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)

MRV Americas Service and Support
295 Foster Street
Littleton, MA 01460
Tel: 800-435-7997
Tel: +001 978-952-4888 (Outside U.S.)
Email: service@mrv.com

MRV America Sales
295 Foster Street
Littleton, MA 01460
Tel: 800-338-5316 (U.S.)
Email: sales@mrv.com

MRV International Sales
Business Park Moerfelden
Waldeckerstrasse 13
64546 Moerfelden-Walldorf
Germany
Tel: (49) 6105/2070
Fax: (49) 6105/207-100
Email: sales@mrv.com

451-0311N

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.

EXPORT NOTICE

MRV models contain 128-bit encryption software. Export of this product is restricted under U.S. law. Information is available from the U.S. Department of Commerce, Bureau of Export Administration at www.bxa.doc.gov.

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 configure IP interfaces.
- **Chapter 6** – Describes how to set up the Data Broadcast Feature.
- **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.
- **Chapter 11** – Describes how to configure the Trigger-Action Feature.
- **Chapter 12** – Describes how to configure the Cluster Configuration and Control feature.
- **Chapter 13** – Describes the MIB structure and how to configure SNMP.
- **Chapter 14** - Describes how to configure the High Density Alarm Manager (HDAM).

- **Chapter 15** - Describes how to configure PPP Dial-On-Demand.
- **Chapter 16** - Describes how to configure Redundant Ethernet.
- **Chapter 17** - Describes how to configure the Internal Modem.
- **Chapter 18** - Describes how to configure Alarm Input/Control Output Points.
- **Chapter 19** - Describes how to configure the IPv6 Internet Protocol.
- **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.
- **Appendix E** – Describes Multi-Level Command Execution.
- **Appendix F** – Describes how to enable/disable TCP ports/IR Listener ports.
- **Appendix G** – Describes RADIUS Vendor Specific Dictionary files.
- **Appendix H** – Describes how to configure rlogin support.
- **Appendix I** – Describes FIPS support.

Conventions

The following conventions are used throughout this guide:

- **Command execution –** Unless otherwise specified, commands are executed when you press <RETURN>.
- **Command syntax –** Where command options or command syntax are shown, keywords and commands are shown in lowercase letters.

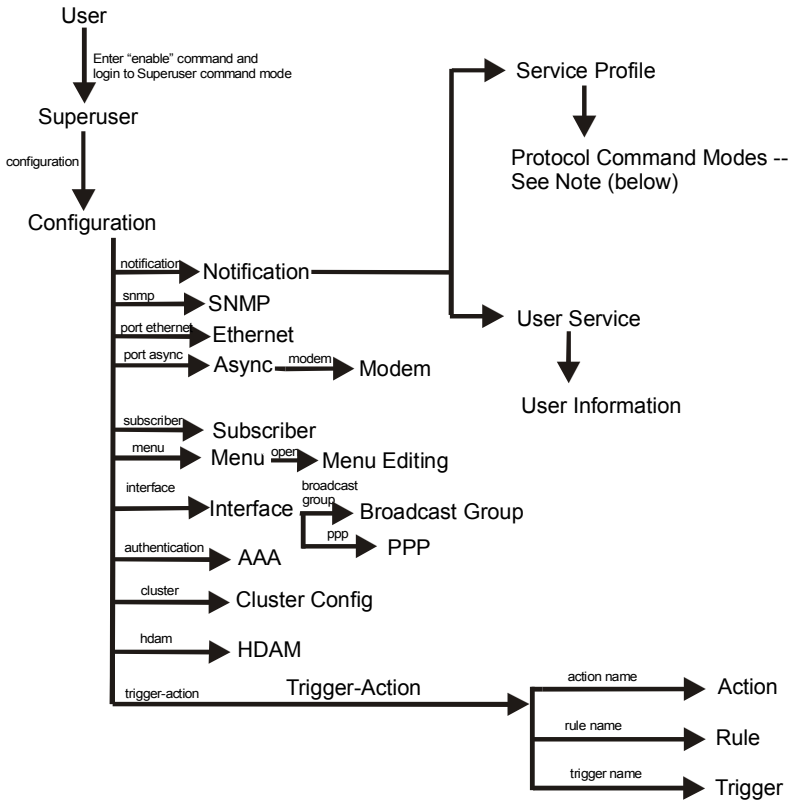
- **Keyboard characters (keys)** – Keyboard characters are represented using left and right angle brackets (< and >). For example, the notation <CTRL> refers to the CTRL key; <A> refers to the letter A; and <RETURN> refers to the RETURN key.
- **Typographical conventions –** The following typographical 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.

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 (below) lists the command modes in the LX CLI.



Note: The Protocol Command Modes include Async, Localsyslog, Remotesyslog, SMTP, SNPP, TAP, and WEB.

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.

Type `^K` to clear the current command line.

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 Configuration command mode to return to the Superuser command mode.

You can execute the `monitor/show` commands in each of the LX command modes. The `monitor/show` commands are used to display global information for the LX unit.

The CLI supports execution of multiple level commands on the same line. For example:

InReach>> `config port async 1 1 prompt tim`

You can execute a command from any level, if you know the complete path.

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

Command Mode Descriptions

- **User Command Mode –** Contains commands for performing user functions on the LX unit.
  - When you log on to the LX unit, you are in the **User Command Mode**.
  - **Command prompt:** `InReach:0 >`

    For more information, see "User Commands" in the *LX-Series Commands Reference Guide*.

- **Superuser Command Mode** – Contains commands for performing Superuser functions on the LX unit.
  - Accessed by executing the `enable` command in the **User Command Mode**, and then entering the Superuser password when prompted. (The default Superuser password is `system`.)
  - **Command prompt:** `InReach:0 >>`

    For more information, see "Superuser Commands" in the *LX-Series Commands Reference Guide*.

- **Configuration Command Mode** – Contains commands for configuring the LX unit at the server level and accessing nested command modes.
  - Accessed by executing the `configuration` command in the **Superuser Command Mode**.
  - **Command prompt:** `Config:0 >>`

    For more information, see "Configuration Commands" in the *LX-Series Commands Reference Guide*.

- **Authentication, Accounting, and Authorization (AAA) Command Mode** – Contains commands for configuring local and server-based authentication and authorization, and RADIUS and TACACS+ accounting, on the LX unit.
  - Accessed by executing the `aaa` command in the **Configuration Command Mode**.
  - **Command prompt:** `AAA:0 >>`

    For more information, see "Authentication, Accounting, and Authorization Commands" in the *LX-Series Commands Reference Guide*.

- **Asynchronous Command Mode** – Contains commands for configuring asynchronous ports on the LX unit.
  - Accessed by executing the `port async <port_number>` command in the **Configuration Command Mode**.
  - **Command prompt:** `Async 4-4:0 >>`

    For more information, see "Asynchronous Commands" in the *LX-Series Commands Reference Guide*.

- **Ethernet Command Mode** – Contains commands for configuring the Ethernet port on the LX unit.
  - Accessed by executing the `port ethernet <port_number>` command in the **Configuration Command Mode**.
  - **Command prompt:** `Ether 1-1:0 >>`

    For more information, see "Ethernet Commands" in the *LX-Series Commands Reference Guide*.

- **PPP Command Mode** – Contains commands for configuring PPP sessions on the LX unit.

  - Accessed by executing the `ppp` command in the **Interface Command Mode**.
  - **Command prompt:** `PPP 4-4:0 >>`

    For more information, see "PPP Commands" in the *LX-Series Commands Reference Guide*.

- **Modem Command Mode** – Contains commands for configuring modems on LX asynchronous ports.
  - Accessed by executing the `modem` command in the **Asynchronous Command Mode**.
  - **Command prompt:** `Modem 4-4:0 >>`

    For more information, see "Modem Commands" in the *LX-Series Commands Reference Guide*.

- **Subscriber Command Mode** – Contains commands for configuring LX subscriber accounts.
  - Accessed by executing the `subscriber <subscriber_name>` command in the **Configuration Command Mode**.
  - **Command prompt:** `Subs_mark >>`

    For more information, see "Subscriber Commands" in the *LX-Series Commands Reference Guide*.

- **SNMP Command Mode** – Contains commands for configuring SNMP on the LX unit.
  - Accessed by executing the `snmp` command in the **Configuration Command Mode**.
  - **Command prompt:** `Snmp:0 >>`

    For more information, see "SNMP Commands" in the *LX-Series Commands Reference Guide*.

- **Interface Command Mode** – Contains commands for configuring IP interfaces on the LX unit.
  - Accessed by executing the `interface <interface_number>` command in the **Configuration Command Mode**.
  - **Command prompt:** `Intf 1-1:0 >>`

    For more information, see "Interface Commands" in the *LX-Series Commands Reference Guide*.

- **Menu Command Mode** – Contains commands for creating, displaying, and accessing subscriber menus.
  - Accessed by executing the `menu` command in the **Configuration Command Mode**.
  - **Command prompt:** `Menu :0 >>`

    For more information, see "Menu Commands" in the *LX-Series Commands Reference Guide*.

- **Menu Editing Command Mode** – Contains commands for creating and modifying entries in subscriber menus.
  - Accessed by executing the `open <menu_name>` command in the **Menu Command Mode**.
  - **Command prompt:** `menu_name-1:0 >>`

    For more information, see "Menu Editing Commands" in the *LX-Series Commands Reference Guide*.

- **Notification Command Mode** – Contains commands for configuring the LX Notification Feature.
  - Accessed by executing the `notification` command in the **Configuration Command Mode**.
  - **Command prompt:** `Notification:0 >>`

For more information, see "Notification Commands" in the *LX-Series Commands Reference Guide*.

- **Broadcast Group Command Mode** – Contains commands for configuring Broadcast Groups on the LX unit.
  - Accessed by executing the `broadcast group <group_number>` command in the **Interface Command Mode**.
  - **Command prompt:** `BrGroups 6:0 >>`

    For more information, see "Broadcast Group Commands" in the *LX-Series Commands Reference Guide*.

- **Service Profile Command Mode** – Contains commands for specifying the protocol for a Service Profile.
  - Accessed by executing the `profile service <profile_name>` command in the **Notification Command Mode**.
  - **Command prompt:** `Noti_Serv_Protocol:0 >>`

    For more information, see "Service Profile Commands" in the *LX-Series Commands Reference Guide*.

- **Async Protocol Command Mode** – Contains the port command for specifying the asynchronous port parameter for a Service Profile of the Async type.
  - Accessed by executing the `async` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_Async:0 >>`

    For more information, see "Async Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **Localsyslog Protocol Command Mode** – Contains the `file` command for specifying the local file to which syslog messages will be sent under a Service Profile of the Localsyslog type.

- Accessed by executing the `localsyslog` command in the **Service Profile Command Mode**.
- **Command prompt:** `Noti_Serv_LSyslog:0 >>`

  For more information, see "Localsyslog Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **Remotesyslog Protocol Command Mode** – Contains the `host` command for configuring the remote host IP address for a Service Profile of the Remotesyslog type.
  - Accessed by executing the `remotesyslog` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_RSyslog:0 >>`

    For more information, see "Remotesyslog Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **SMTP Protocol Command Mode** – Contains the `server` command for configuring the server for a Service Profile of the SMTP type.
  - Accessed by executing the `smtp` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_SMTP:0 >>`

    For more information, see "SMTP Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **SNPP Protocol Command Mode** – Contains commands for configuring a Service Profile of the SNPP type.
  - Accessed by executing the `snpp` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_SNPP:0 >>`

    For more information, see "SNPP Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **TAP Protocol Command Mode** – Contains commands for configuring a Service Profile of the TAP type.
  - Accessed by executing the `tap` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_TAP:0 >>`

    For more information, see "TAP Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **WEB Protocol Command Mode** – Contains the `driver` command for specifying the web driver for a Service Profile of the WEB type.
  - Accessed by executing the `web` command in the **Service Profile Command Mode**.
  - **Command prompt:** `Noti_Serv_Web:0 >>`

    For more information, see "WEB Protocol Commands" in the *LX-Series Commands Reference Guide*.

- **User Service Command Mode** – Contains the `service` command for specifying a Service Profile for a User Profile.
  - Accessed by executing the `profile user <username>` command in the **Notification Command Mode**.
  - **Command prompt:** `Noti_User_Service:0 >>`

    For more information, see "User Service Commands" in the *LX-Series Commands Reference Guide*.

- **User Information Command Mode** – Contains commands for specifying the contact, facility, and priority parameters of a User Profile.
  - Accessed by executing the `service` command in the **User Service Command Mode**.
  - **Command prompt:** `Noti_User_Info:0 >>`

For more information, see "User Information Commands" in the *LX-Series Commands Reference Guide*.

- **Trigger-Action Command Mode** – Contains commands for creating, or accessing, Actions, Rules, and Triggers for the Trigger-Action Feature.
  - Accessed by executing the `trigger-action` command in the **Notification Command Mode**.
  - **Command prompt:** `Trigger-Action:0 >>`

    For more information, see "Trigger-Action Commands" in the *LX-Series Commands Reference Guide*.

- **Rule Command Mode** – Contains commands for enabling, disabling, and specifying Actions and Triggers for Rules.
  - Accessed by executing the `rule name <rule_name>` command in the **Trigger-Action Command Mode**.
  - **Command prompt:** `Rule_AC7TurnOnRule:0 >>`

    For more information, see "Rule Commands" in the *LX-Series Commands Reference Guide*.

- **Action Command Mode** – Contains the `command` command for specifying an LCX CLI command for an Action.
  - Accessed by executing the `action name` command in the **Trigger-Action Command Mode**.
  - **Command prompt:** `Action_TurnOnAC7:0 >>`

    For more information, see "Action Commands" in the *LX-Series Commands Reference Guide*.

- **Trigger Command Mode** – Contains commands for specifying the conditions for triggers.

  - Accessed by executing the `trigger name` command in the **Trigger-Action Command Mode**.
  - **Command prompt:** `Trigger_TempPortCT30:0 >>`

    For more information, see "Trigger Commands" in the *LX-Series Commands Reference Guide*.

- **Cluster Command Mode** – Contains commands for creating and monitoring clusters.
  - Accessed by executing the `cluster` command in the **Configuration Command Mode**.
  - **Command prompt:** `Cluster:0 >>`

    For more information, see "Cluster Configuration and Control Commands" in the *LX-Series Commands Reference Guide*.

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 mode command prompt:

```
clear          Clear screen and reset terminal line
enable         Turn on privileged commands
exit           Exit up one level
menu           Menu utility
monitor        Monitor running system information
no             Negate a command
outlet         Manipulate outlets
ping           Send echo messages
```

```
shell          Run a shell as Superuser
show           Show running system information
ssh            Secure Shell (3DES/Blowfish)
telnet         Open a telnet connection
terminal       Set the terminal type
<cr>
```

- 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.

Using the Function Keys

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

- **Tab key** – Completes a partially typed command. For example, if you type the tab key after you type **show ve** at the Superuser command prompt, the `show version` command will be executed.
- **Up arrow** – Recalls the last command.
- **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.

Related Documents

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

For more information on the LX-8000 hardware, refer to *Getting Started with the LX-8000 Series* (P/N 451-0331).

The *LX-8000 Quick Start Instructions* (P/N 451-0332) describes how to get the LX-8000 unit up and running.

For more information on the LX-4000 hardware, refer to *Getting Started with the LX-4000 Series* (P/N 451-0308).

The *LX-4000 Quick Start Instructions* (P/N 451-0312) describes how to get the LX-4000 unit up and running.

For more information on the LX-1000 hardware, refer to *Getting Started with the LX-1000 Series* (P/N 451-0320).

The *LX-1000 Quick Start Instructions* (P/N 451-0321) describes how to get the LX-4000 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 `"Enter your superuser password"` message appears, followed by the Superuser Password prompt.
3. Enter the superuser 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 Cluster Secret
            7 Superuser Password
            8 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 `8` (`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 Cluster Secret                        Configured
            7 Superuser Password                    Changed
            8 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 41. 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 82.

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 LDAP, RADIUS, TACACS+, and SecurID security. Under LDAP, 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 Server-Based Authentication and Accounting" on page 43.

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 page 26 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 page 26 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 Server-Based Authentication and Accounting

You can implement four methods of server-based authentication, and two methods of server-based accounting, for the LX unit. The four methods of server-based authentication are SecurID, RADIUS, TACACS+, and LDAP. The two methods of server-based accounting are RADIUS and TACACS+. For more information, refer to the following:

- "Setting Up LDAP" (below)
- "Setting Up RADIUS" on page 48
- "Setting Up TACACS+" on page 53
- "Setting Up SecurID" on page 59

Setting Up LDAP

The LX can implement LDAP authentication for specific interfaces and asynchronous ports. However, you must configure LDAP 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 LDAP authentication at the server level are:

1. Installing and configuring the LDAP server on a Network-based Host (see page 44).
2. Specifying the LDAP server settings on the LX (see page 45).

For more information on LDAP authentication, refer to http://www.directory-applications.com/ldap3_files/frame.htm.

You also have the option of configuring an LDAP Local Subscriber. For more information, refer to "LDAP Local Subscriber Feature" on page 47.

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

Before you can authenticate with LDAP on your LX unit, you must configure an LDAP server on your network.

In general, LDAP server implementations are available on the Internet.

Under LDAP, each attempted login is treated as a request for directory services. When a user attempts to log in via LDAP, he must enter a username/password combination. The username must match the *uid* component of the user's Distinguished Name (DN). The password must match the *userPassword* attribute for the user's *uid*. In order to authenticate the user, the LX binds anonymously to the LDAP server and searches for the user's *uid*. After the *uid* entry is found, a subsequent bind is used to authenticate with the LDAP server using the DN and the password supplied.

To configure the LDAP server, refer to your LDAP server documentation.

Specifying the LDAP Server Settings on the LX

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

1. Verify that the primary LDAP Server has been installed on the primary LDAP Server host.
2. Access the AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA Command Mode.)
3. Use the `ldap primary authentication server address` command to specify the IP address of the LDAP primary authentication server; for example:

   ```
   AAA:0 >>ldap primary authentication server address
   143.34.87.93
   ```

4. Use the `ldap primary authentication server port` command to specify the TCP socket your LDAP server is listening to; for example:

   ```
   AAA:0 >>ldap primary authentication server port 1823
   ```

   NOTE: The LX listens to port 389 by default.

5. Use the `ldap primary authentication server base dn` command to specify the search path that will be used to find a match for the *uid* (User ID) component of the Distinguished Name on the LDAP primary authentication server; for example:

   ```
   AAA:0 >>ldap primary authentication server base dn
   O=box7.acme.boston.sqa.com
   ```

6. Specify the maximum number of retries that the LX unit will have for transmitting an Access Request to the LDAP primary authentication server; for example:

   ```
   AAA:0 >>ldap primary authentication server
   retransmit 7
   ```

7. Specify the length of time that the LX unit will wait for the LX unit to respond before retransmitting packets to the LDAP primary authentication server; for example:

```
AAA:0 >>ldap primary authentication server timeout 4
```

8. To verify the LX LDAP configuration, execute the `show ldap characteristics` command; for example:

```
AAA:0 >>show ldap characteristics
```

In order to use an LDAP secondary authentication server, you must specify the following values for it: IP address, search path, TCP socket, retransmit value, and timeout value. For examples of the commands that you would use to set these values, refer to "LDAP Secondary Authentication Server Commands" on page 46.

NOTE: The use of an LDAP secondary authentication server is optional.

LDAP Command Examples

This section provides examples of all of the commands that are used to specify settings for the LDAP servers. Refer to the "Authentication, Accounting, and Authorization Commands" chapter of the *LX-Series Commands Reference Guide* for detailed descriptions of the commands in this chapter.

LDAP Primary Authentication Server Commands

```
AAA:0 >>ldap primary authentication server address
143.34.87.93
AAA:0 >>ldap primary authentication server base dn O=box7.acme.
boston.sqa.com
AAA:0 >>ldap primary authentication server port 1823
AAA:0 >>ldap primary authentication server retransmit 7
AAA:0 >>ldap primary authentication server timeout 4
```

LDAP Secondary Authentication Server Commands

```
AAA:0 >>ldap secondary authentication server address
143.35.86.122
```

```
AAA:0 >>ldap secondary authentication server base dn
O=box7.acme.boston.sqa.com
AAA:0 >>ldap secondary authentication server port 1948
AAA:0 >>ldap secondary authentication server retransmit 7
AAA:0 >>ldap secondary authentication server timeout 4
```

LDAP Local Subscriber Feature

Under the LDAP Local Subscriber Feature, a subscriber can be logged on in one of two ways:

- As an LX subscriber with the attributes of that subscriber (if the LX subscriber account exists)
- Or, if the LX subscriber account does *not* exist, as the default (InReach) subscriber.

Under either scenario, the subscriber must have an LDAP account on the LDAP authentication server. If the subscriber account also exists on the LX unit, the subscriber is logged on under that account and with the attributes of that account. If the subscriber account does *not* exist on the LX unit, the subscriber is logged on under his LDAP account with the attributes of the default (InReach) account.

Use the `ldap local subscriber enable` command to configure the LDAP Local Subscriber Feature for the LX unit; for example:

```
AAA:0 >>ldap local subscriber enable
```

When the LDAP Local Subscriber Feature is set to `only`, the subscriber can only be logged in if the subscriber account is configured on both the LX unit and the LDAP authentication server *and* the subscriber account on the LX server has the same name as the subscriber account on the LDAP authentication server.

Use the `ldap local subscriber only` command to set the LDAP Local Subscriber Feature to `only`; for example:

```
AAA:0 >>ldap local subscriber only
```

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 48).
2. Specifying the RADIUS server settings on the LX (see page 49).
3. Specifying the RADIUS period on the LX (see page 52).

For more information on RADIUS authentication, refer to "Overview of RADIUS Authentication" on page 371.

For more information on RADIUS accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 377.

You also have the option of configuring a RADIUS Local Subscriber. For more information, refer to "RADIUS Local Subscriber Feature" on page 52.

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 AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA Command Mode.)
3. Use the `radius primary authentication server address` command to specify the IP address of the RADIUS primary authentication server; for example:

   ```
   AAA: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. You can use upper and lower case in combination, as long as the case matches that of the secret on the other side. For example:

   ```
   AAA: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:

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

   NOTE: The LX listens to port 1812 by default.

