those chains. It alters the destina tion IP address to send the packet to the machine itself (locally-generated packets are mapped to the 127.0.0.1 address). It takes one option:

--to-ports <port>[-<port>]
This specifies a destination port or range or ports to use: without this, the destination port is never altered. This is only valid with if the rule also specifies -p tcp or -p udp).

EXTRA EXTENSIONS
The following extensions are not included by default in the standard distribution.

ttl
This module matches the time to live field in the IP header.

```
   --ttl ttl
          Matches the given TTL value.

TTL
    This  target  is  used to modify the time to live field in
    the IP header.  It is only valid in the mangle table.

    --ttl-set ttl
          Set the TTL to the given value.

    --ttl-dec ttl
          Decrement the TTL by the given value.

    --ttl-inc ttl
          Increment the TTL by the given value.

ULOG
    This target provides userspace logging of  matching  pack
    ets.  When this target is set for a rule, the Linux kernel
    will multicast this packet through a netlink  socket.  One
    or  more userspace processes may then subscribe to various
    multicast groups and receive the packets.

    --ulog-nlgroup <nlgroup>
          This specifies the netlink group  (1-32)  to  which
          the packet is sent.  Default value is 1.

    --ulog-prefix <prefix>
          Prefix  log  messages with the specified prefix; up
          to 32 characters long, and useful fro  distinguish
          ing messages in the logs.

    --ulog-cprange <size>
          Number  of bytes to be copied to userspace. A value
          of 0 always copies the entire packet, regardless of
          its size. Default is 0

    --ulog-qthreshold <size>
          Number  of  packet  to queue inside kernel. Setting
          this value to,  e.g.  10  accumulates  ten  packets
```

inside the kernel and transmits them as one netlink multpart message to userspace. Default is 1 (for backwards compatibility)

DIAGNOSTICS

Various error messages are printed to standard error. The exit code is 0 for correct functioning. Errors which appear to be caused by invalid or abused command line parameters cause an exit code of 2, and other errors cause an exit code of 1.

BUGS

Check is not implemented (yet).

COMPATIBILITY WITH IPCHAINS

This iptables is very similar to ipchains by Rusty Rus sell. The main difference is that the chains INPUT and OUTPUT are only traversed for packets coming into the local host and originating from the local host respec tively. Hence every packet only passes through one of the three chains; previously a forwarded packet would pass through all three.

The other main difference is that -i refers to the input interface; -o refers to the output interface, and both are available for packets entering the FORWARD chain.

iptables is a pure packet filter when using the default `filter' table, with optional extension modules. This

its size. Default is 0

--ulog-qthreshold <size>

Number of packet to queue inside kernel. Setting this value to, e.g. 10 accumulates ten packets inside the kernel and transmits them as one netlink multpart message to userspace. Default is 1 (for backwards compatibility)

DIAGNOSTICS

Various error messages are printed to standard error. The exit code is 0 for correct functioning. Errors which appear to be caused by invalid or abused command line parameters cause an exit code of 2, and other errors cause an exit code of 1.

BUGS

Check is not implemented (yet).

COMPATIBILITY WITH IPCHAINS

This iptables is very similar to ipchains by Rusty Rus sell. The main difference is that the chains INPUT and OUTPUT are only traversed for packets coming into the local host and originating from the local host respec tively. Hence every packet only passes through one of the three chains; previously a forwarded packet would pass through all three.

The other main difference is that -i refers to the input interface; -o refers to the output interface, and both are available for packets entering the FORWARD chain.

iptables is a pure packet filter when using the default `filter' table, with optional extension modules. This should simplify much of the previous confusion over the combination of IP masquerading and packet filtering seen previously. So the following options are handled differ ently:

-j MASQ
-M -S
-M -L

There are several other changes in iptables.

SEE ALSO

The iptables-HOWTO, which details more iptables usage, the NAT-HOWTO, which details NAT, and the netfilter-hacking-HOWTO which details the internals.

```
AUTHORS
       Rusty Russell wrote iptables, in early  consultation  with
       Michael Neuling.
       Marc Boucher made Rusty abandon ipnatctl by lobbying for a
       generic packet selection framework in iptables, then wrote
       the mangle table, the owner match, the mark stuff, and ran
       around doing cool stuff everywhere.

       James Morris wrote the TOS target, and tos match.

       Jozsef Kadlecsik wrote the REJECT target.

       Harald Welte wrote the ULOG target, TTL  match+target  and
       libipulog.

       The  Netfilter  Core  Team is: Marc Boucher, James Morris,
       Harald Welte and Rusty Russell.
```

Appendix 3

```
IPTABLES-SAVE(8)                                    IPTABLES-SAVE(8)

NAME
       iptables-save - Save IP Tables

SYNOPSIS
       iptables-save [-c] [-t table]

DESCRIPTION
       iptables-save  is used to dump the contents of an IP Table
       in easily parseable format to STDOUT. Use  I/O-redirection
       provided by your shell to write to a file.

       -c, --counters
              include  the  current values of all packet and byte
              counters in the output
```

```
       -t, --table tablename

       restrict output to only  one  table.  If  not  specified,
       output includes all available tables.

BUGS
       None known as of iptables-1.2.1 release

AUTHOR
       Harald Welte <laforge@gnumonks.org>

SEE ALSO
       iptables-restore(8), iptables(8)

       The iptables-HOWTO, which details more iptables usage, the
       NAT-HOWTO,  which  details NAT, and the netfilter-hacking-
       HOWTO which details the internals.
```

Appendix 4

```
IPTABLES-RESTORE(8)                              IPTABLES-RESTORE(8)

NAME
       iptables-restore - Restore IP Tables

SYNOPSIS
       iptables-restore [-c] [-n]

DESCRIPTION
       iptables-restore  is  used  to restore IP Tables from data
       specified on STDIN. Use I/O redirection provided  by  your
       shell to read from a file

       -c, --counters
              restore the values of all packet and byte counters

       -n, --noflush
       don't flush the previous contents of the table. If not
       specified, iptables-restore  flushes  (deletes)  all
       previous contents of the respective IP Table.
```

```
BUGS
       None known as of iptables-1.2.1 release

AUTHOR
       Harald Welte <laforge@gnumonks.org>

SEE ALSO
       iptables-restore(8), iptables(8)

       The iptables-HOWTO, which details more iptables usage, the
       NAT-HOWTO,  which  details NAT, and the netfilter-hacking-
       HOWTO which details the internals.
```

INDEX

T

U

W