6. To verify the LX RADIUS configuration, execute the `show radius characteristics` command; for example:

   AAA:0 >>`show radius characteristics`

   Refer to Table 1 on page 50 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 51
   - "RADIUS Secondary Authentication Server Commands" on page 52
   - "RADIUS Secondary Accounting Server Commands" on page 52

   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

```
AAA:0 >>radius primary authentication server address 152.34.65.33
AAA:0 >>radius primary authentication server port 1645
AAA:0 >>radius primary authentication server retransmit 3
AAA:0 >>radius primary authentication server secret AaBbCc
AAA:0 >>radius primary authentication server timeout 7
```

RADIUS Primary Accounting Server Commands

```
AAA:0 >>radius primary accounting server address 181.28.68.56
AAA:0 >>radius primary accounting server port 1646
AAA:0 >>radius primary accounting server retransmit 3
AAA:0 >>radius primary accounting server secret reuyyurew
```

```
AAA:0 >>radius primary accounting server timeout 7
```

RADIUS Secondary Authentication Server Commands

```
AAA:0 >>radius secondary authentication server address 178.67.82.78
AAA:0 >>radius secondary authentication server port 1812
AAA:0 >>radius secondary authentication server retransmit 3
AAA:0 >>radius secondary authentication server secret AsJkirbg
AAA:0 >>radius secondary authentication server timeout 7
```

RADIUS Secondary Accounting Server Commands

```
AAA:0 >>radius secondary accounting server address 198.20.84.77
AAA:0 >>radius secondary accounting server port 1813
AAA:0 >>radius secondary accounting server retransmit 3
AAA:0 >>radius secondary accounting server secret GgJjoreou
AAA: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 AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA Command Mode.)
2. Use the `radius period` command to specify the RADIUS period; for example:

```
AAA:0 >>radius period 10
```

RADIUS Local Subscriber Feature

Under the RADIUS Local Subscriber Feature, a subscriber can be logged on in one of two ways:

- As an LX subscriber with the attributes of that subscriber (if the LX subscriber account exists)
- Or, if the LX subscriber account does *not* exist, as the default (InReach) subscriber.

Under either scenario, the subscriber must have a RADIUS account on the RADIUS server. If the subscriber account also exists on the LX unit, the subscriber is logged on under that account and with the attributes of that account. If the subscriber account does *not* exist on the LX unit, the subscriber is logged on under his RADIUS account with the attributes of the default (InReach) account.

Use the `radius local subscriber enable` command to configure the RADIUS Local Subscriber Feature for the LX unit; for example:

```
AAA:0 >>radius local subscriber enable
```

When the RADIUS Local Subscriber Feature is set to `only`, the subscriber can only be logged in if the subscriber account is configured on both the LX unit and the RADIUS server *and* the subscriber account on the LX server has the same name as the subscriber account on the RADIUS server.

Use the `radius local subscriber only` command to set the RADIUS Local Subscriber Feature to `only`; for example:

```
AAA:0 >>radius local subscriber only
```

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 54).

2. Specifying the TACACS+ server settings on the LX (see page 55).
3. Specifying the TACACS+ period on the LX (see page 59).

For more information on TACACS+ authentication, refer to "Overview of TACACS+ Authentication and Authorization" on page 383.

For more information on TACACS+ accounting, refer to "Overview of RADIUS and TACACS+ Accounting" on page 377.

You also have the option of configuring a TACACS+ Local Subscriber. For more information, refer to "TACACS+ Local Subscriber Feature" on page 57.

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 AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA Command Mode.)
3. Use the `tacacs+ primary authentication server address` command to specify the IP address of the TACACS+ primary authentication server; for example:

   ```
   AAA: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:

   ```
   AAA: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:

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

   NOTE: The LX listens to port 49 by default.

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

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

   Refer to Table 1 on page 50 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 58
- "TACACS+ Secondary Authentication Server Commands" on page 58
- "TACACS+ Secondary Accounting Server Commands" on page 58

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+ Local Subscriber Feature

Under the TACACS+ Local Subscriber Feature, a subscriber can be logged on in one of two ways:

- As an LX subscriber with the attributes of that subscriber (if the LX subscriber account exists)
- Or, if the LX subscriber account does *not* exist, as the default (InReach) subscriber.

Under either scenario, the subscriber must have a TACACS+ account on the TACACS+ server. If the subscriber account also exists on the LX unit, the subscriber is logged on under that account and with the attributes of that account. If the subscriber account does *not* exist on the LX unit, the subscriber is logged on under his TACACS+ account with the attributes of the default (InReach) account.

Use the `tacacs+ local subscriber enable` command to configure the TACACS+ Local Subscriber Feature for the LX unit; for example:

```
AAA:0 >>tacacs+ local subscriber enable
```

When the TACACS+ Local Subscriber Feature is set to `only`, the subscriber can only be logged in if the subscriber account is configured on both the LX unit and the TACACS+ server *and* the subscriber account on the LX server has the same name as the subscriber account on the TACACS+ server.

Use the `tacacs+ local subscriber only` command to set the TACACS+ Local Subscriber Feature to `only`; for example:

```
AAA:0 >>tacacs+ local subscriber only
```

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

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

TACACS+ Primary Accounting Server Commands

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

TACACS+ Secondary Authentication Server Commands

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

TACACS+ Secondary Accounting Server Commands

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

```
AAA: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 AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA Command Mode.)
2. Use the `tacacs+ period` command to specify the TACACS+ period; for example:

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

Setting Up SecurID

NOTE: PPP CHAP is not supported with authentication 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 54).
2. Specifying the SecurID server settings on the LX (see page 55).

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

You also have the option of configuring a SecurID Local Subscriber. For more information, refer to "SecurID Local Subscriber Feature" on page 63.

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 AAA Command Mode on the LX. (Refer to page 27 for information on accessing the AAA 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:

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

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

   ```
   AAA: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:

   ```
   AAA: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:

```
AAA:0 >>securid authentication encryption des
AAA:0 >>securid authentication encryption sdi
```

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

```
AAA: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.

```
AAA:0 >>securid primary authentication server address 138.30.65.34
AAA:0 >>securid authentication port 4500
AAA:0 >>securid primary authentication server name bigsky1.com
AAA:0 >>securid authentication encryption des
AAA:0 >>securid authentication retransmit 7
AAA:0 >>securid authentication timeout 3
AAA: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*.

SecurID Local Subscriber Feature

Under the SecurID Local Subscriber Feature, a subscriber can be logged on in one of two ways:

- As an LX subscriber with the attributes of that subscriber (if the LX subscriber account exists)
- Or, if the LX subscriber account does *not* exist, as the default (InReach) subscriber.

Under either scenario, the subscriber must have a SecurID account on the SecurID server. If the subscriber account also exists on the LX unit, the subscriber is logged on under that account and with the attributes of that account. If the subscriber account does *not* exist on the LX unit, the subscriber is logged on under his SecurID account with the attributes of the default (InReach) account.

Use the `securid local subscriber enable` command to configure the SecurID Local Subscriber Feature for the LX unit; for example:

```
AAA:0 >>securid local subscriber enable
```

When the SecurID Local Subscriber Feature is set to `only`, the subscriber can only be logged in if the subscriber account is configured on both the LX unit and the SecurID server *and* the subscriber account on the LX server has the same name as the subscriber account on the SecurID server.

Use the `securid local subscriber only` command to set the SecurID Local Subscriber Feature to `only`; for example:

```
AAA:0 >>securid local subscriber only
```

SecurID sdconf.rec File

The LX software now supports the **`sdconf.rec`** file (the configuration file created by the SecurID Host installation program, which holds the Primary and Replica host addresses). The `sdconf.rec` file is read the first time SecurID is attempted. If the Primary host address is unreachable, the Replica address is tried. To use the `sdconf.rec` file, download it into the LX `/config` directory. If this file is present on the LX, the SecurID system characteristics from the `sdconf.rec` file will be used, and configuration of the SecurID attributes will be blocked at the CLI command level.

To download the `sdconf.rec` file:

1. Go to the shell.
2. Change to the directory `cd /config` directory.
3. From `/config`, perform an FTP and retrieve the `sdconf.rec` file.

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 its factory defaults. This may be done in one of several ways:

From an LX asynchronous port:

1. Access the Configuration Command Mode. (Refer to page 26 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.

   After you select Option `[1]` and the reset is complete, the changes are saved to Flash.

5. Select `[2]` to reset the Linux system configuration. This 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 102 for further information on defaulting from ppciboot and defaulting from the CLI.

Syslog Overview

The local Syslog size is set to 64K by default and can be increased to a maximum size of 128K. When a remote Syslog is configured it receives the same information as the local syslog. The local syslog wraps when it reaches its maximum size.

When the syslog reaches its maximum size, it is automatically saved as a gzip file to compress the syslog file and save space. For example, a syslog file named `/var/log/syslog` of 64K would be saved as `var/log/syslog.gz` of perhaps 10K. Once the latter file reaches 64K, it too is saved, as, for example, `var/log/syslog.old.gz` of perhaps 20K. Once the compressed file totals 64K in size and can be compressed no more, the oldest data in the file will be dropped to provide space.

Command logging is another useful tool. It is an attribute of the subscriber and is disabled by default. When enabled, all commands entered by the user are also written to syslog. The command log CLI commands act like a filter to screen the specific users commands from the syslog.

For more information on the Command Logging Feature, refer to the `command log enable` command and the `monitor/show command log` command in the *LX-Series Commands Reference Guide*.

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 69).
- Setting up security for the LX asynchronous port to which the network element is connected (see page 73).
- Creating the subscriber(s) that have remote access to the asynchronous port where the Network Element is connected (see page 76).

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 68.

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).

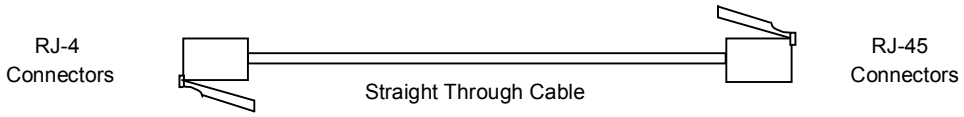


Figure 2 - Straight-through Wiring Scheme

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 page 27 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	stopbits 1 stopbits 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 page 27 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 `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`

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

   Modem 5-5:0 >>`initstring S0=1 V1 X4 E1 Q0=1 \J0 &K3`

   NOTE: The initialization string may vary between modem types.

9. 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`

10. 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`

Configuring Modems for the RAS Dial Feature

A subscriber can use the RAS Dial Feature to make a console connection to an LX unit. (For more information on the RAS Dial Feature, refer to the `dial direct` command in the *LX-Series Configuration Guide*.)

The RAS Dial Feature uses a Modem Pool to make direct dial connections. (For more information on Modem Pools, refer to the `pool enable` command in the *LX-Series Configuration Guide*.) In order to support the RAS Dial Feature, each modem in the Modem Pool must have an initialization string that is equivalent to the following:

Answer mode	S0=1
Result word	V1
Extended Results	X4
Echo ON	E1
Result code ON	Q0=1
Mode Buffer	\J0
RTS Flow control	&K3

NOTE: The symbols in the initialization string may be different for your type of modem. Refer to your modem manual for the correct symbols for your modem. Step 8 (above) provides an example of an `initstring` command that configures a modem string to support the RAS Dial Feature.

Setting Up Security for a Console Port

You can use LOCAL authentication, LDAP 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, LDAP, 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 page 27 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 48 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 page 27 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 75.

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 53 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 page 27 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.

Setting Up SecurID Authentication

NOTE: PPP CHAP is not supported with authentication Securid.

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 59 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 page 27 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., LDAP, 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 LDAP, 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.

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

NOTE: When using SSH and Fallback, make sure your SSH client is configured to send a minimum of four Password prompts (refer to your SSH client documentation). You may also need to increase the `LoginGraceTime` on the LX. To increase the `LoginGraceTime`, go to the shell, change the directory to `/config`, and edit the `sshd_config` file.

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 page 27 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

NOTE: The administrator must configure the first password for a new subscriber in order for that subscriber account to be active.

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 page 28 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 78.
3. Execute the `access console enable` command to specify that the subscriber will have console access to the LX unit; for example:

   Subs_mark:0 >>`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:0 >>`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:0 >>`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:0 >>`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:0 >>`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:0 >>`telnet mode character`

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

   Subs_mark:0 >>`telnet mode line`

Specifying SSH As an Access Method

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

   Subs_mark:0 >>`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:0 >>`ssh cipher triple-des`

   Subs_mark:0 >>`ssh cipher any`

   Subs_mark:0 >>`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:0 >>`access web enable`

Connect Port Escape Character

You can configure an escape character in the local subscriber database. The default value is ^Z.

To configure an escape character:

1. Change the escape sequence; for example:

   Subs_Tom:0 >>`connect escape ^<`*`character`*`>`

   where <*`character`*> is a character from A-Z.

2. To set the escape character back to the default value:

   Subs_Tom:0 >>`default connect escape`

3. For example, the connect command will establish a connection to the specified remote port. To break the connection, execute the connect escape character:

   InReach:0 >>`connect port async 1`

   Remote_device: ^Z

   InReach>>

Use the `show subscriber <subscriber_name> characteristic` command to display the Subscriber Characteristics Screen. The `Connect Escape Char` field displays the escape character. An example of this screen follows, with the `Connect Escape Char` field highlighted:

```
Subscriber Name:              InReach  Rlogin Ded. Service
Preferred Service:                     Dedicated Service
Security:      User Read Outlet Shell  User Password:             Configure
Login Mode  :                     Cli  Change User Password:        Disable
Maximum Connections:               50  Maximum Sessions:                4
Command Logging:              Disabled  Audit Logging  :            Disabled
Idle Timeout:                      0    User Prompt:                  InReach
Web Login Mode:                Config   Screen Pause:                  Enable
Forward Switch:                    ^F   Local Switch:                      ^L
Backward Switch:                   ^B   Rlogin Transparent:          Disable
Connect Escape Char:               ^Z   Dialback Feature:            Disable
Dialback Number:
Menu Name:                                          /config/M_InReach
Web Menu Name:                                      /config/M_InReach
Port Access   list:                                            0-33
Remote Access list:                          Telnet Ssh Web_Server Console
Outlet Access list:
Outlet Group Access list:
```

Figure 3 - Subscriber Characteristics Screen

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-1 hashing algorithm. The SHA-1 hashing algorithm 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 (e.g., 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 "Saving the Configuration File" on page 81. 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
   - LDAP, 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
- LDAP, 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

NOTE: You must define an LX address in the ppciboot menu before loading a saved configuration from a TFTP server. See "Changing the Unit IP Address" on page 99.

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
```

An enhancement to the System Status screen shows from where the LX loads its parameter file when the unit configuration is defaulted. The `Configuration Loaded From:` field displays the TFTP server source of the `.prm` file. The `Network Configuration File Name:` field displays the name of the `.prm` file.

Figure 4 shows an example of the System Status Screen.

```
Time:   Mon, 23 Jun 2003 20:17:20 UTC  System Uptime:               0 8:7:50
Software Loaded From               :                      Local Flash Memory
Active System Gateway              :                            102.19.169.1
Configuration Loaded From          :                            102.19.169.3
Network Configuration File Name    :                            lx000d6c.prm
Configuration File to Boot From    :                     /config/Config.prm
Configuration Settings to Boot From :                                  Flash
Configuration Status               :                    Configuration Saved
Configuration Version              :                                      4
Configuration Conversion Status    :             Converted to Version  310
Process Load Average:                  Memory usage (in KB):
1 min. Avg usage      :          0.00  Total Memory        :           62760
5 min. Avg usage      :          0.00  Cached Memory       :            6320
15 min. Avg usage     :          0.00  Free Memory         :           28488

Temperature Status (degrees Celsius):
Critical Temp.      :            60.0  Hysteresis Temp.    :             5.0
Low Temperature     :             0.0  Threshold Temp.     :            55.0
Current Temp.       :            38.5
```

Figure 4 - System Status Screen

Loading the Configuration from Network

Loads a previously saved (to network) configuration zip file into flash on an LX, so the LX can boot from the saved configuration from flash from this point forward.

1. To load the configuration from network, enter:

   Config:0 >>`load configuration from network <ip_address> <filename>`

   where <*ip_address*> specifies the IPv4 address of the TFTP server where the configuration zip file resides, and filename is the name of the configuration zip file without the ".zip" extension. The filename will be appended with a `.zip` suffix on the TFTP server when it is saved. For example, `local` and `local.zip` are valid filenames.

2. When this command is entered, you are prompted with two warnings:

   `"This will overwrite your current configuration. Are you sure? y/n"`

3. If you enter `y`, the LX will TFTP get the configuration file and write it into memory, and the following message appears. If you enter `n`, the command aborts without changing the configuration in flash, and issues the message "`Operation aborted`".

   `"You must reboot for the new configuration to take effect. Reboot now? y/n"`

4. If you enter `y`, the LX reboots, loading the new configuration from flash upon reboot. If you enter `n`, the command ends and returns to the prompt. The new configuration is now written in flash, and upon the next reboot loads the new configuration.

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 82. 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.

NOTE: The `ppciboot.img.sign` and `linuxito.img.sign` digital signature files are used to authenticate load images. Place these files on the TFTP server if `Authenticate Image` is enabled (on the Show System Characteristics screen) or if you are running in the FIPS mode of operation so the LX unit can download them. This download occurs automatically. See "Enabling/Disabling FIPS Security" on page 95 for further information on FIPS.

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.

NOTE: Main Menu entry `[8] EM316LX Configuration` appears on the Main Menu only when you are managing an EM316LX.

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. Enter `L` and then the password. The Main Menu appears:

```
            Welcome to In-Reach ppciboot Version x.x
                      Main Menu
  [1] Boot from network:      Network, Flash
    [f] Save software image to flash when boot from network:no
  [2] Time Out, in seconds (0=disabled): 8
  [3] IP Configuration Menu
  [4] Update ppciboot Firmware
  [5] Ethernet Network Link
  [6] Change ppciboot Password
  [7] FIPS 140-2 Security:                                  yes
  [8] EM316LX Configuration
  [*] 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` repeatedly to toggle between `Network only`, `Flash only`, `Network, Flash`, or `Flash, Network` (FIPS mode only allows `Flash only`). The choices are defined as follows:

- `Network only` - The LX loads from Network only. If it is unsuccessful, you must choose another load method.
- `Flash only` - The LX loads from Flash only. If it is unsuccessful, you must choose another load method.
- `Network, Flash` - The LX attempts to load from the Network. If it is unsuccessful, it then automatically attempts to load from Flash.
- `Flash, Network` - The LX attempts to load from Flash. If it is unsuccessful, it then automatically attempts to load from the Network.

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 network 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 Image to Flash When Booting From the Network

The `Save image to flash when boot from network` option lets you save the software image from the network to flash when booting from the network. To save the software image to flash:

1. Press `f` to toggle between yes and no. To save the software image to flash when booting from the network, 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.

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 `2 (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" on page 98 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 `4 (Update ppciboot Firmware)`. The ppciboot firmware begins loading from the TFTP server.
2. If the firmware loads successfully (taking only a few seconds) the firmware is saved and the unit is reset. Enter L and then the password, and 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 `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 number `5 (Ethernet Network Link)` repeatedly to toggle between the following speed/duplex options (the default is `Auto`):
   - `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. Toggle to the option you want and **press S to save the configuration**.

Changing the ppciboot Password

NOTE: In FIPS Mode the password must be at least six characters long.

The `Change ppciboot Password` option lets you change the ppciboot password for the unit. To change the ppciboot password:

1. Press the number `6 (Change ppciboot Password)`. The following prompt is displayed:

   ```
   Enter your current ppciboot password:
   ```

   Enter the current ppciboot password at the above prompt. After you have entered the current ppciboot password, the following prompt is displayed:

   Enter your NEW password: :

2. Enter the new ppciboot password at the above prompt.

   After you have entered the new ppciboot password, the following prompt is displayed:

   Re-enter your NEW password:

Re-enter the new ppciboot password at the above prompt. A confirmation message is displayed.

Enabling/Disabling FIPS Security

NOTE: If you enable FIPS Security, option `[1] Boot from Network` is set to `Flash Only` automatically. You can only update from the CLI while FIPS is enabled. Option `[4] Update ppciboot Firmware` also does not work while FIPS is enabled.

The `FIPS 140-2 Security` option lets you enable or disable FIPS security. To enable or disable FIPS security:

1. Press the number `7 (FIPS 140-2 Security)`. The following prompt appears:

   ```
   Enabling FIPS security will reset run-time
   configuration to defaults. Are you sure? (y/n):
   ```

2. If you select `y` (this defaults the flash immediately), a `Resetting Linux Configuration` message appears, and the Main Menu reappears after a few seconds. If you select `n`, the Main Menu reappears immediately.

3. If FIPS is already enabled and you want to disable it, press `7 (FIPS 140-2 Security)` from the Main Menu.

EM316LX Configuration Menu

NOTE: Main Menu entry `[8] EM316LX Configuration` appears on the Main Menu only when you are managing an EM316LX.

The `EM316LX Configuration` Menu option lets you control and configure module settings. Refer to "Using the EM316LX Configuration Menu" on page 101 for details.

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)`. You are prompted for the password, which is `access.` The following options appear:

   ```
   [1] Reset ppciboot Configuration

   [2] Reset Linux System Configuration

   [3] Reset PPCiBoot and Linux configurations

   Warning: Options 1 and 3 will cause system reset in the end!!
   ```

2. Select `1, 2,` or `3`. If you select `[1] Reset ppciboot Configuration,` the command sets the ppciboot configuration to system defaults and saves the configuration to flash. If you select `[2] Reset Linux System Configuration,` the command erases all of the configurations you have saved, except for the ppciboot configuration. If you select `[3] Reset PPCiBoot and Linux configurations,` options `[1]` and `[2]` are performed.
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 102 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 `3` 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.

Using the EM316LX Configuration Menu

The `EM316LX Configuration` Menu option lets you control and configure module settings. To configure the EM316LX settings:

1. At the Main menu, enter `9` to open the EM316LX Configuration Setup-menu.

```
[0] Module Restart:                yes
[1] Management Enable:             yes
[2] External I2C Bus Enable        yes

[S] Save New 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.

Restarting the Module

The `Module Restart` option lets you reset the EM316LX module. To reset the EM316LX module, press `0 (Module Restart)`. Pressing `0` toggles between restart on and restart off, shown on the EM316LX Configuration Menu as `yes` or `no`.

Enabling the Management Port

The `Management Enable` option lets you enable the Management from the EM316NM management module. If this is disabled, the EM316NM management module can still monitor the status of the EM316LX, but not make changes. To enable management:

1. Press the number `1 (Management Enable)` to enable management. Pressing `1` toggles between Management enabled and Management disabled, shown on the EM316LX Configuration Menu as `yes` or `no`.

2. Press S to save the configuration. The EM316LX Configuration menu reappears. Press R to return to the Main Menu.

Disabling the External I2C Bus

The External I2C Bus Enable option lets you disconnect the EM316LX module from the External I2C management bus. In this case, the module will be invisible to the Management unit. To disable the External I2C Bus, press the number 2 (External I2C Bus Enable). Pressing 2 toggles between enabling and disabling the I2C Bus, shown on the EM316LX Configuration Menu as yes or no.The system automatically saves your new setting.

Saving the Configuration

The Saving New Configuration option lets you save the new EM316LX configuration. To save the configuration:

1. When you are finished configuring using the EM316LX Configuration menu, press S to save the configuration.
2. Press R to return to the Main Menu.

Booting from Defaults

When you boot a unit from defaults, it can take up to four minutes because the system must re-generate the SSH keys. The SSH 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 may take up to four minutes 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 `monitor/show interface 1 status` command displays the actual setting of the interface. The `monitor/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.

Changing the ppciboot Password via the CLI

To change the password from the CLI, enter, for example:

1. If you enter:

   Config:0 >>`default ppciboot password`

   The following message appears:

   ```
   Enter your CURRENT password:
   ```

2. Enter your current password. The **Config:0 >>** prompt appears.

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
`authpriv`	The Superuser authentication process.
`daemon`	A system daemon, such as `in.ftpd`.
`kern`	The Linux kernel.
`local0 - local7`	Remote syslog levels 0 through 7
`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
`info`	Normal, informational messages **Note:** You can not specify a facility characteristic of `all` with a priority characteristic of `info` for User Profiles that are based on a Service Profile of the TAP type.
`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.

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 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 108.

- 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 117.

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 108, 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, each specifying a different Short Message Service Center (SMSC). The LX unit supports a maximum of 20 Service Profiles.

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 110).
- **WEB** – Used to send event messages to pagers or cell phones via a Web Driver (see "Configuring WEB Service Profiles" on page 115).
- **TAP** – Used to send event text messages to pagers via TAP (see "Configuring TAP Service Profiles" on page 111).
- **SNMP** – Used to send event messages to SNMP trap clients (see "Creating Service Profiles" on page 108).
- **LOCALSYSLOG** – Used to send event messages to a local file on the LX unit (see "Configuring LOCALSYSLOG Service Profiles" on page 109).

- **REMOTESYSLOG** – Used to send event messages to syslogd on a remote host (see "Configuring REMOTESYSLOG Service Profiles" on page 114).
- **ASYNC** – Used to send event messages to outbound asynchronous ports on the LX unit (see "Configuring ASYNC Service Profiles" on page 113). Users can receive the event messages by connecting a terminal or a printer to the configured asynchronous port(s). 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 115).

Creating Service Profiles

To create a Service Profile, do the following:

1. Access the Notification Command Mode. (Refer to page 29 for information on accessing the Notification Command Mode.)
2. Use the `profile service` command to create a Service Profile. For example, the following command creates a Service Profile called `Skytel`:

   Notification:0 >>`profile service Skytel`

   When you execute the `profile service` command, the CLI enters the Service Profile command mode. In the Service Profile command mode, you can begin configuring the Service Profile. Refer to the following sections for more information.
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 109
   - "Configuring SNPP Service Profiles" on page 110
   - "Configuring TAP Service Profiles" on page 111
   - "Configuring ASYNC Service Profiles" on page 113

- "Configuring REMOTESYSLOG Service Profiles" on page 114
- "Configuring WEB Service Profiles" on page 115
- "Configuring SMTP Service Profiles" on page 115

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

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as LOCALSYSLOG:

```
Noti_Serv_Protocol:0 >>localsyslog
```

When you execute the `localsyslog` command, the CLI goes into the LOCALSYSLOG Protocol command mode. Execute the `file` command in the LOCALSYSLOG Protocol command mode, to specify the local file to which event messages will be sent; for example:

```
Noti_Serv_LSyslog:0 >>file ricklog
```

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/ricklog` 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 117.

Configuring SNPP Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as SNPP:

```
Noti_Serv_Protocol:0 >>snpp
```

When you execute the `snpp` command, the CLI goes into the SNPP Protocol command mode. To finish configuring the Service Profile, do the following:

1. Execute the `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:

   ```
   Noti_Serv_SNPP:0 >>server 118.28.118.34
   ```

   NOTE: If you specify a symbolic name (e.g., `snpp.Skytel.com`) as the SNPP server, you must have a primary DNS server, a domain name suffix, and a Network Time Server 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 `port` command to specify the LX TCP port that will be used to send messages to the SNPP server; for example:

   ```
   Noti_Serv_SNPP:0 >>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 117.

Configuring TAP Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as TAP:

```
Noti_Serv_Protocol:0 >>tap
```

When you execute the `tap` command, the CLI goes into the TAP Protocol Command mode. To finish configuring the Service Profile, do the following:

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

   ```
   Noti_Serv_TAP:0 >>smsc 18668230501
   ```

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

   ```
   Noti_Serv_TAP:0 >>parity even
   ```

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

   ```
   Noti_Serv_TAP:0 >>bits 7
   ```

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

   ```
   Noti_Serv_TAP:0 >>stopbits 2
   ```

   NOTE: The bits-per-byte setting, and the stop bits setting, that you specify for a Service Profile, must match the corresponding settings of the modem port(s) that you specify in the next command.

5. Use the `modem port` command to specify the modem port(s) that syslog can dial out to send a message with this Service Profile; for example:

   ```
   Noti_Serv_TAP:0 >>modem port 2 3 5 6
   ```

For an internal modem, the default configuration is usually sufficient to support a TAP Service Profile. However, the following guidelines are recommended for external modems:

- **All External Modems:**

  S0=1 – Autoanswer on one ring.

  V1 – Displays result codes as words – The modem code looks for word responses, not numbered responses.

  X4 – Extended result codes – The modem code looks for word responses that the extended result codes provide.

  &B1 – Makes the modem use the speed of the LX port. The TAP sites can have all different speed modems. This setting ensures that at least your port and the attached modem are always in sync.

- **US Robotics Sportster and Faxmodem modems:**

  - The port needs CTS flow control.
  - The port speed should be set to a speed that the modem supports.
  - The initstring should be `^MAT S0=1 V1 X4 &H1 &B1^M`, where:

    `S0=1` – Autoanswer on one ring.

    `V1` – Display result codes as words

    `X4` – Extended result codes

    `&H1` – Hardware Flow Control

    `&B1` – Makes the modem use the speed of the LX port.
  - Dipswitches 3,7, and 8 need to be in the "down" position per the US Robotics website:

    http://www.usr.com/support/docs-template.asp?prod=s-modem

- **US Robotics Courier V. Everything modem:**

  - The port needs CTS flow control.
  - The port speed should be set to a speed that the modem supports.

- The initstring should be `^MAT S0=1 V1 X4 &K0 &B1^M`, where:

  `S0=1` – Autoanswer on one ring

  `V1` – Display result codes as words

  `X4` – Extended result codes

  `&K0` – No data compression

  `&B1` – Makes the modem use the speed of the LX port.

- Dipswitches 3, 8, and 10 need to be in the "down" position per the US Robotics website:

  http://www.usr.com/support/docs-template.asp?prod=s-modem

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 117.

Configuring ASYNC Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as Async:

```
Noti_Serv_Protocol:0 >>async
```

When you execute the `async` command, the CLI goes into the ASYNC Protocol command mode. Execute the `port` command in the ASYNC Protocol command mode, to specify the asynchronous port(s) to which event messages will be sent; for example:

```
Noti_Serv_Async:0 >>port 2 3 4 5
```

You can create User Profiles to filter, by facility and priority, the event messages that will be sent to the asynchronous ports. For more information, refer to "Creating a User Profile" on page 117.

Configuring REMOTESYSLOG Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as REMOTESYSLOG:

```
Noti_Serv_Protocol:0 >>remotesyslog
```

When you execute the `remotesyslog` command, the CLI goes into the REMOTESYSLOG Protocol command mode. Execute the `host` command to specify the remote UNIX host to which event messages will be sent; for example:

```
Noti_Serv_RSyslog:0 >>host 10.179.170.253
```

Do the following on the UNIX host that you specify in the `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 117.

Configuring SMTP Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as SMTP:

```
Noti_Serv_Protocol:0 >>smtp
```

When you execute the `smtp` command, the CLI goes into the SMTP Protocol command mode. Execute the `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 service provider's server can be specified as an IP Address or as any symbolic name that can be resolved by DNS; for example:

```
Noti_Serv_SMTP:0 >>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 117.

Configuring WEB Service Profiles

The CLI enters the Service Profile command mode when you execute the `profile service` command. Execute the following command, in the Service Profile command mode, to configure a Service Profile as WEB:

```
Noti_Serv_Protocol:0 >>web
```

When you execute the `web` command, the CLI goes into the WEB Protocol command mode. Execute the `driver` command in the WEB Protocol command mode, to specify the web driver that will be used to send the event messages to the pager or cell phone; for example:

```
Noti_Serv_WEB:0 >>driver att_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*. (You can also configure a Network Time Server to get a date and time during a reboot of the LX unit.)

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 117.

Displaying the Characteristics of Service Profiles

Use the `monitor/show notification profile service` command to display the characteristics of Service Profiles; for example:

```
Notification:0 >>show notification profile service 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:

```
Notification:0 >>show notification profile service all
```

Figure 5 shows an example of the Service Profile Screen.

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

ServiceProfile: messages Protocol: localsyslog
File: messages

ServiceProfile: jackremote Protocol: remotesyslog
Remote Host:
```

Figure 5 - Service Profile Screen

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 page 29 for information on accessing the Notification Command Mode.)
2. Use the `profile user` command to create a User Profile; for example:

   Notification:0 >>`profile user adminscell`

   NOTE: Refer to "Restrictions in User Profile Names" on page 118 for restrictions on the user of Special Characters and Reserved Words in User Profile names.
3. When you execute the `profile user` command, the CLI enters the User Service command mode. In the User Service command mode, execute the `service` command to specify an existing Service Profile for the current User Profile; for example:

   Noti_User_Service:0 >>`service Center10`

   When you execute the `service` command, the CLI enters the User Information command mode.
4. If the User Profile is for a Service Profile of the SNPP, SMTP, TAP, or WEB type, you must use the `contact` command to specify the contact field for the User Profile; for example:

   Noti_User_Info:0 >>`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., `jsmith@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.

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

   Noti_User_Info:0 >>`priority warning`

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

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

   Noti_User_Info:0 >>`facility user`

   Event messages that originate from the specified facility, and have the specified priority (see step 5), will be sent to the destination. The allowable values for the facility characteristic are authpriv, daemon, kern, syslog, user, local0, local1, local2, local3, local4, local5, local6, and local7.

Restrictions in User Profile Names

The following characters can not be included in a User Profile name that will be associated with a Service Profile of the SMTP, TAP, WEB, or SNPP type:

- (– open parentheses
-) – close parentheses
- { – open bracket

- `}` – close bracket
- `,` – comma
- `.` – period
- `;` – semicolon
- `:` – colon
- `@` – at sign

The following text strings can be included in a User Profile name that will be associated with a Service Profile of the SMTP, TAP, WEB, or SNPP type. However, such a User profile can not *begin* with the following text strings:

- `true` (case-insensitive) – For example, the name `TrueBillJones` is unacceptable; the name `BillJonesTrue` is acceptable.
- `false` (case-insensitive) – For example, the name `falseBillJones` is unacceptable; the name `BillJonesfalse` is acceptable.
- `no` (case-insensitive) – For example, the name `NObillJones` is unacceptable; the name `BillJonesNo` is acceptable.
- `yes` (case-insensitive) – For example, the name `YesBillJones` is unacceptable; the name `BilljonesYES` is acceptable.

Displaying Characteristics of User Profiles

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

Notification:0 >>`show notification profile user grogers`

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

Notification:0 >>`show notification profile user all`

Figure 6 shows an example of the User Profile Screen.

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

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

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

UserProfile: jacklocal ServiceProfile: jacklocal
Contact:
Facility: user Priority: warning
```

Figure 6 - User Profile Screen

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.

syslogd Message Configuration Example

This example shows how to change the text field, facility, and priority of a configurable syslogd message.

Prerequisites

There are no prerequisites for this task.

Procedure

1. Access the Notification Command Mode of the LX CLI.

```
Login: InReach
Password: access
InReach:0>enable
```

```
Password>> system
InReach:0 >>config
Config:0 >>notification
Notification:0 >>
```

2. Change the text field of the message:

   Notification:0 >>`message 1 string New CLI mode entered by`

3. Change the priority setting of the message:

   Notification:0 >>`message 1 priority notice`

4. Change the facility setting of the message:

   Notification:0 >>`message 1 facility daemon`

Outbound Asynchronous Port Example

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

Notification:0 >>`profile service 3serialport`
Noti_Serv_Protocol:0 >>`async`
Noti_Serv_Async:0 >>`port 5 6 7`
Noti_Serv_Async:0 >>`exit`
Notification:0 >>`profile user serialport`
Noti_User_Service:0 >>`service 3serialport`
Noti_User_Info:0 >>`facility user`
Noti_User_Info:0 >>`priority warning`

Localsyslog Example

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

Notification:0 >>`profile service local`
Noti_Serv_Protocol:0 >>`localsyslog`
Noti_Serv_LSyslog:0 >>`file Build5`
Noti_Serv_LSyslog:0 >>`exit`
Notification:0 >>`profile user locallog`

```
Noti_User_Service:0 >>service local
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>priority warning
```

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

Remotesyslog Example

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

```
Notification:0 >>profile service Rlogvenus
Noti_Serv_Protocol:0 >>remotesyslog
Noti_Serv_RSyslog:0 >>host 10.179.170.253
Noti_Serv_RSyslog:0 >>exit
Notification:0 >>profile user venus
Noti_User_Service:0 >>service Rlogvenus
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>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 >>profile service Skytel
Noti_Serv_Protocol:0 >>snpp
Noti_Serv_SNPP:0 >>server snpp.Skytel.com
Noti_Serv_SNPP:0 >>port 7777
Noti_Serv_SNPP:0 >>exit
Notification:0 >>profile user johnpager
Noti_User_Service:0 >>service Skytel
Noti_User_Info:0 >>contact 8875551212
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>priority warning

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

Email Example

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

Notification:0 >>profile service youremail
Noti_Serv_Protocol:0 >>smtp
Noti_Serv_SMTP:0 >>server 10.10.10.21
Noti_Serv_SMTP:0 >>exit
Noti_Serv_SMTP:0>>name john
Noti_Serv_SMTP:0>>subject Lab2 Floor5 lx11
Notification:0 >>profile user jsmith
Noti_User_Service:0 >>service youremail
Noti_User_Info:0 >>contact 785551111@vtext.com (verizon text phone)
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>priority warning

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

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 >>`profile service verizon`
Noti_Serv_Protocol:0 >>`tap`
Noti_Serv_TAP:0 >>`smsc 18668230501`
(provider's service phone #)
Noti_Serv_TAP:0 >>`bits 7`
Noti_Serv_TAP:0 >>`stopbit 1`
Noti_Serv_TAP:0 >>`parity even`
Noti_Serv_TAP:0 >>`modem port 6`
Noti_Serv_TAP:0 >>`exit`
Notification:0 >>`profile user jmscell`
Noti_User_Service:0 >>`service verizon`
Noti_User_Info:0 >>`contact 785551212`
Noti_User_Info:0 >>`facility user`
Noti_User_Info:0 >>`priority warning`
Noti_User_Info:0 >>`exit`
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`

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	Not Available	@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 >>profile service ricksnmp
Noti_Serv_Protocol:0 >>snmp
Noti_Serv_Protocol:0 >>exit
Notification:0 >>profile user ricksnmp
Noti_User_Service:0 >>service ricksnmp
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>priority warning
```

Web Example

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

```
Notification:0 >>profile service cingular
Noti_Serv_Protocol:0 >>web
Noti_Serv_WEB:0 >>driver cingular_web
Noti_Serv_WEB:0 >>exit
Notification:0 >>profile user kevin
Noti_User_Service:0 >>service cingular
Noti_User_Info:0 >>contact 9785551313
Noti_User_Info:0 >>facility user
Noti_User_Info:0 >>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. (You can also configure a Network Time Server to get a date and time during a reboot of the LX unit.) The supported web drivers can be retrieved from the CLI help.

Chapter 5

Configuring IP Interfaces

NOTE: Refer to "Configuring PPP" on page 321 for information on configuring IP interfaces for PPP.

An IP interface is a logical interface for accessing the LX unit from a network. The maximum number of IP interfaces on an LX unit is **the number of serial ports on the LX unit, plus 2.** For example, the maximum number of IP interfaces on an 8-port unit is 11 or 12 (if the unit has a modem port); the maximum number of IP interfaces on a 16-port unit is 20, and so on.

On LX-8000 units, the maximum number of IP interfaces is **the number of serial ports on the LX unit, multiplied by the number of Ethernet ports (2), plus 2**. For example, the maximum number of IP interfaces on a 40-port unit is 82 ((40 x 2) + 2 = 82).

Each IP interface can have its own IP characteristics. You can access an LX unit via the Address of the IP interface as an alternative to 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 137.

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 155 for more information.

It is possible for a subscriber with superuser privileges to log into the interface using SSH. The client SSH command line can include an LX CLI command. Once the SSH session is established, the CLI command is performed. The return from that screen is sent to the user and the session is then terminated. This capability is not supported by all SSH applications. The syntax follows:

```
ssh -l <username> <lx_ip_address> -p 22 <cli_command>
```

For example:

```
ssh -l InReach 1.2.3.4 -p 22 show users
```

You can authenticate connections via IP interfaces with the same authentication methods that are configured for the LX unit (LOCAL, LDAP, 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 133 and "Configuring Server-Based Authentication on an IP Interface" on page 134.)

Ports can be configured as Master Ports, or Slave Ports, in a Broadcast Group associated with an IP interface. The Slave Ports can receive data from, and send data broadcasts to, the Master Ports in the Broadcast Group. for more information, refer to "Configuring the Data Broadcast Feature" on page 145.

By default, an IP interface is bound to the physical Ethernet interface (Eth0) on the LX unit. For more information, refer to the Interface Commands in the *LX-Series Commands Reference Guide*.

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`

If you do not specify an explicit IP address, you can configure the IP address to re-use the IP address of another interface. Otherwise, the interface will default to using the First Available IP address. Refer to "Re-Using IP Addresses" on page 130 for more information.

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, LDAP, 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 133
   - "Configuring Server-Based Authentication on an IP Interface" on page 134

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

   - "Specifying SSH Keepalive Parameters" on page 131
   - "Specifying Socket Numbers" on page 131
   - "Specifying Maximum Transmission Units (MTU)" on page 133

Re-Using IP Addresses

Unless you configure an IP address, with the `address` command, the IP interface will obtain its IP address from the First Available interface or from the interface that you specify in the `unnumbered interface` command.

In the following example, the `unnumbered interface` command specifies that Interface 4 will use the IP address of Interface 3:

Intf 4-4:0 >>`unnumbered interface 3`

If you do not execute the `unnumbered interface` command, or the `address` command, the interface re-uses the First Available IP address.

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

LX Serial Port	Default Telnet Port	Default SSH Port
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 telnet 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 Server-Based Authentication on an IP Interface

Server-based authentication methods (i.e., LDAP, 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 Server-Based Authentication and Accounting" on page 43 and the `authentication enable` commands in the *LX-Series Commands Reference Guide*.

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

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

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 377.

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 48.

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 377.

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., LDAP, 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 LDAP, 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.

LDAP, RADIUS, TACACS+, or SecurID must be enabled on an IP interface in order for Fallback to function on the interface. (Refer to "Configuring Server-Based Authentication on an IP Interface" on page 134 for information on enabling LDAP, RADIUS, TACACS+, or SecurID.) When all four methods (i.e., LDAP, RADIUS, TACACS+, or SecurID) are disabled on the interface, Fallback is ignored by the interface.

NOTE: Enable Fallback is not supported when used in conjunction with inbound PPP CHAP.

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. A rotary can be configured on an IP interface, with LX ports as the multiple destinations of the rotary. A user can attempt to connect to an IP interface that has a rotary configured on it. 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.

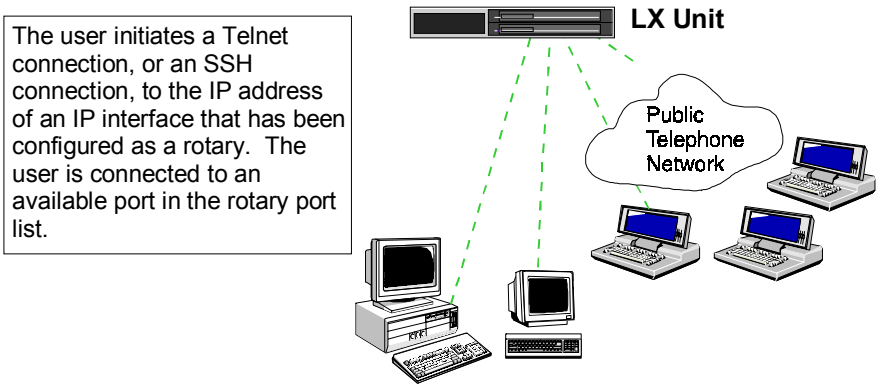


Figure 7 - Rotary Connections on an IP Interface

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 a rotary on an IP interface:

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 port` command to create a rotary, and to assign LX asynchronous ports to the rotary; for example:

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

   In the above example, Rotary `1` is created and the LX asynchronous ports `1`, `2`, and `3` are assigned to it. (You can execute the `rotary port` command on an existing rotary to add asynchronous ports to it.)

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

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

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

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

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

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

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

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

Removing Ports from a Rotary

To remove ports from a rotary, execute the `rotary port` command in the Interface Command Mode; for example:

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

In the above example, ports 2 and 3 are removed from Rotary `1`.

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

In the above example, port 3 is removed from Rotary `1`.

To verify that asynchronous ports have been removed from a rotary, execute the `monitor/show interface rotary` command. If the asynchronous ports have in fact been removed, they will not appear in the "Serial Ports" column of the screen. For more information on the `monitor/show interface rotary` command, refer to "Displaying Rotary Information" on page 143.

Disabling Rotaries

Execute the `no rotary` command in the Interface Command Mode to disable a rotary; for example, the following command disables Rotary `1`:

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

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 `monitor/show interface rotary` command. If the rotary is in fact disabled, it will say "Disabled" in the "Rotary State" column of the screen. For more information on the `monitor/show interface rotary` command, refer to "Displaying Rotary Information" on page 143.

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 `monitor/show interface characteristics` command to display the characteristics of an IP interface; for example:

```
Intf 1-1:0 >>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:

```
Intf 1-1:0 >>show interface all characteristics
```

Figure 8 shows an example of the Interface Characteristics Screen.

```
Time:                                  Wed, 05 Jan 2005 11:40:11 US/EASTERN
Interface Name:           Interface_1  Bound to :                      eth0:1
IP MTU Size:                      N/A  Unnumbered Interface: First Available
IP Address   :                0.0.0.0  Learned IP Address  : 140.179.169.191
IP Mask      :                0.0.0.0  Learned IP Mask     :   255.255.255.0
IP Broadcast :                0.0.0.0  Learned IP Broadcast: 140.179.169.255
Interface Status:              In Use  Learned IP Gateway  :   140.179.169.1
Banner Display:                 Local  Learned IP DNS      :         0.0.0.0
Banner:        /config/banner.default  Radius Accounting:           Disabled
Authentication:                   None  Tacacs+ Accounting:          Disabled
Authentication FallBack:     Disabled  Auth. FallBack Attempts:            0
SSH port:                          22  Telnet port:                       23
```

Figure 8 - Interface Characteristics Screen

Displaying Interface Port Mapping

Use the `monitor/show interface port mapping` command to display the Telnet Socket Number, and the SSH Socket Number, associated with each serial port on the LX unit; for example:

Intf 1-1:0 >>`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:

Intf 1-1:0 >>`show interface all port mapping`

Figure 9 shows an example of the Interface Port Mapping Screen for a 20-port unit.

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
9	2900	2922
10	3000	3022
11	3100	3122
12	3200	3222
13	3300	3322
14	3400	3422
15	3500	3522
16	3600	3622
17	3700	3722
18	3800	3822
19	3900	3922
20	4000	4022

Figure 9 - Interface Port Mapping Screen

Displaying Interface Statuses

Use the `monitor/show interface status` command to display the status information for IP interfaces; for example:

Intf 1-1:0 >>`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:

Intf 1-1:0 >>`show interface all status`

Figure 10 shows an example of the Interface Status Screen.

```
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 Screen

Displaying Interface Summaries

Use the `monitor/show interface summary` command to display summary information for all of the IP interfaces on the LX unit; for example:

Intf 1-1:0 >>`show interface summary`

Figure 11 shows an example of the Interface Summary Screen.

```
         Name           Address         Broadcast        Addr. Mask   Bound to
  Interface_1  *157.145.162.155   157.145.162.255    *255.255.255.0       eth0
  Interface_2           0.0.0.0           0.0.0.0           0.0.0.0      eth0:1
  Interface_3           0.0.0.0           0.0.0.0           0.0.0.0      eth0:2
  Interface_4           0.0.0.0           0.0.0.0           0.0.0.0      eth0:3
'*' before the value denote it was learned from ppciboot
```

Figure 11 - Interface Summary Screen

Displaying Rotary Information

NOTE: There can be up to four rotaries on an interface.

Use the `monitor/show interface rotary` command to display information on rotaries; for example:

Intf 1-1:0 >>`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:

Intf 1-1:0 >>`show interface all rotary`

Figure 12 shows an example of the Rotary Characteristics Screen.

```
Rotary IP Address    TCP    SSH       Rotary Type   Rotary State  Serial Ports
  147.132.145.16    1500   1522     First Available     Disabled
```

Figure 12 - Rotary Characteristics Screen

Chapter 6

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 IP interface. 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 page 26.)
2. Execute the `interface` command to enter the Interface command mode for an IP interface; for example:

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

3. Use the `broadcast group` command to create a Broadcast Group; for example:

   Intf 1-1:0 >>`broadcast group 4`

   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.

4. 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.

5. 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.

6. 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`.

7. Use the `exit` command to return to the Interface Command Mode; for example:

   BrGroups 4:0 >>`exit`

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

   Intf 1-1:0 >>`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.
- A maximum of 5 Broadcast Groups per interface is allowed. If more than 5 broadcast groups are required, you must create additional interfaces.

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 `monitor/show interface broadcast group characteristics` command. (The deleted ports will not be listed in the Broadcast Group Characteristics Screen.) For more information on the `monitor/show interface broadcast group characteristics` command, refer to "Displaying Broadcast Group Characteristics" on page 150.

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 Interface Command Mode; for example:

```
Intf 1-1:0 >>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 `monitor/show interface broadcast group characteristics` command to display the characteristics of Broadcast Groups; for example:

```
BrGroups 4:0 >>show interface 1 broadcast group 4
characteristics
```

In the above example, the Broadcast Group characteristics are displayed for Broadcast Group 4. Use the following syntax to display the Broadcast Group characteristics of *all* Broadcast Groups on the LX unit:

```
BrGroups 4:0 >>show interface 1 broadcast group all
characteristics
```

Figure 13 shows an example of the Broadcast Group Characteristics Screen.

```
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 13 - Broadcast Group Characteristics Screen

Displaying Broadcast Group Summaries

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

BrGroups 4:0 >>`show interface 1 broadcast group summary`

Figure 14 shows an example of the Broadcast Group Summary Screen.

```
Interface number 1
    Broadcast group number:                    State:

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

Figure 14 - Broadcast Group Summary Screen

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

NOTE: The administrator must configure the first password for a new subscriber in order for that subscriber account to be active.

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:0 >>**) 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`.

NOTE: When you create a new subscriber with the `copy subscriber` command, all subscriber characteristics are copied over except the user password, user prompt, menu name, and web menu name.

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` unless you have created another superuser account.

Subscriber Account Settings

When you create a new subscriber account with the `subscriber` command, its account settings are 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 subscriber account:

- "Specifying the Subscriber Access Methods" on page 155
- "Setting Up the Session and Terminal Parameters" on page 162
- "Configuring the Subscriber Password" on page 165
- "Specifying a Preferred Service" on page 167
- "Specifying a Dedicated Service" on page 166
- "Enabling the Menu Feature" on page 168
- "Adding Superuser Privileges to a Subscriber Account" on page 166
- "Configuring the Subscriber Password" on page 165
- "Enabling Audit Logging" on page 168
- "Enabling Command Logging" on page 169

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 156)
- "Web Browser Access" (see page 158)

- "Console Access" (see page 159)
- "Outlet Access" (see page 159)
- "Outlet Group Access" (see page 160)

You can also provide subscribers with access via Dialback. For more information, refer to "Dialback Access" on page 161.

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:0 >>access telnet enable
   ```

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

   ```
   Subs_jack:0 >>telnet mode line
   Subs_jack:0 >>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 159 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:0 >>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:0 >>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:0 >>ssh cipher triple-des
Subs_jack:0 >>ssh cipher any
Subs_jack:0 >>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 159 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 158 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:0 >>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. The minimum length of an SSH key is 96 characters (768 bits). The maximum length of an SSH key is 1200 characters (9600 bits).

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:0 >>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 156 and "SSH Access" on page 156.

Refer to "Console Access" on page 159 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:0 >>access console enable
   ```

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

   ```
   Subs_jack:0 >>access port 2 4 6
   ```

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

Outlet Access

A subscriber must have access to specific outlets in order to manage those outlets from the LX unit.

To configure a subscriber account for outlet access, do the following:

1. Execute the `security level outlet` command to specify outlet management privileges for the subscriber; for example:

   ```
   Subs_jack:0 >>security level outlet
   ```

2. Execute the `outlet access` command to specify the outlets that the subscriber can manage; for example:

```
Subs_jack:0 >>access outlet 3:4 5:1 6:7-10
```

In the above example, the subscriber is given outlet management privileges to outlet `3:4`, outlet `5:1`, and outlets `6:7`, `6:8`, `6:9`, and `6:10`.

Outlet Group Access

A subscriber must have access to outlet groups in order to manage those outlet groups from the LX unit.

To configure a subscriber account for outlet group access, do the following:

1. Execute the `security level outlet` command to specify outlet management privileges for the subscriber; for example:

```
Subs_jack:0 >>security level outlet
```

2. Execute the `outlet access group` command to specify the outlet groups that the subscriber can manage; for example:

```
Subs_jack:0 >>access outlet group 2 6 12-14
```

In the above example, the subscriber is given outlet group management privileges to outlet group 2, outlet group 6, and outlet groups 12 through 14.

It is also possible to specify outlet group access for a named outlet group. In the following example, the subscriber is given outlet group management privileges to the outlet group `Testoutlets`:

```
Subs_jack:0 >>access outlet group name Testoutlets
```

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

   Subs_jack:0 >>`dialback number 19785551978`

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

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

   Subs_jack:0 >>`dialback enable`

When a subscriber is configured for Dialback, and the LX has a Modem Pool, the subscriber can establish a reverse dial connection from the LX CLI. (Under reverse dialing, the subscriber is logged in with his username and password to a Modem Pool so that the next available modem makes the call back to the subscriber.)

The `dial reverse` command is used to establish reverse dial connections from the LX CLI. The `dial reverse` command exists in the User Command Mode and in the Superuser Command Mode. (For more information, refer to the `dial reverse` command in the *LX-Series Commands Reference Guide*.)

To create a Modem Pool on the LX, do the following:

1. Access the Modem Command Mode for the modem ports that you want to add to the Modem Pool. (Refer to page 28 for information on accessing the Modem Command Mode.)
2. Execute the `pool enable` command to `enabled` for the modem ports that you want to add to the Modem Pool; for example:

   Modem 3-7:0 >>`pool enable`

   In the above example, Modem Ports 3 through 7 are added to the Modem Pool.

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:

- **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:0 >>`prompt mxxxx9`

  In the above example, the subscriber's default login prompt (e.g., `jack:0 >`) is changed to `mxxxx9:0 >`.

- **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:0 >>`terminal ansi`
  Subs_jack:0 >>`terminal vt100`

- **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:0 >>`pause enable`

- **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 the Subscriber session mode is `Menu`, the subscriber is logged into his or her menu. Use the `login mode` command to change the Subscriber session mode; for example:

  Subs_jack:0 >>`login mode cli`
  Subs_jack:0 >>`login mode shell`
  Subs_jack:0 >>`login mode menu`

  The default Subscriber session mode is `CLI`.

NOTE: When subscriber login mode is set to `menu`, you can use session-switching keys to move between sessions, up to the maximum number of sessions you configured. Each session displays the same menu configured via the `menu name` command. Refer to the "Subscriber Commands" chapter in the *LX-Series Commands Reference Guide* for details on the `menu name` command.

- **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:0 >>`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:0 >>`maxsubscriber 10`

- **Maximum Sessions** – You can configure 1 through 10 sessions for a subscriber. Use the `maxsessions` command to set the maximum sessions for the subscriber; for example:

  Subs_jack:0 >>`maxsessions 10`

- **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 164).

Setting Up the Session Switch Characters

The LX unit supports up to 10 sessions per subscriber. (Refer to "Setting Up the Session and Terminal Parameters" on page 162 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:0 >>`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:0 >>`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:0 >>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

NOTE: The administrator must configure the first password for a new subscriber. New subscribers can no longer assign their own first password. The new subscriber may subsequently change the password created by the administrator.

The default password for the LX InReach 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:0 >>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 32 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:0 >>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 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:0 >>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 155 to enable Telnet for a subscriber.

Use the `dedicated service` command to specify a dedicated service for the subscriber; for example:

```
Subs_jack:0 >>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:0 >>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 155 to enable Telnet for a subscriber.

Specifying a Security Level

The Security Level specifies the privileges that the subscriber has on the LX unit. The highest security level is "superuser". A subscriber with superuser privileges can execute all of the commands in the LX CLI.

By default, subscribers without superuser privileges can execute all of the commands in the User command mode, except for the `monitor/show commands`. When the "read" privilege level is specified for a subscriber account, the subscriber can use the `monitor/show commands`.

Privilege levels of "outlet" and "shell" can also be configured for non-superuser subscriber accounts. A subscriber with the outlet privilege level can manage outlets, or outlet groups, from the LX unit. A subscriber with the shell privilege level can access the Linux shell from the LX CLI.

Use the security level command to specify the security level for a subscriber account; for example:

```
Subs_jack:0 >>security level outlet
Subs_jack:0 >>security level read
Subs_jack:0 >>security level shell
Subs_jack:0 >>security level superuser
```

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:0 >>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 173.

Enabling the Menu Feature

A Subscriber Menu is a preconfigured menu that displays for a subscriber when he/she logs in to the LX unit. A menu is displayed when the subscriber logs into a physical port. In order for a menu to display for a subscriber, you must enable the Menu Feature and specify a menu for the subscriber.

Use the `menu name` command to specify a menu for the subscriber; for example:

```
Subs_jack:0 >>menu name financegroup
```

The above command specifies that the menu `financegroup` will be displayed for the subscriber `jack` when he logs into the LX unit.

Use the `menu enable` command to set the subscriber login mode to `menu`. Then once the user logs into the LX, the menu is displayed. If you do not enable the menu, the normal CLI prompt is displayed. When the menu name is configured, you can access the menu by entering the `menu` command at the CLI prompt.

Enable the Menu Feature for the subscriber; for example:

```
Subs_jack:0 >>menu enable
```

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:0 >>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 174.

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 `monitor/show subscriber characteristics` command to display subscriber characteristics; for example:

```
Subs_frank: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:

```
Subs_frank:0 >>show subscriber all characteristics
```

Figure 15 shows an example of the Subscriber Characteristics Screen.

```
Subscriber Name:              InReach  Rlogin Ded. Service
Preferred Service:                     Dedicated Service
Security:      User Read Outlet Shell  User Password:             Configure
Login Mode  :                     Cli  Change User Password:        Disable
Maximum Connections:               50  Maximum Sessions:                4
Command Logging:              Disabled  Audit Logging  :            Disabled
Idle Timeout:                      0  User Prompt:                  InReach
Web Login Mode:                Config  Screen Pause:                  Enable
Forward Switch:                    ^F  Local Switch:                     ^L
Backward Switch:                   ^B  Rlogin Transparent:          Disable
Connect Escape Char:               ^Z  Dialback Feature:            Disable
Dialback Number:
Menu Name:                                          /config/M_InReach
Web Menu Name:                                      /config/M_InReach
Port Access   list:                                            0-33
Remote Access list:                          Telnet Ssh Web_Server Console
Outlet Access list:
Outlet Group Access list:
```

Figure 15 - Subscriber Characteristics Screen

Refer to the `monitor/show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Characteristics Screen.

Displaying the Subscriber Status

Use the `monitor/show subscriber status` command to display the status information for a subscriber; for example:

Subs_jack:0 >>`show subscriber tim status`

In the above example, 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:

Subs_jack:0 >>`show subscriber all status`

Figure 16 shows an example of the Subscriber Status Screen.

```
Time:                              Mon, 23 May 2004  15:20:02 US/Eastern
Subs.name:          miller       Number of Connections:              2
Configured TermType:         Ansi
           Remote IP Address      Local Port    Protocol     Device
miller           0.0.0.0              41       Serial     /dev/ttyGN41
           Session 0   User
           Session 0   telnet 10.242.130.145
           Session 0   Superuser
           Session 0   telnet 10.242.130.150
miller          10.242.130.106         5040     Web Server    Tcp/23840
           Session 0   Superuser
```

Figure 16 - Subscriber Status Screen

Refer to the `monitor/show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Status Screen.

Displaying the Subscriber TCP Information

Use the `monitor/show subscriber tcp` command to display the subscriber TCP information; for example:

Subs_jack:0 >>`show subscriber tim tcp`

In the above example, 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:

Subs_jack:0 >>`show subscriber all tcp`

Figure 17 shows an example of the Subscriber TCP Screen.

```
Time:                                        Mon, 08 Apr 2002 14:39:16 UTC
Subscriber Name:              InReach
Telnet Escape:                    ^]  Telnet Line Mode:      Character Mode
SSH Name:                     InReach  SSH Encryption:                   Any
SSH Port:                          22  SSH Log Level:                  INFO
SSH Key:               Not Configured
```

Figure 17 - Subscriber TCP Screen

Refer to the `monitor/show subscriber` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber TCP Screen.

Displaying the Subscriber Summary Information

Use the `monitor/show subscriber summary` command to display a Subscriber Summary; for example:

Subs_jack:0 >>`show subscriber summary`

Figure 18 shows an example of the Subscriber Summary Screen.

```
                Name   Connections   Terminal Type
           In-Reach         0             Ansi
               demo         1             Ansi
               jack         0             Ansi
```

Figure 18 - Subscriber Summary Screen

Refer to the `monitor/show subscriber summary` command in the *LX-Series Commands Reference Guide* for detailed descriptions of the fields in the Subscriber Summary Screen.

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 `monitor/show audit log` command, in the Superuser Command Mode, to display the audit log for a subscriber; for example:

Subs_jack:0 >>`show audit log tim`

In the above example, the `show audit log` command is used to display the audit log for the subscriber `tim`.

Figure 19 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 19 - Audit Log Screen

Displaying the Command Log for a Subscriber

A command log is an audit trail of subscriber input in a subscriber session. Use the `monitor/show command log` command, in the Superuser Command Mode, to display the command log for a subscriber; for example:

```
Subs_jack:0 >>show command log tim
```

In the above example, the `show command log` command is used to display the command log for the subscriber `tim`.

Figure 20 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 20 - Command Log Screen

Assigning a Public Key to a Subscriber

With a Public Key, the subscriber can automate SSH connections between machines without interaction between users. The subscriber only needs to enter his username and password the first time he logs in, after which the LX stores them. On subsequent sessions, the subscriber can log in without specifying a name and password.

This example shows how to create and assign a Public Key to a Subscriber.

Prerequisites

There are no prerequisites for this configuration example.

Procedure

1. Connect to an SSH client that will be connecting to the LX via SSH.

   NOTE: In this example, the SSH client is a Linux host.

2. Log in to the Linux host with the user name and password with root privileges:
3. Generate the SSH public key without a passphrase:

   ```
   gina# ssh-keygen -f sshgina -t dsa
   ```

   NOTE: In the above example, the attribute `-f` is for filename and the attribute `-t` is for type of encryption. The dsa encryption type is for SSH Version2.

   The ssh-keygen command creates the files `sshgina` and `sshgina.pub`. The file `sshgina` is the identity file and `sshgina.pub` is the public key.

   You will be prompted for a passcode; press <Enter>.
4. Open the file that contains the Public Key (`sshgina.pub` in the above example):
5. Select and copy the Public Key from the file.
6. Log out of the Linux client that will be used to initiate the SSH connections to the LX unit:
7. Connect to the LX unit on which the subscriber (`gina` in this example) has an account. Log in to the LX unit:

   ```
   Login: InReach
   Password: ******
   ```
8. Access the Configuration Command Mode of the LX CLI.

   ```
   InReach:0>enable
   Password:>> system
   InReach:0 >>config
   Config:0 >>
   ```
9. Access the subscriber account for which you are creating the Public Key:

   ```
   Config:0 >>subscriber gina
   ```

10. Execute the ssh key command:

    Subs_gina:0 >>`ssh key`

    The following prompt is displayed:

    Please enter your key:

    Paste the Public Key for the subscriber at the above prompt. (The Public Key should be in the Paste Buffer from when it was copied in step 5.)

11. From the Linux host connect via SSH to the LX port 1:

    gina$ `ssh - i sshgina 10.242.131.48 -p 2122`

This should allow the subscriber gina to connect straight into their user prompt, without being prompted for a password.

Chapter 8

Configuring Async Port Features

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 `monitor/show device status` command to display the current temperature and humidity readings on a Sensor port; for example:

```
Async 4-4:0 >>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:

```
Async 4-4:0 >>show device all status
```

Figure 21 shows an example of the Device Status Screen for a Sensor port.

```
Time:   Tue, 01 Jul 2003 21:14:29 UTC
Port Name:                  Port_25  Device Number:                    5
Device Type:                                                      Sensor
Humidity Level(%):                                                 65.00
Temperature (Celsius):                                             25.00
Temperature (Fahrenheit):                                          77.00
```

Figure 21 - Device Status Screen for a Sensor Port

Displaying Sensor Summaries

Use the `monitor/show device summary` command to display summary information for all of the Temperature/Humidity Sensors that are currently connected to the LX unit; for example:

Async 4-4:0 >>`show device summary`

Figure 22 shows an example of the Device Summary Screen.

Device Number	Device Type	Model Name
1	Sensor	N/A

Figure 22 - Device Summary Screen for Sensors

NOTE: If any of the ports on the LX unit are configured as POWER ports, the Device Summary Screen will display information for the attached Power Management Device (IR-5100 or IR-5150).

Configuring the IdleBuffer

IdleBuffer is enabled by default. Therefore, the async port will buffer data before a TCP connection arrives when autohangup is disabled. If you want to flush (discard) all data upon a TCP connection's arrival, disable the IdleBuffer feature. If IdleBuffer is disabled, the port will not buffer erroneous data that enters the port prior to a telnet session.

To enable IdleBuffer, enter:

Async 1-1:0 >>`idlebuffer enable`

To disable IdleBuffer, enter:

Async 1-1:0 >>`no idlebuffer`

Use the `show port async <port_number> characteristics` command to display the `IdleBuffer` field in the Port Async Characteristics Screen. An example of this screen follows, with the field highlighted:

```
Time:                                        Fri, 02 Jan 2005 01:09:56 UTC
Banner:       /config/banner.default  Banner Display:                 Both
Port Number:                     1    Transparent Mode:            Disabled
Access:                     Remote    Flow Control:                    Xon
Port Name:                  Port_1    Stop Bits:                         1
Port Type:                Physical    Parity:                         None
Device Name:          /dev/ttyGN1     Bits per Character:                8
Port Prompt String:         Login     Autobaud:                    Disabled
Break:                    Enabled     Autobaud Retry:                    5
Special Break String:
Inbound Authentication:     Local     Autohangup:                  Disabled
Outbound Authentication:    Local     Radius Accounting:           Disabled
Authentication FallBack:  Disabled    Tacacs+ Accounting:          Disabled
Auth. FallBack Attempts:         0    Data Buffer Display:           Prompt
Data Buffer Size:             1024    Data Buffer Time Stamp:      Disabled
Data Buffer Syslog:       Disabled
Signal Notif. CTS High:   Disabled    Signal Notif. DSR-DCD High:  Disabled
Signal Notif. CTS Low:    Disabled    Signal Notif. DSR-DCD Low:   Disabled
Port Debug Option:        Disabled    Idlebuffer:                   Enabled
Connect Command:
```

Figure 23 - Port Characteristics Screen for IdleBuffer

Customizing Asynchronous Port Settings

The default settings for an LX asynchronous port meet the defacto standard for Console Access ports. The default settings for an LX asynchronous port are as follows:

- **Telnet Negotiations:** Enabled
- **Telnet Cr filter:** Disabled

- **Transparent Mode:** Disabled
- **Flow Control:** Xon
- **Stop Bits:** 1
- **Parity:** None
- **Bits per Character:** 8
- **Autobaud:** Disabled
- **Auto Dial:** Disabled
- **Autohangup:** Enabled
- **Baud Rate:** 9600

The default port settings are sufficient to support most remote console applications. However, for some applications you may need to specify a customized (non-default) value for one or more asynchronous port settings.

This section provides examples of all of the commands that would be used to specify non-default values for asynchronous port settings.

Prerequisites

There are no prerequisites for this configuration example.

Procedure

1. Access the Configuration Command Mode of the LX CLI.

```
Login: InReach
Password: access
InReach:0>enable
Password>> system
InReach:0 >>config
Config:0 >>
```

2. Access the Asynchronous Command Mode for the asynchronous port(s) for which you want to specify non-default settings:

```
Config:0 >>port asynchronous 4
```

3. Execute any of the following commands to specify non-default values for port settings:

   – Disable Telnet Negotiations:

     Async 4-4:0 >>`no telnet negotiation`

   – Enable Telnet Carriage Return (CR) Filtering

     Async 4-4:0 >>`telnet cr filtering enable`

   – Enable the Transparent Mode for the port:

     Async 4-4:0 >>`transparency enable`

   – Set the port Flow Control to CTS:

     Async 4-4:0 >>`flowcontrol cts`

   – Specify that the port will transmit and receive 5 data bits per character:

     Async 4-4:0 >>`bits 5`

   – Specify that the port will use the Autobaud Feature:

     Async 4-4:0 >>`autobaud enable`

   – Specify that the port will be automatically dialed:

     Async 4-4:0 >>`autodial enable`

   Set the number of stop bits to be used to maintain synchronization of data to 2:

     Async 4-4:0 >>`stopbits 2`

   – Specify that each byte that is transmitted or received by the port will contain an odd number of 1's, including the parity bit:

     Async 4-4:0 >>`parity odd`

   – Specify that the port will automatically log out when the attached device drops its signal to the DSR pin of the LX port.

     Async 4-4:0 >>`autohangup enable`

Configuring Asynchronous Ports for Data Buffering

This example shows how to configure an asynchronous port on the LX unit for data buffering. For background information on this task, refer to the following commands in the *LX-Series Commands Reference Guide*.

```
access
databuffer display
databuffer size
databuffer syslog enable
databuffer timestamp enable
```

Prerequisites

The prerequisite for this task is the following:

- Set up a connection between a network device's serial console port and a port on the LX unit. (**Note:** The LX port that receives the data will be the port that you configure for data buffering in step 2 of the following procedure.)

Procedure

1. Access the Configuration Command Mode of the LX CLI.

   Login: `InReach`

   Password: `******`

   InReach:0>`enable`

   Password: >> `******`

   InReach:0 >>`config`

   Config:0 >>

2. Access the Asynchronous Command Mode for the port that you want to configure for data buffering:

   Config:0 >>`port asynchronous 3`

3. Disable Autohangup for databuffer:

   Async 3-3:0 >>`no autohangup`

4. Specify `databuffer` as the port access method:

   Async 3-3:0 >>`access databuffer`

5. Specify that a timestamp will be added to every line of data that is printed from the port to the connected client:

   Async 3-3:0 >>`databuffer timestamp enable`

6. Specify the size, in bytes, for the data buffer on the port:

   Async 3-3:0 >>`databuffer size 1024`

7. Specify that the data received on the port will be logged to the local syslogd:

   Async 3-3:0 >>`databuffer syslog enable`

   NOTE: syslogd sends the data buffer messages to the `databuffer` file in `/var/log/`directory.

8. Specify the data buffer display option:

   Async 3-3:0 >>`databuffer display enable`

   NOTE: In the above example, the data buffer display option `enable` specifies that the contents of the data buffer will be displayed as soon as the user logs into the port. Set to `prompt` if you want the option of seeing the databuffer contents.

9. Go to the Superuser Command Mode:

   Config:0 >>`end`

10. Verify that the port has been configured for databuffer access:

    InReach:0 >>`show port asynchronous 3 characteristics`

The highlighted fields on the following Port Characteristics Screen indicate that databuffer access has been configured on port 3:

```
Time:                                        Fri, 02 Jan 2005 01:09:56 UTC
Banner:        /config/banner.default  Banner Display:                 Both
Port Number:                        3  Transparent Mode:            Disabled
Access:                    Databuffer  Flow Control:                     Xon
Port Name:                     Port_3  Stop Bits:                        1
Port Type:                   Physical  Parity:                          None
Device Name:               /dev/ttyGN2 Bits per Character:              8
Port Prompt String:              Login Autobaud:                     Disabled
Break:                         Enabled Autobaud Retry:                   5
Special Break String:
Inbound Authentication:          Local Autohangup:                   Disabled
Outbound Authentication:         Local Radius Accounting:            Disabled
Authentication FallBack:     Disabled  Tacacs+ Accounting:           Disabled
Auth. FallBack Attempts:            0  Data Buffer Display:           Enabled
Data Buffer Size:                1024  Data Buffer Time Stamp:        Enabled
Data Buffer Syslog:           Enabled
Signal Notif. CTS High:      Disabled  Signal Notif. DSR-DCD High:   Disabled
Signal Notif. CTS Low:       Disabled  Signal Notif. DSR-DCD Low:    Disabled
Port Debug Option:           Disabled  Idlebuffer:                    Enabled
Connect Command:
```

Figure 24 - Port Characteristics Screen

11. At the InReach:0 > prompt, enter:

InReach:0 >`show databuffer log <port>`

NOTE: The databuffer contents are lost during a reboot of the LX and when the databuffer size is changed.

Chapter 9

Configuring Power Control Units

The In-Reach Power Control Units (IR-4800 and IR-5150) can be managed remotely from asynchronous ports on an LX unit. The management tasks that can be performed remotely include rebooting outlets and turning outlets 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*.)

For IR-5150 units, the LX CLI also supports power boot sequencing, control of the Factory Reset button, the ability to change the IR-5150 username and password, and the ability to access the IR-5150 CLI.

Power Control units are remotely managed from LX asynchronous ports that are configured as POWER ports. This chapter describes how to configure ports as POWER ports, how to configure Power Control units via POWER ports, and how to display information on Power Control units.

The Outlet Management Feature is disabled by default. When the Outlet Management Feature is disabled, only Superusers can manage outlets.

Configuring an LX Asynchronous Port as a POWER Port

Use the `access power model` command, in the Asynchronous Command Mode, to configure an LX asynchronous port as a POWER port; for example:

```
Async 5-5:0 >>access power model ir4800
```

In the above example, port 5 is configured as a POWER port for an IR-4800 unit. Use the following syntax to configure an asynchronous port as a POWER port for an IR-5150 unit:

```
Async 5-5:0 >>access power model ir5150
```

When a port has been configured as a POWER port, you can connect a Power Control unit to it. The connection to the POWER 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.

When a Power port's access is changed to something other than "power", the outlets that exist for the port will be removed from any existing Outlet group and the port setting will be defaulted. If the port is changed back into a Power port, the previous outlets groups will have to be re-added.

Default Name for an Outlet

The default name for an outlet is derived from its POWER port and the number of the outlet on the Power Control unit. For example, `5:7` is the default name of the 7th outlet on the Power Control Unit that is managed from POWER port 5.

You can specify a descriptive name for an outlet or an outlet group. A descriptive name is a unique text name of up to 15 alphanumeric characters. For more information, refer to "Naming an Outlet" on page 188 and "Naming an Outlet Group" on page 189.

You must specify the default name, or the descriptive name, of an outlet, in the `outlet group` command in the Configuration Command Mode.

However, you only need to specify the number, or descriptive name, of the outlet in the `outlet name` command in the Asynchronous Command Mode. This is because the LX software "knows" that the POWER port 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 IR-4800 and IR-5150 Units

Outlets can be assigned to a group and managed and configured as a group. The Off Time for outlets can be specified using the LX CLI. This section describes how to assign outlets to a group and how to specify the Off Time for outlets.

Assigning Outlets to a Group

When outlets are assigned to a group, they can be configured and managed as a group. This can be more efficient than configuring and managing outlets individually.

Use the `outlet group` command to assign outlets 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 outlets `2:5 3:7 4:2 4:3 4:5` are assigned to Group `2`.

The Power Control unit must be serially attached to the LX asynchronous port when you create outlet groups. This allows for the LX to poll the Power Control unit to determine the maximum number of outlets available. Checks have been put in place to prevent a user from configuring outlet groups with outlet numbers that do not exist.

Specifying the Off Time

The Off Time is the length of time, in seconds, that outlets 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 an outlet group.

Specifying the Off Time for an Outlet Group

Use the `outlet group off time` command, in the Configuration Command Mode, to specify the Off Time for an outlet group; 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 outlets that are managed from a POWER 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 outlets 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 POWER port and has a Power Control unit attached to it.

Naming an Outlet

You can assign a descriptive name of up to 15 alphanumeric characters to an outlet.

Use the `outlet name` command, in the Asynchronous Command Mode, to specify a descriptive name for an outlet; for example:

Async 5-5:0 >>`outlet 2 name Build5NTserver`

In the above example, the descriptive name `Build5NTserver` is assigned to Outlet `2` on the Power Control unit that is managed from POWER port 5.

NOTE: The POWER port number is not specified in the `outlet name` command (e.g., `5:2`) because the POWER port is *implied* to be the current port in the Asynchronous Command Mode. In the above example, the implied POWER port is port 5. (The CLI is in the Asynchronous Command Mode for port 5.)

Naming an Outlet Group

You can assign a descriptive name of up to 15 alphanumeric characters to an outlet group.

Use the `outlet group name` command, in the Configuration Command Mode, to specify a descriptive name for an outlet group; for example:

```
Config:0 >>outlet group 14 name TestEquipment
```

In the above example, the descriptive name `TestEquipment` is assigned to outlet group `14`.

Disabling the Off Option for Power Outlets

Mission-critical outlets are those outlets that must remain on at all times. You can ensure that mission-critical outlets remain on by disabling the `Off` option for them. Outlets that have their `Off` option disabled can not be turned off with the `outlet` command or the `outlet group` command.

Use the `no outlet off` command, in the Asynchronous Command Mode, to disable the `Off` option for outlets; for example:

```
Async 5-5:0 >>no outlet off 3,7-11
```

In the above example, the `Off` option is disabled for outlet `5:3` and outlets `5:7` through `5:11`.

After you have disabled the `Off` option, you can re-enable it by executing the `outlet off enable` command; for example:

```
Async 5-5:0 >>outlet off 3,7-11 enable
```

NOTE: The `no outlet off` command and the `outlet off enable` command can only be executed on a port that is configured as a POWER port and has a Power Control unit attached to it.

Accessing the IR-4800/IR-5150 CLI

In order to access the IR-4800/IR-5150 CLI from an LX unit, the port to which the IR-4800/IR-5150 unit is attached must be configured for CLI access. Refer to "Configuring a Port for IR-4800/IR-5150 CLI Access" on page 190 to configure a port for IR-4800/IR-5150 CLI access.

To access the IR-4800/IR-5150 CLI from an LX unit, do the following:

1. Execute the `connect port async` command to make a connection to the IR-4800/IR-5150 unit, going through the access remote LX port. In this example, assume the LX port involved is port 5:

   ```
   InReach:0 >>connect port async 5
   ```

2. When you are connected to the IR-4800/IR-5150 unit, you will be prompted to log in to the unit. The default login username is "`admn`" and the password is "`admn`". The IR-4800/IR-5150 CLI will be displayed when you have finished logging in.

   Refer to your IR-4800/IR-5150 documentation for information on using the IR-4800/IR-5150 CLI.

Configuring the Unique IR-4800/IR-5150 Features

This section describes how to configure the unique IR-4800/IR-5150 Features from the LX CLI. The unique IR-4800/IR-5150 Features include power boot sequencing, control of the Factory Reset button, the ability to change the IR-4800/IR-5150 username and password, and the ability to access the IR-4800/IR-5150 CLI.

Configuring a Port for IR-4800/IR-5150 CLI Access

You can configure the POWER port of an IR-4800/IR-5150 to support access to the CLI of the IR-4800/IR-5150 unit. The CLI of the IR-4800/IR-5150 can then be accessed, via Telnet, from the CLI of the LX unit. Refer to "Accessing the IR-4800/IR-5150 CLI" on page 190 for more information on Telneting to an IR-4800/IR-5150 unit.

Do the following to configure a port for access to the CLI of the IR-4800/IR-5150 unit:

1. Access the Asynchronous Command Mode for an asynchronous port that is configured as a POWER port for an IR-4800/IR-5150 unit. (Refer to page 27 for information on accessing the Asynchronous Command Mode.)

   Async>>`access power model ir4800`

2. Use the `power cli enable` command to enable CLI access for the IR-4800/IR-5150 that is managed from the port; for example:

   Async 7-7:0 >>`power cli enable`

NOTE: The port settings on the POWER port must match the port settings on the IR-4800/IR-5150 unit. If the settings do not match on both ports, the LX unit and the IR-4800/IR-5150 unit will not be able to communicate.

Enabling the Factory Reset Button

The IR-4800/IR-5150 unit includes a Factory Reset Button, which is used to reset the IR-4800/IR-5150 unit to factory-default values. However, you must enable the Factory Reset Button in order to use it for this purpose.

Do the following to enable the Factory Reset Button:

1. Access the Asynchronous Command Mode for an asynchronous port that is configured as a POWER port for an IR-4800/IR-5150 unit. (Refer to page 27 for information on accessing the Asynchronous Command Mode.)

2. Use the `power factory reset button enable` command; for example:

   Async 7-7:0 >>`power factory reset button enable`

   The following confirmation prompt is displayed:

   ```
   Are you sure you want to enable the factory-reset
   button on the IR-5150 <yes/no>?
   ```

3. Enter `y` to enable the factory reset button on the IR-4800/IR-5150 unit, or enter `n` to abort the command.

Configuring the Authentication Feature for the IR-4800/IR-5150

The LX supports an Authentication Feature for the IR-4800/IR-5150. Under this Authentication Feature, the IR-4800/IR-5150 Admin Name and Password are passed transparently to the IR-4800/IR-5150. If the Admin Name/Password combination from the LX unit matches the one that is configured for the LX unit, the LX can manage and modify the power unit's configuration. If the username does not match, you must default the power unit to clear the stored username and password.

Specifying the IR-4800/IR-5150 Admin Name

The IR-4800/IR-5150 Admin Name and Password are passed automatically from the LX POWER port to the IR-4800/IR-5150 unit; the user does not enter these values.

Do the following to specify the IR-4800/IR-5150 Admin Name:

1. Access the Asynchronous Command Mode for an asynchronous port that is configured as a POWER port for an IR-4800/IR-5150 unit. (Refer to page 27 for information on accessing the Asynchronous Command Mode.)

   Async>>`access power model ir4800`

2. Use the `power scp admin name` command to specify the Admin Name; for example:

   Async 7-7:0 >>`power scp admin name HenryK`

In order to communicate to the IR-4800/IR-5150 unit, there must be a Login Password for the IR-4800/IR-5150 unit and IR-4800/IR-5150 authentication must be enabled. For more information, refer to "Specifying the Password for the IR-4800/IR-5150 Unit" on page 193.

This command can only be executed on a port that is configured for IR-4800/IR-5150 power access and currently has an IR-4800/IR-5150 unit connected to it. Refer to "Configuring an LX Asynchronous Port as a POWER Port" on page 185 to configure an asynchronous port for IR-4800/IR-5150 power access.

This command configures the IR-4800/IR-5150 Admin Name for both the port *and* the IR-4800/IR-5150 unit that is connected to the port. If you connect the IR-4800/IR-5150 unit to another port, you re-specify the IR-4800/IR-5150 Admin Name, and Password, for that port.

After the Admin Name and Login Password are configured, you can enable authentication. For more information, refer to "Enabling IR-4800/IR-5150 Authentication" on page 194.

Specifying the Password for the IR-4800/IR-5150 Unit

The Password for the IR-4800/IR-5150 is passed transparently, with the IR-4800/IR-5150 Admin Name, to the IR-4800/IR-5150 unit when the LX attempts to communicate to the Power unit.

Do the following to specify the Login Password of the IR-4800/IR-5150 Administrator:

1. Create a Power port:

   Async>>`access power model ir4800`

2. Execute the `power scp admin password` command; for example:

   Async 7-7:0 >>`power scp admin password`

   The following prompt is displayed:

   Enter your NEW password:

3. Enter the password at the above prompt. The following prompt is displayed:

   Re-Enter your NEW password:

4. Re-enter the password at the above prompt.

This command can only be executed on a port that is configured for IR-4800/IR-5150 power access and currently has an IR-4800/IR-5150 unit connected to it. Refer to "Configuring an LX Asynchronous Port as a POWER Port" on page 185 to configure an asynchronous port for IR-4800/IR-5150 power access.

This command configures the IR-4800/IR-5150 Login Password for both the port *and* the IR-4800/IR-5150 unit that is connected to the port. If you connect the IR-4800/IR-5150 unit to another port, you re-specify the IR-4800/IR-5150 Login Password, and Admin Name, for that port.

After the Admin Name and Login Password are configured, you can enable authentication. For more information, refer to "Enabling IR-4800/IR-5150 Authentication" on page 194.

Enabling IR-4800/IR-5150 Authentication

After you have specified the IR-4800/IR-5150 Admin Name and the IR-4800/IR-5150 Login Password for a POWER port, you can enable IR-4800/IR-5150 authentication on the port.

Do the following to enable IR-4800/IR-5150 authentication:

1. Access the Asynchronous Command Mode for an asynchronous port that is configured as a POWER port for an IR-4800/IR-5150 unit. (Refer to page 27 for information on accessing the Asynchronous Command Mode.)
2. Execute the `power scp authentication enable` command; for example:

```
Async 7-7:0 >>power scp authentication enable
```

Configuring Power Boot Sequencing

A Power Boot Sequence is a break that is sent from the IR-4800/IR-5150 to indicate that an outlet has been cold-booted. The Power Boot Sequence Feature also causes the LX, rather than the IR-4800/IR-5150, to turn on the IR-4800/IR-5150 outlets from a cold boot.

The Power Boot Sequence Feature can only be enabled on a port that is configured as a POWER port for an IR-4800/IR-5150 unit. When the Power Boot Sequence Feature is enabled on such a port, it applies to all of the outlets that are managed from that port.

To enable the Power Boot Sequence Feature on a port, do the following:

1. Access the Asynchronous Command Mode for an asynchronous port that is configured as a POWER port for an IR-4800/IR-5150 unit. (Refer to page 27 for information on accessing the Asynchronous Command Mode.)
2. Use the `power boot sequence enable` command to enable the Power Boot Sequence Feature on the port; for example:

   Async 7-7:0 >>`power boot sequence enable`

Enabling SCP

If you are unable to communicate to the Power unit, SCP may be disabled on the unit. To enable SCP, do the following:

1. Default the LX async port to default parameters:

   InReach:0 >>`config port async 3 default port`

   InReach:0 >>`logout port 3`

2. Connect and log into the (remote access) port to talk directly to the IR-4800/IR-5150 CLI:

   InReach:0 >>`connect port async 3`

3. You will now be prompted to log into the port:

   `Welcome to MRV Communications,`

   Login: `InReach`

   Password: `******`

   Press the <Enter> key at least three times.

4. After you have logged into port async 3 you now need to log into the IR-4800/IR-5150:

   `InReach Version 5.3a`

   `Username: admn`

   `Password: admn`

5. At the Sentry prompt, enter the following command to enable SCP and then logout:

   InReach: `set port scp console enabled`

   `command successful`

   InReach: `logout`

6. The remote session to port async 3 will close and at the InReach prompt reconfigure the port for Power Management IR-4800/IR-5150 and save your configuration:

   InReach:0 >> `config port async 3 access power model ir4800`

   InReach:0 >> `save config flash`

Displaying Information on Power Control Units

This section describes how to display information on Power Control units and outlets. The information that can be displayed includes statuses and summaries for Power Control units, and statuses for groups of outlets.

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 21 on page 178 for the status display for a Temperature/Humidity Sensor port.

Figure 25 shows an example of the Device Status Screen for a 5150 POWER port.

```
Time:   Tue, 08 Jul 2003 21:12:06 UTC     Device Number:                      9
Device Type:                                                             IR5150
Model Name:                                                        IR-5150-1116V
Firmware:                                  MRV Comm In-Reach IR-5150 Version 1.0j
Total Outlet Strip Load:                                                  0.25A
Total Outlet % Current Utilization (%):                                   21.67
Outlet Minimum Off Time:          10     Power Boot Sequence:           Disabled
Power Cli:                   Enabled     Power SCP Authentication:       Enabled
SCP Admin name:            Configured     SCP Admin password:           Configured
Power Factory Reset Button:   Enabled

Outlet      Name       State   Boot     Status  Wakeup   Load    Off       Groups
   1                      On      0      Normal    On      N/A     Enabled
   2                      On      1      Normal    On      N/A     Enabled
   3                      On      2      Normal    On      N/A     Enabled
   4                      On      3      Normal    On      N/A     Enabled
   5                      On      4      Normal    On      N/A     Enabled
   6                      On      5      Normal    On      N/A     Enabled
   7                      On      6      Normal    On      N/A     Enabled
   8                      On      7      Normal    On      N/A     Enabled
   9                      On      8      Normal    On      N/A     Enabled
  10                      On      9      Normal    On      N/A     Enabled
  11                      On     10      Normal    On      N/A     Enabled
  12                      On     11      Normal    On      N/A     Enabled
  13                      On     12      Normal    On      N/A     Enabled
  14                      On     13      Normal    On      N/A     Enabled
  15                      On     14      Normal    On      N/A     Enabled
  16                      On     15      Normal    On      N/A     Enabled
```

Figure 25 - Device Status Screen for a 5150 POWER Port

Figure 26 shows an example of the Device Status Screen for a 4800 POWER port.

```
Time: 29 Mar 2004 12:24:46 US/EASTERN  Device Number:                    39
Device Type:                                                          IR4800
Model Name:
Firmware:                                                Sentry Version 5.3a
Total Outlet Strip Current Load:                                       1.50
Total Outlet Strip % Current Utilization(%):                            N/A
Outlet Minimum Off Time:           11  Power Boot Sequence:          Enabled
Power Cli:                   Disabled  Power SCP Authentication:    Disabled
SCP Admin name:        Not configured  SCP Admin password:    Not configured
Power Factory Reset Button:   Enabled

Enclosure 1:                           Status: Normal
Input     A:                           Control Status: On Load: N/A
Outlet      Name          State    Status  Boot   Wakeup      Load       Off
   1  IR4800OutletAA1        On        On     0   Off     0.0 Amps   Enabled
   Groups: 2,4,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,
   49,51,53,55,57,59,61,63,65,67,69,71,73,75,77,79,81,83,85,87,89,91,93,95,97,99
   2  IR4800OutletAB1        On        On     1   Off     0.5 Amps   Enabled
   Groups: 2,4,6,8,10,12,14,16,18,20,22,24,26,28,30,32,34,36,38,40,42,44,46,48,
   50,52,54,56,58,60,62,64,66,68,70,72,74,76,78,80,82,84,86,88,90,92,94,96,98

Input     B:                           Control Status: On Load: N/A
Outlet      Name          State    Status  Boot   Wakeup      Load       Off
   3  IR4800OutletAA2        On        On     2   Off     0.5 Amps   Enabled
   Groups: 1,4
   4  IR4800OutletAB2        On        On     3   Off     0.5 Amps   Enabled
   Groups: 4
```

Figure 26 - Device Status Screen for a 4800 Port

Displaying Status Information for Outlet Groups

Use the `monitor/show outlet group status` command to display status information for outlet groups; 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* outlet groups that are managed from the LX unit:

InReach:0 >>`show outlet group all status`

Figure 27 shows an example of the Device Status Screen for an outlet group.

```
Time:      Mon, 16 Sep 2002 17:55:19   Group Number:                    2
Group Name:           TestEquipment   Group Off Time:                  4
Port  Outlet    State
  2      1       ON
  2      2       ON
```

Figure 27 - Device Status Screen for an Outlet Group

Displaying Summary Information for Power Control Units

Use the `monitor/show device summary` command 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 28 shows an example of the Device Summary Screen.

```
Device Number   Device Type       Model Name

        4         IR5150         IR-5150-1108H
        5         IR5150         IR-5152-3116VL
        6         Sensor              N/A
        7         IR4800         IR-4800-4870
```

Figure 28 - Device Summary Screen

NOTE: The `monitor/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 22 on page 178 for the Summary Screen for a Temperature/Humidity Sensor port.

Chapter 10

Configuring iptables and ip6tables

NOTE: ip6tables commands are for use with IPv6 support on the LX-Series.

IP Firewall

The MRV Graphical User Interface (GUI) provides a simple, limited method by which you can configure iptables.

The following IP Firewall GUI feature procedure uses terms familiar to Linux users, but not to non-Linux users. These Linux terms are defined as follows:

- **Chain** – A grouping of rules that specifies when the rules should be applied to traffic (INPUT, OUTPUT).
- **Rule –** The actual filter definition. For example:

  ```
  source ip address x.x.x.x destination port 23
  ```

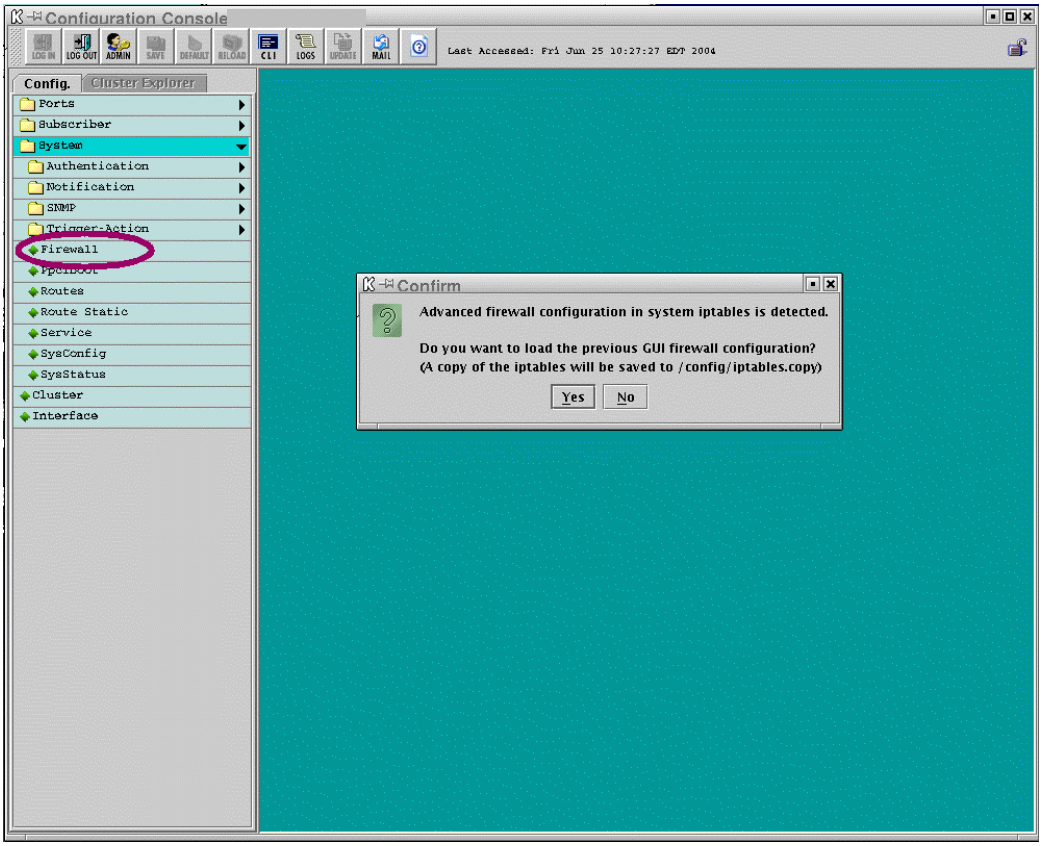
- **Policy –** The action to the rule (Accept or Drop).

  ```
  source ip address x.x.x.x destination port 23 drop
  ```

  ```
  source ip address x.x.x.x destination port 23 accept
  ```

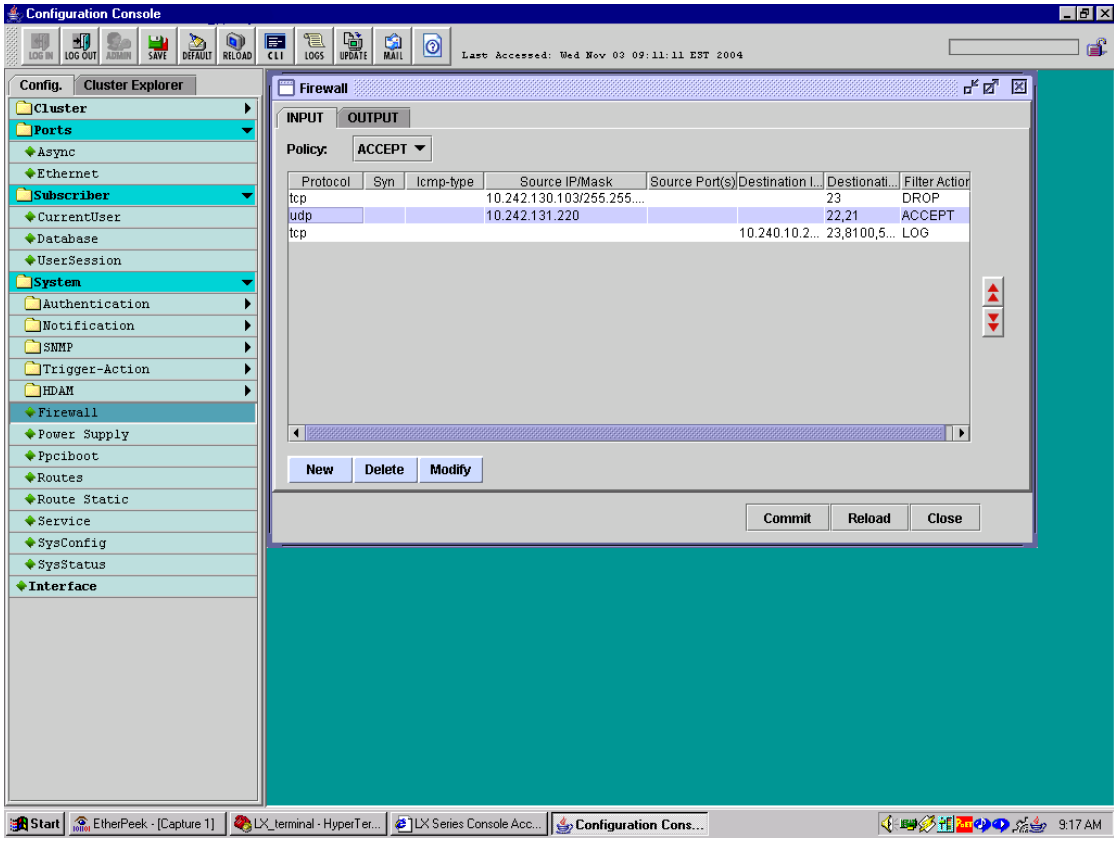
- **Default Policy** – The default action of the entire chain. If a packet makes it through all the rules in a chain, the default policy decides which final action to take (Accept or Drop).

A firewall consists of several rules for establishing (or setting) the input and output firewall policies. There is now a new **Firewall** menu item in the GUI Configuration Console. When you click on Firewall, the GUI gathers the firewall information from the LX unit. If the GUI detects an advanced firewall configuration in system iptables (advance firewall configurations are created through the shell level only, and the GUI cannot recognize these rules) a confirmation window appears:

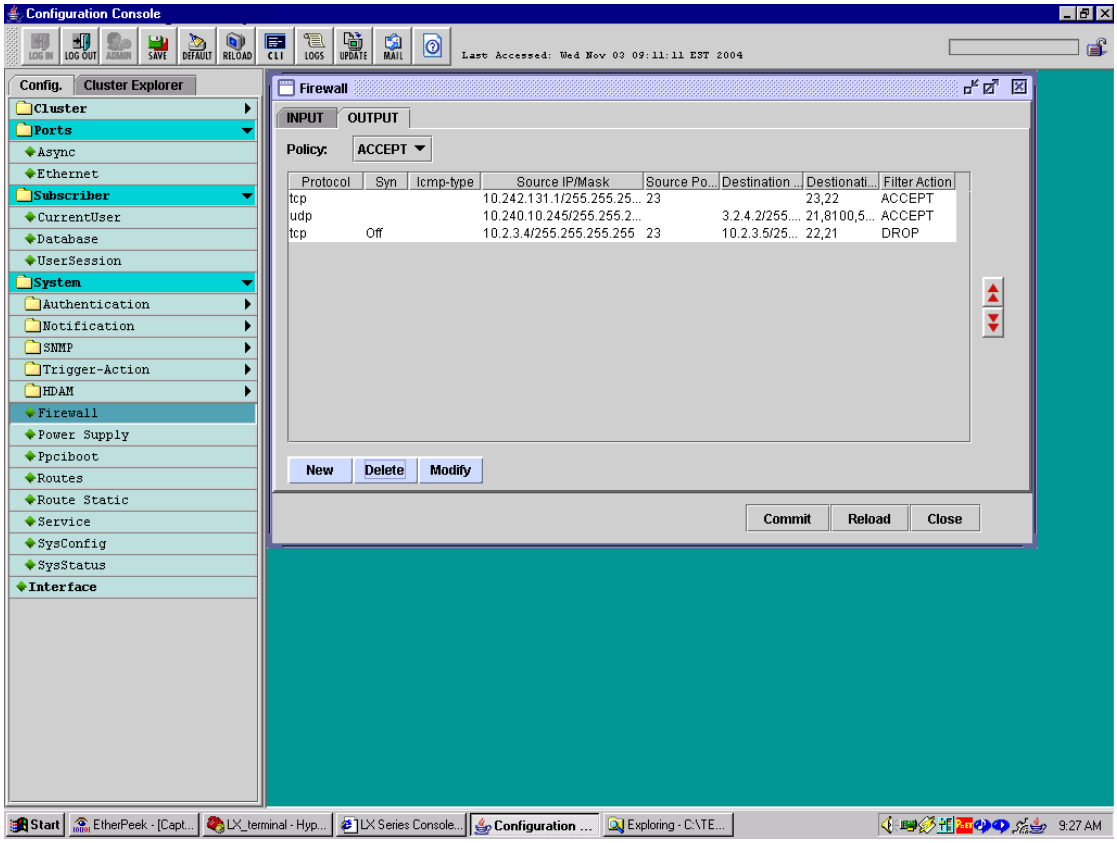


If you click **Yes**, the GUI loads the previous firewall configuration, saves a copy of iptables, overwrites iptables, and automatically displays a filled-in input table. If no previous firewall is detected, a blank input table appears.

The following window shows a "loaded" input table.



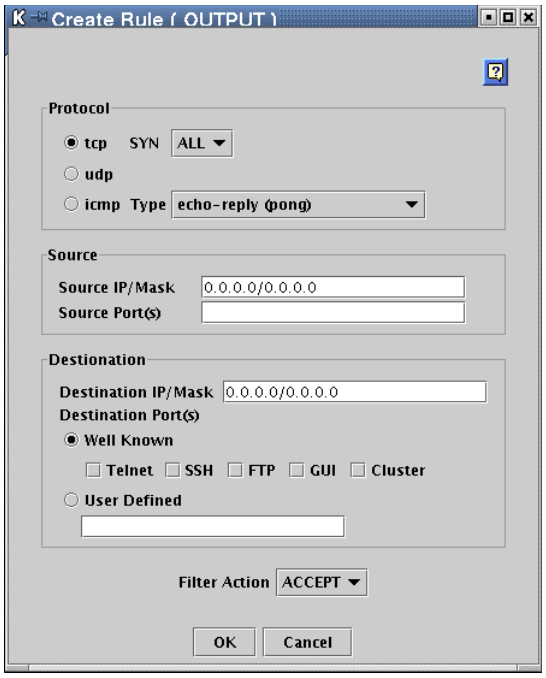
The following window shows a “loaded” output table.



Once you are in the Firewall window (whether it contains input/output or is blank), use the **New**, **Delete**, and **Modify** buttons to make changes, and use the up and down arrows on the right side of the window to change the order of the entries within the list. When you finish configuring, press **Commit** to update the configuration to the LX unit.

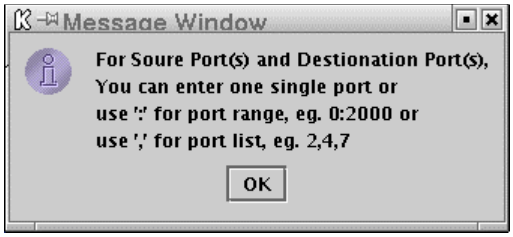
Creating A Firewall and Rules

1. Set the policy for both Input and Output by selecting one option from the **Policy** dropdown box under the **Input** and **Output** tabs. The options are **ACCEPT** and **DROP**. The policy is the default action that occurs to all traffic entering the chain. This action accepts or drops all traffic, and then executes the specific rules that you created.
2. Click on the **New** button. The **Create Rule** window appears.



3. Fill in all required fields and choose a **Filter Action** (**ACCEPT**, **DROP**, **QUEUE**, **RETURN**, and **LOG**).
4. Enter the desired rule filter characteristics and press **OK**. The GUI checks to ensure that your inputs are in the right format. If your inputs are valid, a new entry (rule) is inserted into the table.

5. Optionally, you can click on the button with a question mark in the upper-right corner of the screen to display some information about the format of specific fields in the window. A sample informational message window follows:

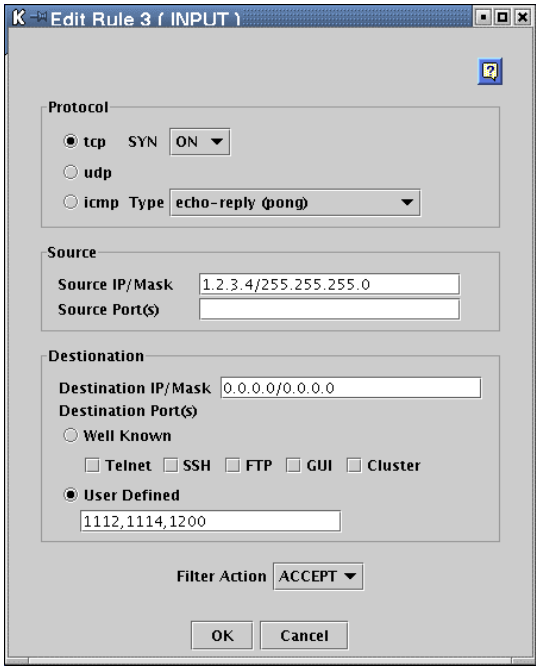


Deleting A Rule

Select one or more entries in the table and click on the **Delete** button. The entries are removed from the table.

Modifying A Rule

1. Select one entry (rule) from the Firewall table and press the **Modify** button. The Edit Rule window (with pre-filled values) appears.



2. Modify the values you want and click **OK**. The Firewall window reappears, with the changes reflected in the table.
3. Click on **Commit** to save the changes to this rule.

Changing the Rule Order

Select one entry in the table and click the up or down arrows on the right side of the window to shift the order of the entry (rule).

Updating the Firewall

All the above operations are first changed locally – nothing has yet been changed on the LX unit. When you click **Commit**, the GUI updates the local firewall configuration to the LX unit iptables, and also creates a firewall configuration copy in the LX unit.

Clicking **Commit** propagates your changes and closes the firewall window. Clicking **Reload** also propagates your changes, but leaves the firewall window open. Clicking **Close** cancels all operations after the last update to the LX unit.

NOTE: You must save the configuration for the changes to take effect after a reboot (enter `save config flash`).

Configuring Packet Filters with the `iptables` and `ip6tables` Commands

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` or `ip6tables` command to add a rule to a chain. The `iptables` and `ip6tables` commands are accessed from the CLI.

Config:0 >>`iptables <`*`string`*`>`

Config:0 >>`ip6tables <`*`string`*`>`

The following sections provide examples of how to create rules using various options of the `iptables` and `ip6tables` commands.

For detailed information on the `iptables` and `ip6tables` commands, refer to Appendix D ("Details of the iptables and ip6tables Commands") on page 389.

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:

Config:0 >> `iptables -A INPUT -s 10.240.10.240 -j DROP`

The following `ip6tables` command creates a rule that will drop any packets coming to the LX from source address `fe80::220:edff:febe:3cae`:

Config:0 >>`ip6tables -A INPUT -s`
`fe80::220:edff:febe:3cae -j DROP`

The options in the above commands 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 and ip6tables Command Options" on page 212 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 and ip6tables Command Options" on page 212 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Example: Allowing Outbound Connections to a Specific 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:

```
Config:0 >> iptables -A OUTPUT -d 123.146.17.129 -j ACCEPT
```

The following `ip6tables` command creates a rule that will allow the LX unit to output packets to the destination IP address 123.146.17.129:

```
Config:0 >>ip6tables -A OUTPUT -d fe80::220:edff:febe:3cae
-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 and ip6tables Command Options" on page 212 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 and ip6tables Command Options" on page 212 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Example: Preventing 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:

```
Config:0 >> iptables -A INPUT -s 143.114.56.104 -p tcp
--destination-port telnet -j DROP
```

The following `ip6tables` command creates a rule that ignores Telnet requests from the IP address `fe80::220:edff:febe:3cae`:

```
Config:0 >>ip6tables -A INPUT -s fe80::220:edff:febe:3cae
-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 and ip6tables Command Options" on page 212 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 and ip6tables Command Options" on page 212 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 and ip6tables Command Options" on page 212 for a description of all of the allowable values (i.e., ACCEPT, DENY, or DROP) of the `-j` option.

Notes on the `iptables` Command and `ip6tables` 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

  iptables -I INPUT 11 -s fe80::220:edff:febe:3cae -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

  iptables -R OUTPUT 8 -s fe80::220:edff:febe:3cae -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

Execute the `save configuration` command, in the Superuser Command Mode, to save the `iptables` 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*.

Chapter 11

Configuring the Trigger-Action Feature

The Trigger-Action Feature is an LX feature that executes LX commands in response to triggering events. LX command execution is an automated process, in the background, in response to a triggered event.

A triggering event is associated with an Action in a **Rule**. When the triggering event occurs, the LX unit executes the action command that is associated with it by an enabled rule.

The following events can be configured as triggering events (i.e., triggers) for a rule:

- A humidity reading that is equal to, greater than, or less than a specified threshold.
- A temperature reading that is equal to, greater than, or less than a specified threshold.
- The system clock of the LX unit reaches a certain time.
- The system calendar of the LX unit reaches a specified date or day of the week.
- The CTS signal on a specified asynchronous port changing to high or low.
- The DSR/DCD signal on a specified asynchronous port changing to high to low.
- A specified ping host returning a status of Up or Down.
- A pattern-match string is received at a specified LX asynchronous port.
- When an LX unit reboots.

- The input status on both Power Input A and Power Input B on both AC and DC versions of the LX-8000 Series.

In order to use the Trigger-Action Feature, you must first create actions and triggers. After you have created actions and triggers, you can associate actions with triggers in rules.

Refer to "Creating or Modifying an Action" (below) to create an action.

Refer to "Creating or Modifying a Trigger" on page 218 to create a trigger.

Refer to "Creating or Modifying a Rule" on page 224 to create a rule.

Creating or Modifying an Action

Do the following to create or modify an action:

1. Access the Trigger-Action Command Mode. Refer to page 33 for information on accessing the Trigger-Action Command Mode.
2. Use the `action name` command to create an action, or to access an existing action; for example:

   Trigger-Action:0 >>`action name TurnOnAC7`

   When you execute the `action name` command, you enter the Action Command Mode for the specified action. For example, the Action Command prompt for the action `TurnOnAC7` is `Action_TurnOnAC7:0 >>`.
3. Use the `command` command to specify an LX command for the action; for example:

   Action_TurnOnAC7:0 >>`command outlet 5:2 on`

   After you have specified an LX command for the action, you can bind a trigger with the action by a rule. For more information, refer to "Creating or Modifying a Rule" on page 224.

Notes and Exceptions

Keep the following in mind when you create or modify an action:

- If an action is associated with an enabled rule, you must disable the rule before you can modify the action. For more information, refer to "Disabling a Rule" on page 225 for more information.
- If you specify the `send trap message` command in an Action, you must have SNMP enabled and trap client(s) configured.
- The LX command that you specify for an action must be a Superuser command or a Multi-Level command that begins with the `configuration` command; for example:

  Action_TurnOnAC7:0 >>`command outlet 5:2 on`

  Action_TurnOnAC7:0 >>`command configuration snmp get client 4 125.65.45.34`

- If you want to specify more than one LX command for an action, use the script command; for example:

  Action_TurnOnAC7:0 >>`command script TurnOffAndDenyAccess.txt`

  Refer to the script command in the LX-Series Commands Reference guide for more information about LX command scripts.

Displaying Information on Actions

Use the `show trigger-action action` command to display information on actions; for example:

Action_TurnOnAC7:0 >>`show trigger-action action TurnonAC7`

Figure 29 shows an example of the Action Information Screen.

```
Action Name: TurnOnAC7
Command: outlet 3:7 on
```

Figure 29 - Action Information Screen

Creating or Modifying a Trigger

Do the following to create or modify a trigger:

1. Access the Trigger-Action Command Mode. Refer to page 33 for information on accessing the Trigger-Action Command Mode.
2. Use the `trigger name` command to create a trigger, or to access an existing trigger; for example:

```
Trigger-Action:0 >>trigger name TempPort4GT34
```

When you execute the `trigger name` command, you enter the Trigger Command Mode for the specified trigger. For example, the Trigger Command prompt for the trigger `TempPort4GT34` is `Trigger_TempPort4GT34:0 >>`.

In the Trigger Command Mode, you can configure a trigger. Refer to the following sections for information on configuring each type of trigger:

- "Configuring a Ping Trigger" on page 218
- "Configuring a Signal Trigger" on page 219
- "Configuring a Humidity Trigger" on page 220
- "Configuring a Pattern Trigger" on page 220
- "Configuring a Temperature Trigger" on page 221
- "Configuring a Timer Trigger" on page 221
- "Configuring a Power Trigger" on page 222
- "Configuring an Analog Trigger" on page 223

Configuring a Ping Trigger

A Ping Trigger is used to initiate an action in response to a specified ping host returning a status of Up or Down. Do the following in the Trigger Command Mode to configure a Ping Trigger:

1. Execute the `ping address` command to specify the ping host for the ping condition; for example:

```
Trigger_CapeIsReachable:0 >>ping address 119.20.110.87
```

The Ping Condition is true if host specified in this command is `up` or `down` as specified in the `ping status` command.

2. Execute the `ping status` command to specify the status that must be returned by the ping host to make the Ping Condition true; for example:

   Trigger_CapeIsReachable:0 >>`ping status up`

3. Execute the `ping interval` command to specify the interval (in seconds) at which ping messages will be sent to the specified ping host; for example:

   Trigger_CapeIsReachable:0 >>`ping interval 30`

   In this example, a ping message will be sent to the host at IP Address 119.20.110.87 at 30-second intervals. The Trigger Condition is true as long as the ping status is `Up`.

Configuring a Signal Trigger

A Signal Trigger is used to initiate an action in response to a signal transition on the CTS pin, or the DSR/DCD pin, of an LX asynchronous port. You can configure a Signal Trigger in the Trigger Command Mode.

CTS Signal Trigger

Use the `signal port cts` command to specify a signal transition on the CTS pin of a specified port as the condition for a signal trigger; for example:

Trigger_Port5CTSHigh:0 >>`signal port 5 cts high`

The above command specifies that the trigger condition is true when the CTS signal on port 5 transitions to high.

DSR/DCD Signal Trigger

Use the `signal port dsr-dcd` command to specify a signal transition on the DSR/DCD pin of a specified port as the condition for a signal trigger; for example:

Trigger_Port6DSR-DCDHigh:0 >>`signal port 6 dsr-dcd high`

The above command specifies that the trigger condition is true when the DSR/DCD signal on port 6 transitions to high.

Configuring a Humidity Trigger

A Humidity Trigger is used to initiate an action in response to a humidity reading. To configure a Humidity Trigger, execute the `humidity` command in the Trigger Command Mode; for example:

```
Trigger_HumPort4GT60:0 >>humidity port 3 > 60 hysteresis 7
```

The above example also includes an optional hysteresis value of 7. The hysteresis is a range that exists above and below the actual threshold setting. After a threshold is crossed, any readings within the hysteresis range are not considered a crossing of the threshold until a measurement outside the hysteresis has been taken. You should only configure the hysteresis to prevent "sporadic" or "spike" humidity levels from producing inappropriate firings of the Rule associated with this Trigger.

Configuring a Pattern Trigger

A Pattern Trigger is used to initiate an Action in response to a Pattern match received at an LX Databuffer or remote access ports only. Do the following in the Trigger Command Mode to configure a Pattern Trigger:

1. Execute the `pattern port string` command to specify the match pattern for the port; for example:

   ```
   Trigger_Port5Match:0 >>pattern port 5 string EdwardW
   ```

   In the above example, the pattern condition is true when a data string matching the pattern `EdwardW` is received on DATABUFFER or Remote Access port 5.

2. Execute the `pattern case` command to specify whether or not the match pattern is case sensitive or case insensitive; for example:

   ```
   Trigger_Port5Match:0 >>pattern case sensitive
   ```

NOTE: Pattern trigger is limited to the port async access types of databuffer or remote only.

Configuring a Temperature Trigger

A Temperature Trigger is used to initiate an action in response to a temperature reading. To configure a Temperature Trigger, execute the `temperature` command in the Trigger Command Mode; for example:

```
Trigger_TempPort3GT34:0 >>temperature port 3 > 34 celsius
hysteresis 4
```

In the above example, the temperature condition is true when the temperature reading on SENSOR port 3 is greater than 34 degrees Celsius.

The above example also includes an optional hysteresis value of 4. The hysteresis is a range that exists above and below the actual threshold setting. After a threshold is crossed, any readings within the hysteresis range are not considered a crossing of the threshold until a measurement outside the hysteresis has been taken. You should only configure the hysteresis to prevent "sporadic" or "spike" temperature levels from producing inappropriate firings of the Rule associated with this Trigger.

Configuring a Timer Trigger

A Timer Trigger is used to initiate an action in response to timer- or calendar-related events. A timer-related event occurs when the system clock of the LX unit reaches a certain time. A calendar-related event occurs when the system calendar of the LX unit reaching a specified date or day of the week.

Configuring a Clock-based Timer

Use the `timer time` command to specify a Timer Trigger that is based on the LX system clock reaching a specified time of day; for example:

```
Trigger_SixTwelve_AM:0 >>timer time 06:12
```

In the above example, the Timer Condition is true when the LX system clock reaches 6:12 AM each morning.

Configuring a Date-based Timer

Use the `timer date` command to specify a Timer Trigger that is based on the LX system calendar reaching a specified date; for example:

```
Trigger_MayEleventh:0 >>timer date 05/11
```

In the above example, the Timer Condition is true when the LX system calendar reaches midnight (12:00 AM) on May 11th.

Configuring a Day-based Timer

Use the `timer day` command to specify a Timer Trigger that is based on the LX system calendar reaching a specified day of the week; for example:

```
Trigger_Tuesday:0 >>timer day tue
```

In the above example, the Timer Condition is true when the LX system calendar reaches midnight (12:00 AM) on Tuesday.

Configuring a Power Trigger

A Power Trigger is used to initiate an action in response to a power failure (no power) or power restore (powered) on Power Input A or Power Input B of an LX-8000 Series unit. To configure a trigger to track a power failure on Power A Input of an LX-8000 Series unit:

1. Execute the trigger name command in the Trigger Command Mode; for example:

   ```
   Trigger_Action:0 >>trigger name track_powerA
   ```

2. Configure the power status of Power Input A; for example:

   ```
   Trigger_track_powerA:0 >>power input A status no power
   ```

Configuring an Analog Trigger

An Analog Trigger is used to initiate an action in response to an analog sensor reading. To configure an Analog Trigger, execute the `analog` command in the Trigger Command Mode; for example:

Trigger_SensorPort3GT34:0 >>`analog 10_1_5 > 34 [hysteresis 4]`

In the above example, the trigger condition is true when the sensor reading on the point with the given name is greater than 34.

The above example also includes an optional hysteresis value of 4. The hysteresis is a range that exists above and below the actual threshold setting. After a threshold is crossed, any readings within the hysteresis range are not considered a crossing of the threshold until a measurement outside the hysteresis has been taken. You should only configure the hysteresis to prevent "sporadic" or "spike" sensor levels from producing inappropriate firings of the Rule associated with this Trigger.

Displaying Information on Triggers

Use the `show trigger-action trigger` command to display information on triggers; for example:

Trigger_TempPort3GT34:0 >>`show trigger-action trigger TempPort3GT34`

Figure 30 shows an example of the Trigger Information Screen.

```
Trigger Name: TempPort3GT34  Type: Temperature(C)  Errors: 0
                    Port: 3
          Hysteresis: +/- 4 degrees celsius
              Temperature > 34 celsius
```

Figure 30 - Trigger Information Screen

NOTE: Figure 30 shows an example of the Trigger Information Screen for a Temperature Trigger. The content of the Trigger Information Screen varies according to the trigger type.

Creating or Modifying a Rule

Do the following to create or modify a rule:

1. Access the Trigger-Action Command Mode. Refer to page 33 for information on accessing the Trigger-Action Command Mode.
2. Execute the `rule name` command to create a rule, or to access an existing rule; for example:

   Trigger-Action:0 >>`rule name ACTurnOnRule7`

   When you execute the `rule name` command, you enter the Rule Command Mode for the specified rule. For example, the Rule Command prompt for the action `ACTurnOnRule7` is `Rule_ACTurnOnRule7:0 >>`.
3. Execute the `trigger` command to specify a trigger for the rule; for example:

   Rule_ACTurnOnRule7:0 >>`trigger TempPort3GT34`
4. Execute the `action` command to specify an action for the rule; for example:

   Rule_ACTurnOnRule7:0 >>`action TurnonAC7`
5. Execute the `enable` command to enable the rule; for example:

   Rule_ACTurnOnRule7:0 >>`enable`

When the rule is enabled, it is put into use by the Trigger-Action Feature; the Trigger-Action Feature executes the action associated with the rule when the condition specified for the rule trigger is true.

In the above example, the trigger associated with `ACTurnOnRule7` is `TempPort3GT34`; the action associated with `ACTurnOnRule7` is `TurnonAC7`.

If the trigger condition is `temperature port 3 > 34 celsius` and the action `is outlet 5:7 on`, this rule will cause outlet 5:7 to be turned on when the temperature on SENSOR port 3 is greater than 34 degrees Celsius.

Disabling a Rule

When a rule is disabled, it is taken out of use by the Trigger-Action Feature; the Trigger-Action Feature *does not* execute the action associated with the rule when the condition specified for the rule trigger is true.

You can disable a rule by executing the `disable` command in the Rule Command Mode; for example:

Rule_ACTurnOnRule7:0 >>`disable`

You can also disable a rule by executing the `rule` command with the `disable` command in the Trigger-Action Command Mode; for example:

Trigger-Action:0 >>`rule name ACTurnOnRule7 disable`

Displaying Information on Rules

Use the `show trigger-action rule characteristics` command to display information on rules; for example:

Rule_ACTurnOnRule7:0 >>`show trigger-action rule ACTurnOnRule7 characteristics`

Figure 31 shows an example of the Trigger Information Screen.

```
Rule Name: ACTurnOnRule7
State: enabled
Trigger Name: TempPort3GT34 Type: Temperature (F)
Action Name: TurnOnAC7 Command: outlet 5:7 on
```

Figure 31 - Rule Information Screen

Trigger-Action – Turning Off an Outlet Based on a Temperature Sensor Reading

The following example explains how to turn off an outlet based on a temperature value via Trigger-Action.

Prerequisites

You must have port 5 configured for sensor.

Procedure

1. At the **InReach:0 >>** prompt, enter:

   ```
   config trigger
   ```

2. At the **Trigger Action:0 >>** prompt, enter:

   ```
   trigger name check4-temp
   ```

3. At the **Trigger_check4-temp:0 >>** prompt, enter:

   ```
   temperature port 5 > 25 cel hysteresis 3
   ```

   where 3 is the tolerance level in degrees.

4. At the **Trigger_check4-temp:0 >>** prompt, enter:

   ```
   exit
   ```

5. At the **Trigger-action:0 >>** prompt, enter:

   ```
   action name temp-ac-power-off
   ```

6. At the **Action_temp-ac-power-off:0 >>** prompt, enter:

   ```
   command outlet 11:5 off
   ```

7. At the **Action_temp-ac-power-off:0 >>** prompt, enter:

   ```
   exit
   ```

8. At the **Trigger-action:0 >>** prompt, enter:

   ```
   rule name high-temp-off
   ```

9. At the **Rule_high-temp-off:0 >>** prompt, enter:

   `trigger check4-temp`

10. At the **Rule_high-temp-off:0 >>** prompt, enter:

    `action temp-ac-power-off`

11. At the **Rule_high-temp-off:0 >>** prompt, enter:

    `enable`

12. At the **Rule_high-temp-off:0 >>** prompt, enter `exit` three times.

13. At the **InReach:0 >>** prompt, save your configuration:

    `save config flash`

14. At the **InReach:0 >>** prompt, enter:

    `show trigger-action trigger name check4-temp`

    The following screen appears:

```
Trigger Name: check4-temp   Type: Temperature (C)       Errors: 0
Port: 5
Hysteresis: - 2 Celsius
Temperature: > 25 Celsius
```

Figure 32 - Show Trigger Action Trigger Screen

15. At the **InReach:0 >>** prompt, enter:

    `show trigger-action action name temp-ac-power-off`

    The following lines appear:

    `Action Name: temp-ac-power-off`

    `Command: outlet 11:5 off`

16. At the **InReach:0 >>** prompt, enter:

    ```
    show trigger rule name high-temp-off characteristics
    ```

    The following lines appear:

```
Rule Name: high-temp-off
State: enabled
Trigger Name: check4-temp Type: Temperature (C)
Action Name: temp-ac-power-off Command: outlet 11:5 off
```

Figure 33 - Show Trigger Rule Name Characteristics Screen

Refer to the *LX-Series Configuration Guide* for more information on Trigger Action.

Chapter 12

Configuring the Cluster Configuration and Control Feature

Overview

The new Cluster Configuration and Control (C^3) feature saves time and effort by allowing you to propagate changes to any or all units in a cluster, without having to script or manually configure each unit individually. This also allows rapid recovery and replacement if there should be a problem anywhere within the cluster.

The editor or interface for this feature is either the LX CLI or the Configuration GUI (Graphic User Interface). Both are easy to use, and both interfaces allow you to perform changes and propagate them to all units that are cluster members.

Cluster Configuration and Control also provides a mechanism for updating software (both linuxito and ppciboot) to all units within a cluster. You can schedule updates using the time-of-day rules feature to set when you want the updates done. This allows you to preschedule when updates will run - you don't even have to be there.

You can share any or all configuration attributes to all units in a cluster. You can also unshare any or all of the same administrator configurable attributes from the cluster, and keep those attributes local.

At any time you can view cluster status, including which units are in the cluster, the health of individual units, and lists of all the shared attributes and settings. You can also view the synchronization status. If attributes are not synchronized, the reason is displayed.

Each LX unit can get a software update from the TFTP server and write it to flash. The reboot image is downloaded to all cluster members. Again, Cluster Configuration and Control provides update status.

What is a Cluster?

A cluster is an independent group of LX Console Servers numbering anywhere from 2 to 1000 units that share some number of common configuration attributes. The cluster has a defined secret: all the units associated with that cluster are configured with that same secret. A cluster member's IP address table (configured on any one of the LX units) associates each individual LX with the cluster.

Cluster members can traverse switches and routers, so they do not need to be on the same network. Each LX unit in a cluster is a peer, and each unit can act as a virtual master, thus eliminating a single point of failure if something should be amiss at any one of the nodes.

For security reasons, LX units can be members of only one cluster. You can create multiple clusters when your situation demands departmental security or unit/units isolation.

How the Protocol Works

Cluster Configuration and Control uses Distributed Shared Memory. The memory exchange is done via TCP/IP protocol (fully routable via LAN/WAN routers and switches). The data exchange is encrypted through Blowfish cipher secure data exchanges. Because all cluster shared memory exchange is administrator driven, and the protocol does not perform background exchange unless prompted by the administrator, the protocol works efficiently with low network overhead. The protocol uses TCP port 8100.

Cluster Configuration and Control Terminology

This section lists some terms common to cluster operations.

- **Master** - Any unit in the cluster from which changes are being made. Any unit in the cluster can be the master, but it is a good practice to always use the same unit as the master to avoid confusion. Any configuration changes are always pushed to the cluster from the master.
- **Slave -** Any and all units in the cluster that are *not* the master. This means that once you have chosen your master unit, all other units in the cluster should be considered slaves. All configuration changes to the slaves will be pushed to them via the master unit.
- **Cluster Save Config -** The command issued to the master unit to push the configuration to the cluster.
- **Save Config Flash -** The command issued to any unit to save its *own* configuration locally.
- **Show Cluster Status -** This displays the attributes that are currently being shared with the cluster, and the status of each node in the cluster. `In Sync` is normal status for the nodes, which means they agree with the master's configuration. If there is a node out of sync, there is a brief description of why it does not agree with the master.

Cluster Configuration and Control Rules

- *Your cluster can have only one master unit at any one time.* If you have more than one master at a time, the configuration will be out of sync, and will only reflect the changes that were made by the last execution of the `cluster save configuration` command.
- After making any cluster changes to a master, your final step should *always* be to save the configuration to the cluster. This is only necessary if you changed one of the shared cluster attributes. Otherwise, you need only save to local flash.

- Do not put an individual LX into more than one cluster. Cross Clustering is not allowed, and will create some issues while saving and while talking to the cluster.
- The cluster LX nodes must be running the same version of software in order to be in-sync with each other. New features are being added all the time to the software, and the other LX nodes must also be aware of the new features, so they can be in sync with each other. RULE OF THUMB: When updating software on a LX in a cluster, use the cluster `update software` command, so that the entire cluster is updated at the same time.
- Select a unit with the highest density port count in the cluster to be your master, because if you have varying port density units in your cluster, the number of ports information to be shared will be the lowest common denominator. For example, if you have a 2-port unit, and you share ALL ports configurations and send it to the cluster containing 48 port units, only ports 1 and 2 will be shared to the cluster. If you want to make sure all the ports are shared, make a 48 port unit the master, then make the changes, and then share them to the cluster. All 48 ports will be sent, but ports 1 and 2 will be the only ones looked at by a 2-port unit.

Accessing Cluster Configuration and Control

Cluster Configuration and Control is in the Configuration Command Mode. To access it, type the following:

Config:0 >>`cluster`

Creating a Cluster Secret

The secret allows authorized LX units access to other LX units with the same secret. The secret should be at least 16 characters long. The maximum is 32 characters. All nodes in the cluster must be configured with the same secret if they are to communicate. You must set up the secret individually on each LX unit.

Setting Up the Secret at the Quick Configuration Menu

To set up the secret at the Quick Configuration Menu:

1. Plug in the terminal at the DIAG port (port 0 - port values are 9600 bps, eight data bits, one stop bit, no parity, and Xon/Xoff flow control).
2. If the unit has loaded from defaults, the following message appears: `The unit has loaded to factory defaults, would you like to run Initial Connectivity Setup? y/n` message appears.
3. Press `y` (yes) and press <Enter>. The Superuser Password prompt appears.
4. Enter 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 Cluster Secret
          7 Superuser Password
          8 Exit and Save
Enter your choice:
```

5. Press the number `6 Cluster Secret`. A `Cluster Secret:` prompt appears.
6. Enter a Cluster Secret 16 to 32 characters in length and press <Enter>. You are prompted to verify the new cluster secret.
7. Re-enter the new cluster secret and press <Enter>. The Quick Configuration menu reappears. The Cluster Secret field appears as "`Changed`".

8. Press `8` (`Exit and Save`) to save your secret. The "`Is this information correct?`" message appears.
9. Press `y` (yes) and press <Enter>. The word `Configured` appears on the Quick Configuration menu to the right of `Cluster Secret`. The `Save this information to flash?` message appears.
10. Press `y` (yes) and press <Enter>. The information is saved to flash.

```
      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 Cluster Secret                       Configured
             7 Superuser Password                   Not Changed
             8 Exit and Save
  Is this information correct?  (y/n) :
```

11. Press <Enter> several times to display the `Login:` prompt.
12. Enter your login name. The default is `InReach`.
13. Enter your password. The default is `access`. You can now use the LX unit.

Now that the secrets are configured, you can create a cluster.

Setting Up a Secret on Individual Nodes in the Cluster via the CLI

Do the following to create or modify a secret:

1. Access the Cluster Command Mode and enter a secret for your master node; for example:

   Cluster:0 >>`secret abcde678ijklmno6`

2. Exit to the Priv level **InReach:0 >>**.

3. Enter `save config to flash`.
4. Configure a secret for the other nodes in the cluster. SSH to each node you want to include in the cluster and perform the same steps.

Creating a Cluster

Do the following to create a cluster:

1. At the Cluster Command Mode, enter the address of all LX units (including your local address) in which you created a secret; for example:

   Cluster:0 >> `address A.B.C.D`

2. Share attributes you want to propagate to the other members of the cluster, then enter `cluster save config` to send the attributes to the other members. Refer to "Sharing Attributes with Other Nodes Within the Cluster" on page 236 for details on sharing attributes.
3. To see the members of the cluster, enter:

   InReach:0>`show cluster characteristics`

```
Time:   Sun, 08 Feb 2004 22:22:47 UTC  System Name:           In-Reach
Cluster Name:                                              ClusterDAone
Cluster Secret:            Configured  Cluster Debug:          Disabled
Cluster Member Addresses:
111.222.33.44
111.222.33.55
111.222.33.66
112.223.33.77
TimeZone is being shared
Snmp is being shared
Ntp is being shared
SSH is being shared
Telnet is being shared
Gui is being shared
```

Sharing Attributes with Other Nodes Within the Cluster

Whichever node you make changes from becomes the master node.

Attributes

Valid attributes are:

System Attributes

- Primary Domain
- Secondary Domain
- Gateway
- TFTP Timeout
- TFTP Retries
- NTP Server
- Alternate NTP Server
- SNMP Daemon
- Finger Daemon
- Timed Daemon
- NTP Daemon
- Telnet Daemon
- SSH Daemon
- Logging Size
- Web_Server
- Outlet Access
- Timezone
- Service: Name, All
- LDAP

- Radius
- SecurID
- TACACS+
- Snmp
- Web_Server (Server and Port)

Subscriber Attributes

- Name /All
- Port Access List
- Outlet Access List
- Outlet Group Access List
- Change Password
- Connect Escape Character

Port Async Attributes

- All, Number
- Access
- Banner, Banner Display
- Transparent Mode
- Flow Control
- Stop Bits, Parity, Bits per Character
- Port Prompt String
- Autobaud
- Break Autobaud Retry
- Special Break String
- Auto Dial

- Inbound Authentication, Outbound Authentication
- Autohangup
- Radius Accounting, Tacacs+ Accounting
- Authentication FallBack
- Telnet Break String, Telnet Negotiations, Telnet Cr filter, TCP Accept Verification, TCP Accept Message String
- Data Buffer Size, Data Buffer Display, Data Buffer Syslog, Data Buffer Time Stamp
- Connect Command
- TCP (Transmission Control Protocol) Window Size, TCP Transmit Mode, TCP Pipe Destination Host, TCP Pipe Destination Port
- Modem Control, Modem Timeout, Modem Retry, Modem Pool, Modem Dialout Num., Modem Init String
- APD (Auto Protocol Detect) Signature, APD Retry, APD Timeout
- Control Dtr, Control Rts
- SCP Username/Password, Off timers/enable
- TCP Pipe Retries

Attributes not shared on port

- Port Name, Outlet Names
- Signal Notification
- Snmp sensor units / alarm severity

Sharing an Attribute

Do the following to share an attribute:

1. At the Cluster Command Mode, share an attribute; for example:

   Cluster:0 >> `share telnet daemon`

This shares the telnet daemon state as on the master machine.

2. Enter `cluster save config` to share the attribute across all nodes in the cluster.
3. Enter `show cluster characteristics` to see which attributes are being shared.

NOTE: This feature is not shared until a `cluster save config` is performed.

Unsharing Attributes

NOTE: When you unshare an attribute, it keeps its current value. It is only unshared.

You can also unshare attributes from an individual node, or across the cluster.

Locally

Do the following to unshare an attribute locally:

1. At the Cluster Command Mode, unshare the attribute; for example:

   Cluster:0 >> `unshare local telnet daemon`

   This unshares the telnet daemon state on the local machine and all other cluster nodes remain shared. You do not need to save the configuration to the cluster, because you are only unsharing the attribute on a local node.

Globally

Do the following to unshare an attribute across the entire cluster:

1. At the Cluster Command Mode, unshare the attribute; for example:

   Cluster:0 >> `unshare telnet daemon`

2. Enter `cluster save config` to unshare the attribute across all nodes in the cluster.

Displaying Cluster Information

Use the `show cluster characteristics` command to display information on characteristics at either of the following command modes; for example:

Cluster:0 >>`show cluster characteristics`

InReach:0 >>`show cluster characteristics`

Figure 34 shows an example of the Cluster Characteristics Screen.

```
System Name:           In-Reach     Time:   Sun, 08 Feb 2004 22:22:47 UTC
Cluster Name:                                              ClusterDAone
Cluster Secret:            Configured  Cluster Debug:          Disabled
Cluster Member Addresses:
111.222.33.44
111.222.33.55
111.222.33.66
112.223.33.77
Interface 1 is being shared
Interface 2 is being shared
Ntp is being shared
SSH is being shared
Telnet is being shared
Gui is being shared
Timed is being shared
Fingerd is being shared
Gateway1 is being shared
Dns1 is being shared
Dns2 is being shared
TftpTimeout is being shared
TftpRetries is being shared
OutletAccess is being shared
Subscriber ab is being shared
Subscriber billm is being shared
Subscriber timb is being shared
```

Figure 34 - Cluster Characteristics Screen

Use the `show cluster status` command to display information on status at either of the following command modes; for example:

Cluster:0 >>`show cluster status`

```
InReach:0 >>show cluster status

Cluster Node IP     Software Version     PpciBoot Version     Synchronized

140.111.222.333      3.3.0                3.2.0                yes
140.111.222.334      3.3.0                3.2.0                yes
```

Figure 35 - Cluster Status Screen

Updating the Software

You can update the software on an individual node, or on all members across an entire cluster.

Updating Software on an Individual Node

Do the following to update the software on an individual node:

1. At the Superuser Command Mode, enter the address of the node on which you want to update the software; for example:

   InReach:0 >> `cluster update software A.B.C.D`

   This updates the software on that node. You do not need to save the configuration, because you are only updating software, not rebooting it.

2. To run the new image, you must perform a reboot. Enter the following:

   InReach:0 >> `cluster reload A.B.C.D`

Updating Software Across the Entire Cluster

Do the following to update the software across all cluster members:

1. At the Cluster Command Mode, enter the following; for example:

   InReach:0 >> `cluster update software`

2. To run the new image, you must perform a reboot. Enter the following:

   InReach:0 >> `cluster reload`

3. The message `Are you sure you want to reload the cluster? y/n` appears. Enter `y` to update the software.

User GUI (Graphic User Interface)

The User GUI simplifies the sometimes complex process of providing menu-defined access and connectivity. You can browse to the IP address of any console server in the cluster, and use the Cluster Explorer search capability across multiple LX units.

The GUI now has two modes: Configuration and Menu. The one you can access depends on what privileges the administrator has given you.

A Web/GUI menu displays the structure of menu labels for the commands available to a specific user. To access the menu via the GUI, you must first modify the subscriber profile.

The LX has a default web menu name called `demo_menu`. The demo_menu is a template that you can modify to fit your specific location. Refer to "Enabling the Menu Feature" on page 168 for more information on modifying menus.

To modify the subscriber profile:

1. At the Subscriber Mode, enter, for example:

   Subs_frank:0 >> `web menu name demo_menu`

   This is the menu you want the subscriber to access when they log into the GUI.

2. Set the Web Login Mode for the GUI to `Menu`. The options are Config or Menu; for example.

   Subs_frank:0 >> `web login mode menu`

NOTE: Set the Web Login Mode to "Menu" if you want the subscriber to access the defined menu. Set the Web Login Mode to "Config" if you want the subscriber to access the standard configuration GUI.

3. To verify that you have configured the subscriber correctly, enter the following:

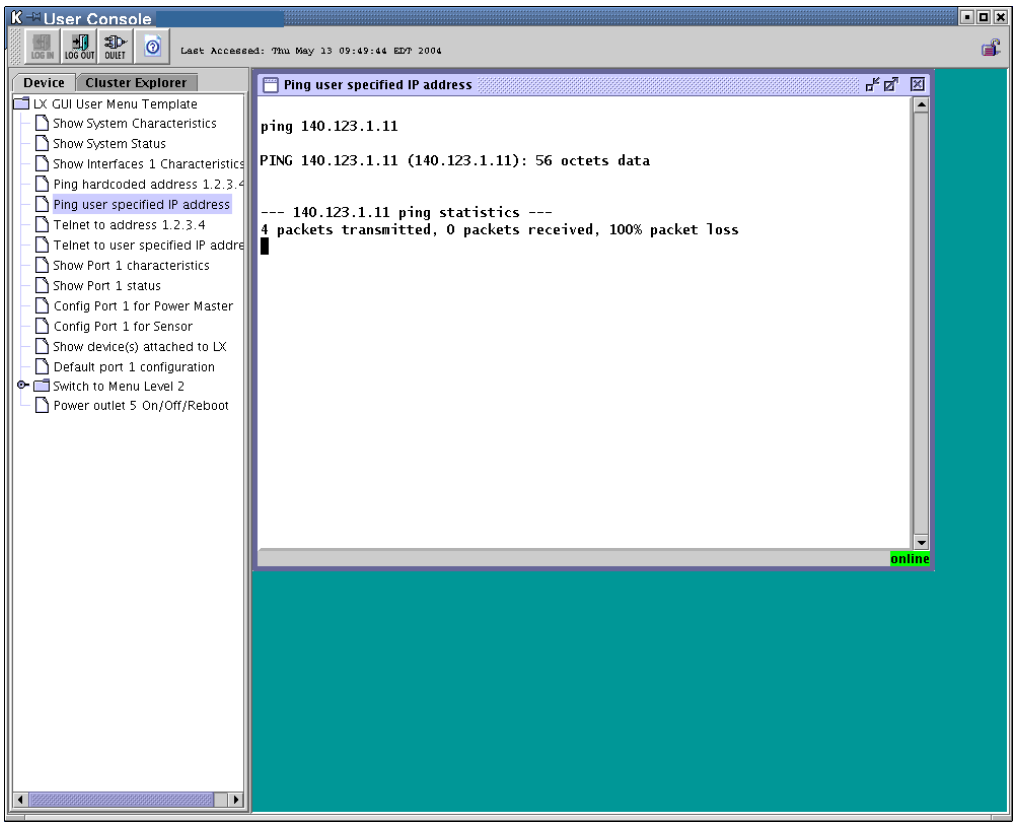
InReach:0 >> `show subscriber frank characteristics`

```
Subscriber Name:                frank
Preferred Service:                     Dedicated Service:
Security:                                                          User
Login Mode  :                     CLI  User Password:              Enabled
Maximum Connections:                5  Maximum Sessions:                4
Command Logging:            Disabled  Audit Logging  :            Disabled
Idle Timeout:                       0  User Prompt:                   frank
Menu Name:           /config/M_frank  Screen Pause:                 Enabled
Web Menu Name:    /config/M_demo_menu  Web Login Mode:                 Menu
Forward Switch:                   ^F  Local Switch:                    ^L
Backward Switch:                  ^B  Dialback Feature:           Disabled
Dialback Number:
Port Access   list:                                                  0-8
Remote Access list:                          Telnet Ssh Web_Server Console
Outlet Access list:
Outlet Group Access list:
```

NOTE: If you are using a Web Menu Name, configure the name as `M_demo_menu` if you want to use the default menu template.

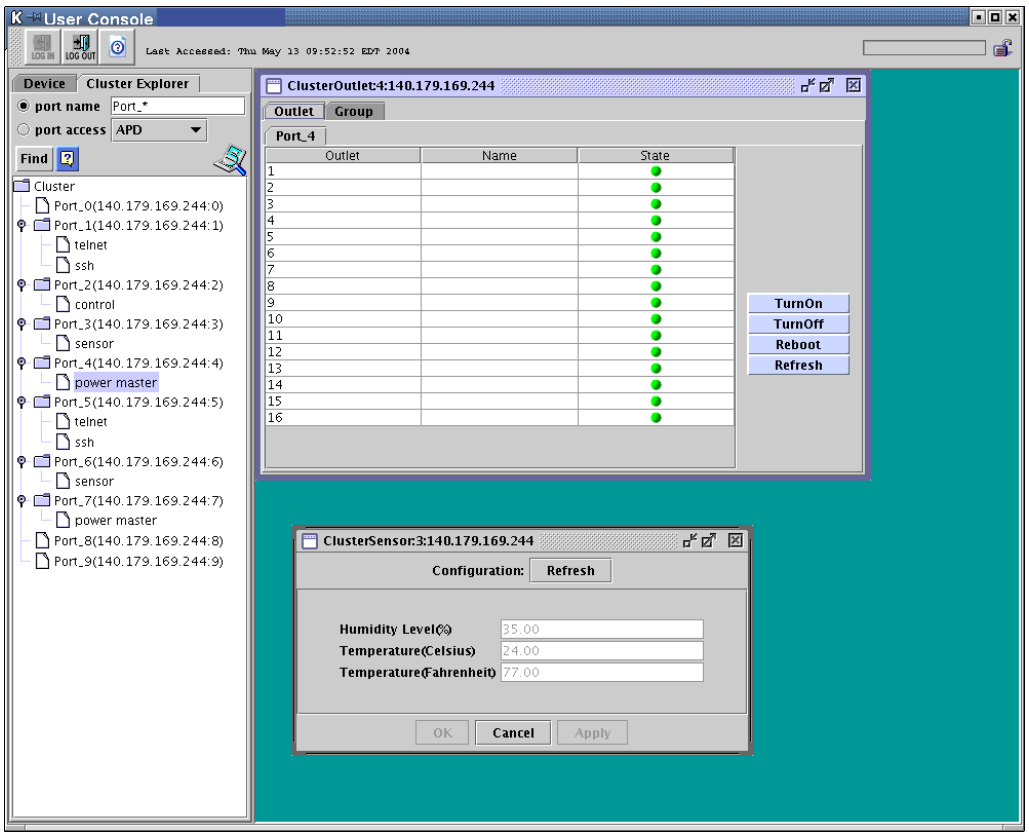
4. Check the Web Menu Name, highlighted above. At this stage, you can login via the GUI and access the web/GUI menu.

5. Access the GUI via the web and login with the username and password. The menu appears; for example:



In this example, you selected **Ping User Specified IP address:**. The window to the right appears automatically with the ping command results.

Clicking the **Cluster Explorer** tab at the top of the window allows you to search across the cluster by port name. Based on permissions, you can also look at sensor values, power module outlet status, and have Telnet and SSH access to Remote Access Ports.



Generating Debug Information

NOTE: When debug cluster is enabled and the LX is rebooted, the debug cluster reverts to the default state of off.

You can generate debug messages for troubleshooting by typing `debug cluster enable` in the Superuser Command Mode. This feature is disabled by default. Type `no debug cluster` to disable this feature.

Use the `show debug cluster` command to display debug information at any of the following command modes; for example:

Cluster:0 >>`show debug cluster`

InReach:0 >>`show debug cluster`

Config:0 >>`show debug cluster`

```
Mar 24 14:40:19 ConfCall: registered port 8101
Mar 24 14:40:19 ConfCall: unregistered port 8101
Mar 24 14:49:59 looking for ssh key /config/ssh_authorized_InReach.pub
Mar 24 14:49:59 adding file /config/ssh_authorized_InReach.pub
Mar 24 14:49:59 looking for menu /config/Menu2
Mar 24 14:49:59 looking for gui menu /config/Menu2
Mar 24 14:49:59 looking for ssh key /config/ssh_authorized_cmurch.pub
Mar 24 14:49:59 looking for menu /config/M_cmurch
Mar 24 14:49:59 looking for gui menu /config/M_cmurch
Mar 24 14:49:59 external ref = /config/ssh_authorized_InReach.pub
Mar 24 14:50:00 calling Agent_Main
Mar 24 14:50:00 calling Tcl_CreateInterp
Mar 24 14:50:00 calling initialize
```

Figure 36 - Debug Cluster Screen

Searching a Cluster

NOTE: The `cluster search` command is now accessible at both the user and superuser levels. At the User level, you do not need to enter a superuser name or password, but you cannot execute Superuser commands. The searches you can perform are different, depending on the level. Refer to the *LX-Series Commands Reference Guide* for details.

You can search a cluster for a port name or an access method with the `cluster search` command. The syntax follows:

InReach:0 >> `cluster search portname <port_name> | <access>`

Searching for a Port Name

To search for a case-sensitive port name, enter:

InReach:0 >> `cluster search portname Port_1`

A screen similar to the following appears:

```
Cluster Node IP Port # Port Name        Access     Telnet Port SSH Port Auth

142.122.166.206 1      Port_1           Remote     2100        2122     Local
142.122.166.221 1      Port_1           Remote     2100        2122     Local
```

Figure 37 - Cluster Search Port Name Screen

Searching for an Access Method

To search for an access method, enter:

InReach:0 >> `cluster search access apd`

A screen similar to the following appears:

```
Cluster Node IP Port # Port Name        Access     Telnet Port SSH Port Auth

142.122.166.206 1      Port_1           Remote     2100        2122     Local
142.122.166.221 1      Port_1           Remote     2100        2122     Local
```

Figure 38 - Cluster Search Access Screen

Naming a Cluster

Do the following to name a cluster:

1. At the Superuser Command Mode, share an attribute; for example:

   Config:0 >>`config cluster name` *`cluster_name`*

   where *`cluster_name`* can be from 1 to 31 characters long.

   This name is shared after you execute `cluster save config`.

Sharing and Unsharing Interfaces

You can share the characteristics of one interface with any or all other interfaces in the cluster. Do the following to share an interface:

1. At the Cluster Mode, share an interface; for example:

   Cluster:0 >>`share interface` *`all`* | *`interface_number`*

   where *`all`* shares all interfaces, and *`interface_number`* shares a specific interface.

   This interface is shared after you execute `cluster save config`.

2. To unshare an interface:

   Cluster:0 >>`unshare interface` *`all`* | *`interface_number`*

   where *`all`* unshares all interfaces, and *`interface_number`* unshares a specific interface.

   To view which interfaces are shared or unshared, type `show cluster characteristics` to display the Cluster Characteristics screen. An example of this screen is found in Figure 34 on page 240.

Sharing and Unsharing Subscribers

You can share the characteristics of one subscriber with any or all other subscribers in the cluster. Do the following to share a subscriber:

1. At the Cluster Mode, share a subscriber; for example:

   Cluster:0 >>`share subscriber all` | *`subscriber_name`*

where *all* shares all subscriber, and *subscriber_name* shares a specific subscriber.

This subscriber is shared after you execute `cluster save config`.

2. To unshare a subscriber:

   Cluster:0 >>`unshare subscriber` *`all | subscriber_name`*

   where *all* unshares all subscribers, and *subscriber_name* unshares a specific subscriber.

   To view which subscribers are shared or unshared, type `show cluster characteristics` to display the Cluster Characteristics screen. An example of this screen is found in Figure 34 on page 240.

Sharing and Unsharing the Authenticate Image

You can share the authenticate image with any or all other members in the cluster. Do the following to share the authenticate image:

1. At the Cluster Mode, share the authenticate image; for example:

   Cluster:0 >>`share authenticate image`

   The image is shared after you execute `cluster save config`.

2. To unshare the authenticate image:

   Cluster:0 >>`unshare authenticate image`

   To view whether the authenticate image is shared or unshared, type `show cluster characteristics` to display the Cluster Characteristics screen. An example of this screen is found in Figure 34 on page 240.

Sharing and Unsharing the Message

You can share the message with any or all other members in the cluster. Do the following to share the message:

1. At the Cluster Mode, share the message; for example:

   Cluster:0 >>`share message`

The message is shared after you execute `cluster save config`.

2. To unshare the message:

   Cluster:0 >>`unshare message`

   To view whether the message is shared or unshared, type `show cluster characteristics` to display the Cluster Characteristics screen. An example of this screen is found in Figure 34 on page 240.

Sharing and Unsharing the Telnet Client

You can share the telnet client with any or all other members in the cluster. Do the following to share the telnet client:

1. At the Cluster Mode, share the telnet client; for example:

   Cluster:0 >>`share telnet client`

   The telnet client is shared after you execute `cluster save config`.

2. To unshare the telnet client:

   Cluster:0 >>`unshare telnet client`

   To view whether the telnet client is shared or unshared, type `show cluster characteristics` to display the Cluster Characteristics screen. An example of this screen is found in Figure 34 on page 240.

Configuring a Remote Cluster Member

NOTE: The `cluster command` command is now accessible at both the user and superuser levels. At the User level, you do not need to enter a superuser name or password, but you cannot execute Superuser commands. Refer to the *LX-Series Commands Reference Guide* for details.

You can issue a CLI command to any remote cluster member without having to log in to that cluster member. This command is available only at the Superuser level. The syntax follows:

InReach:0 >>`cluster command` *`all | <ip_address> <superuser_name> <superuser_password> <cluster_command>`*

where:

- *`all`* - Runs the command across all clusters.
- *`ip_address`* - The IP address of the cluster member to which you want to send a command.
- *`superuser_name`* - The superuser name of the cluster member to which you want to send a command.
- *`superuser_password`* - The superuser password of the cluster member to which you want to send a command.
- *`cluster_command`* - The cluster command you want to send to the cluster member.

At the Superuser level, you must enter the superuser name and password, and then enter the command.

Examples

InReach:0 >>`cluster command all enable system conf port async 1`

InReach:0 >>`cluster command 120.130.222.33 enable system conf port 1`

Chapter 13

SNMP Configuration

Introduction

This guide provides end-users of MRV Communications LX units with fundamentals of SNMP and MIBs, and procedures on how to configure the LX unit to provide SNMP management.

Network Management System

Network Management Systems monitor and control network elements. Network Elements (NE) are devices such as hosts, routers, terminal servers, etc., that are monitored and controlled through access to their management information.

The NMS can potentially monitor several nodes, each with a processing entity termed an agent. An agent is a network management software module that resides in a managed device. It has local knowledge of management information and can translate that information into a form compatible with SNMP. The managed objects might be configuration parameters or performance statistics relating to the device being managed. Operations of the protocol are carried out under an administrative framework that defines both authentication and authorization policies in SNMPv1, SNMPv2C, and SNMPv3.

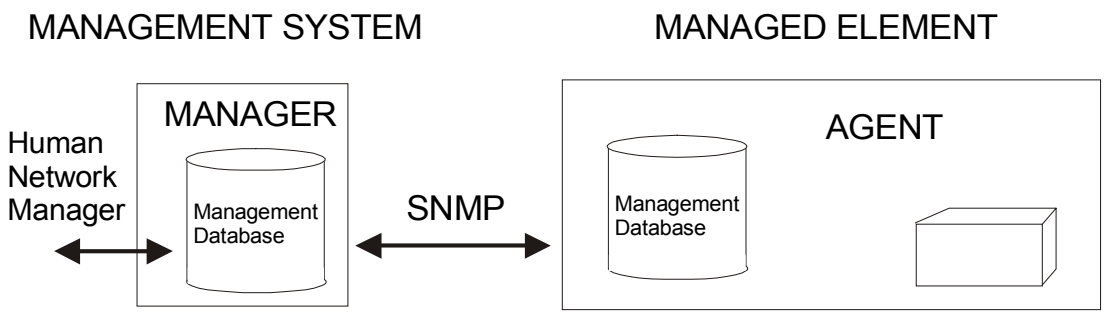


Figure 39 - Typical Network Management System

All SNMP managed devices contain a Management Information Base (MIB) database that stores management information for that device. The database is organized as a tree; branches of the tree name objects and the leaves of the tree contain the values manipulated to effect management. The values are comprised of managed objects and are identified by object identifiers. Objects in the MIB are defined using Abstract Syntax Notation One (ASN.1). The MIB structure is depicted in RFC 1155, "The Structure of Management Information" or SMI.

A managed object is one of any number of characteristics of a managed device. Managed objects are comprised of one or more object instances.

A managed object is identified by an object identifier (OID). The tree consists of a root connected to a number of labeled nodes via edges. Each node may, in turn, have children of its own which are labeled. In this case, we may term the node a subtree.

The Simple Network Management Protocol (SNMP) is an Internet standard defined by the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157, which specifies how network management information is carried through a network.

MRV Communications devices support SNMP by implementing an SNMP Agent. The agent supports SNMP MIB data and makes it available when requested via SNMP Get/Set requests.

In addition, the LX device generates SNMP Traps, which are asynchronous messages used to indicate specific events on the device.

Management information is a collection of managed objects, residing in a virtual information store called the Management Information Base (MIB). Collections of related objects are defined in MIB modules and are written using a subset of ASN.1. The subset is defined by the SMI and is divided into three parts:

1. Module definitions are used when describing information modules. An ASN.1 macro MODULE-IDENTITY is used to convey the semantics of an information module.
2. Object definitions are used when describing managed objects. An ASN.1 macro OBJECT-TYPE is used to convey the syntax and semantics of a managed object.
3. Notification definitions are used when describing unsolicited transmissions of management information. An ASN.1 macro TRAP-TYPE is used to convey the syntax and semantics of a trap.

MIBs are organized into MIB modules. A MIB module is a file defining managed MIB objects. In addition to the standard MIBs, companies usually provide vendor specific enterprise MIBs which define additional MIB objects used to manage the network devices.

Example of an OID Structure

A sample Object identifier follows:

```
Internet    OBJECT IDENTIFIER ::=  (iso (1) org (3) dod (6) internet (1) 1}
```

In tree format, the same object appears as follows:

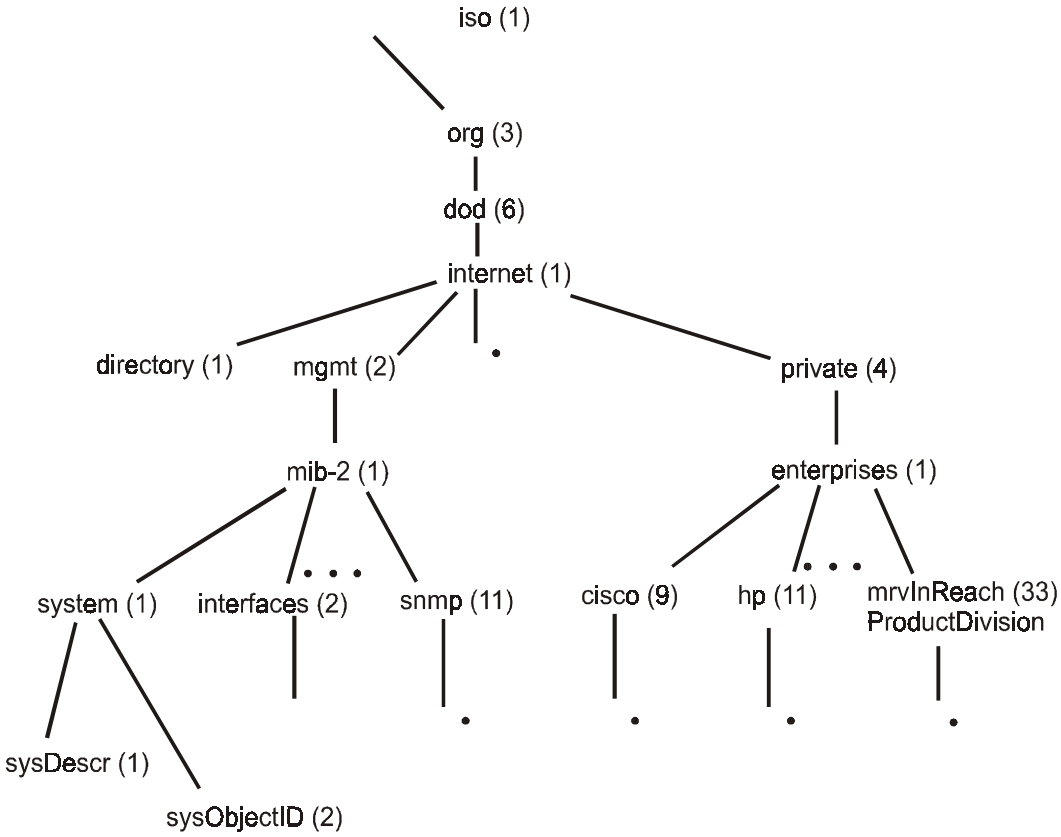


Figure 40 - Hierarchical Tree Structure

Standard MIBs

RFC Number	Description
RFC 1213	MIB-2
RFC 1658	Character MIB
RFC 3411	SNMP V3 Framework MIB
RFC 3414	SNMP V3 User-based Security Model (USM) MIB
RFC 3415	SNMP V3 View-based Access Control Model (VACM) MIB

MRV InReach Enterprise MIBs

MRV InReach MIB	Description
MRV-IR-SYSTEM-MIB	InReach System MIB
MRV-IR-CHAR-MIB	InReach Character MIB
MRV-IR-HDAM-MIB	In-Reach High Density Alarm (HDAM) MIB
MRV-IR-TRAP-MIB	InReach Trap MIB

LX Standard SNMP Traps

The following table lists the standard traps supported by LX:

Trap ID	Trap Name	Trap Description
0	coldStart	Trap generated when the system powers on.
4	authenticationFailure	Trap generated by SNMP agent when an incoming SNMP request fails authentication.

LX Enterprise-Specific SNMP Traps

The following table lists all the enterprise-specific traps supported by LX:

Trap ID	Trap Name	Trap Description
1	irNotifyEvent	Trap generated to send a text message to an SNMP client.
2	irTempHighTholdAlarm-Raised	Temperature trap indicating configured high threshold has been raised.
3	irTempHighTholdAlarm-Cleared	Temperature trap indicating configured high threshold has been cleared.
4	irTempLowTholdAlarm-Raised	Temperature trap indicating configured low threshold has been raised.
5	irTempLowTholdAlarm-Cleared	Temperature trap indicating configured low threshold has been cleared.
6	irHumidityHighThold-AlarmRaised	Humidity trap indicating configured high threshold has been raised.
7	irHumidityHighThold-AlarmCleared	Humidity trap indicating configured high threshold has been cleared.
8	irHumidityLowTholdAlarm-Raised	Humidity trap indicating configured low threshold has been raised.
9	irHumidityLowTholdAlarm-Cleared	Humidity trap indicating configured low threshold has been cleared.
10	irClusterSyncStarted	Cluster trap indicating Cluster Synchronisation has started.
11	irClusterSyncCompleted	Cluster trap indicating Cluster Synchronisation has completed.
12	irClusterSoftwareUpdateStarted	Cluster trap indicating Cluster system software updated has started.
13	irClusterSoftwareUpdate-Completed	Cluster trap indicating Cluster system software updated has completed.

14	irClusterBootloaderUpdat-eStarted	Cluster trap indicating Cluster boot loader software updated has started.
15	irClusterBootloaderUpdate-Completed	Cluster trap indicating Cluster boot loader software updated has completed.
16	irPowerSupplyStatus-Changed	Power supply trap indicating power supply status has changed.
17	irLoginFailed	A user tried to log in and failed.
18	irHdamAlarmRaised	The HDAM unit has generated an alarm.
19	irHdamAlarmCleared	The HDAM unit has cleared an alarm.
20	irHdamContactLost	The LX has lost contact with the HDAM unit.
21	irHdamContactRegained	The LX has regained contact with the HDAM unit.
22	irHdamPowerFeedALost	The HDAM unit has lost power feed A.
23	irHdamPowerFeedARe-gained	The HDAM unit has regained power feed A.
24	irHdamPowerFeedBLost	The HDAM unit has lost power feed B.
25	irHdamPowerFeedBRe-gained	The HDAM unit has regained power feed B.
26	irOnboardTempExceeded	Onboard temperature has exceeded the threshold value.
27	irOnboardTempCleared	Onboard temperature has dropped below the threshold value.
28	irAdminLoginFailed	Administrator login failed.
29	irEnetPortBondLinkStatus-Changed	Enet port bonding link status changed.

LX Fault/Cleared Alarm SNMP Trap Pairings

The following table shows the pairings of a fault alarm and the corresponding cleared alarm trap id's:

Fault Trap ID	Fault Alarm Trap	Cleared Trap ID	Cleared Alarm Trap
2	irTempHighTholdAlarm-Raised	3	irTempHighTholdAlarmCleared
4	irTempLowTholdAlarm-Raised	5	irTempLowTholdAlarmCleared
6	irHumidityHighThold-AlarmRaised	7	irHumidityHighTholdAlarm-Cleared
8	irHumidityLowTholdAlarm-Raised	9	irHumidityLowTholdAlarm-Cleared
18	irHdamAlarmRaised	19	irHdamAlarmCleared
20	irHdamContactLost	21	irHdamContactRegained
22	irHdamPowerFeedALost	23	irHdamPowerFeedARegained
24	irHdamPowerFeedBLost	25	irHdamPowerFeedBRegained
26	irOnboardTempExceeded	27	irOnboardTempCleared

Security

Additional security is provided by only allowing SNMP requests from hosts that are configured in the GET/SET client table.

The SNMP agent is disabled by default. An SNMP Client must be configured on the device before it can communicate with the SNMP agent. An SNMP Client is configured via the Command Line Interface (CLI). The agent must be enabled via the CLI to accept SNMP requests.

SNMP Management

To allow a device to be managed by SNMP, the SNMP agent must be enabled and GET/SET clients configured (see the following section).

Configuring an SNMP Agent

This section describes how to configure SNMP Clients, enable SNMP, and display SNMP-related information.

The tasks in this section are performed in the LX Command Line Interface (CLI). Refer to the *LX-Series Commands Reference Guide* (451-0310) for more information on the commands that are used in this section.

Enabling/Disabling an SNMP Agent

To enable the SNMP agent on a device, enter the following:

```
Config:1>>snmp enable
```

To disable the SNMP agent on a device, enter the following:

```
Config:1>>no snmp enable
```

Adding or Removing an SNMP GET Client

Before an SNMP client can send SNMP GET requests to the agent, it must be configured in the SNMP Get client table.

A GET Client is a specific NOC that is allowed to manage the In-Reach device via GET and GET NEXT requests. You can configure up to 16 of these SNMP clients.

To add an SNMP GET client, type the following:

Snmp:0 >>`get client <number> ip_address`

A *number* value is a number from 0 to 15.

To remove an SNMP GET client, type the following:

Snmp:0 >>`no get client <number>`

SNMP GET Client Configuration Examples

Snmp:1 >>`get client 0 <a.b.c.d>`

Snmp:1 >>`get client 0 community <string>`

Snmp:1 >>`get client 0 version <v1 | v2c>`

Snmp:1 >>`get client 0 mask 255.255.255.0`

Snmp:1 >>`no get client 0`

NOTE: A community string can be up to 32 characters long.

Adding or Removing an SNMP SET Client

Before an SNMP client can send SNMP SET requests to the agent, it must be configured in the SNMP Set client table.

Execute this command at the SNMP command mode. A SET Client is a NOC that may issue SET Requests to the device. You can configure up to 16 of these clients.

To add an SNMP SET client, type the following:

Snmp:0 >>`set client <number> ip_address`

A *number* value is a number from 0 to 15.

To remove an entry, type the following:

`Config0:>>no set client <number>`

SNMP SET Client Configuration Examples

Snmp:1 >>`set client 0 <a.b.c.d>`

Snmp:1 >>set client 0 community <string>

Snmp:1 >>set client 0 version <v1 | v2c>

Snmp:1 >>set client 0 mask 255.255.255.0

Snmp:1 >>no set client 0

Adding or Removing an SNMP Trap Client

Execute this command at the SNMP command mode. An LX will not generate an SNMP Trap message until a Trap Client is defined. A Trap Client is a specific NOC to which the device sends Trap messages. Up to 16 Trap Clients can be configured.

To add an SNMP Trap client, type the following:

Snmp:0 >>trap client <*number*> *ip_address*

A *number* value is a number from 0 to 15. The *ip_address* identifies the NOC that should receive the Trap messages.

To remove an SNMP Trap client, type the following; for example:

Snmp:0 >>no trap client <number>

SNMP TRAP Client Configuration Examples

Snmp:1 >>trap client 0 <a.b.c.d>

Snmp:1 >>trap client 0 community <string>

Snmp:1 >>trap client 0 udp port <number>

Snmp:1 >>trap client 0 version <v1 | v2c | v2c-inform | v3>

Snmp:1 >>trap client 0 retransmit count 0

Snmp:1 >>trap client 0 retransmit interval 0

Snmp:1 >>no trap client 0

Adding or Removing an SNMP V3 User Entry

Use this command to configure an SNMP V3 user entry. Up to 10 V3 Users can be configured.

To add an SNMP V3 user entry, type the following:

Snmp:0 >>`v3 user <number> user user_name`

A *number* value is a number from 0 to 9. The *user_name* identifies the name of the user.

To remove an SNMP V3 user entry, type the following; for example:

Snmp:0 >>`no v3 user 3`

SNMP V3 User Configuration Examples

Snmp:1 >>`v3 user 3 name bob`

Snmp:1 >>`v3 user 3 authpass <password>`

Snmp:1 >>`v3 user 3 authproto <protocol>`

Snmp:1 >>`v3 user 3 privpass <password>`

Snmp:1 >>`v3 user 3 privproto <protocol>`

Adding or Removing an SNMP V3 Group Entry

Use this command to configure an SNMP V3 group entry. Up to 10 V3 Groups can be configured.

To add an SNMP V3 group entry, type the following:

Snmp:0 >>`v3 group <number> group group_name`

A *number* value is a number from 0 to 9. The *group_name* identifies the name of the group.

To remove an SNMP V3 user entry, type the following; for example:

Snmp:0 >>`no v3 group 3`

SNMP V3 Group Configuration Examples

Snmp:1 >>`v3 group 3 group grpAll`

Snmp:1 >>`v3 group 3 user <name>`

Adding or Removing an SNMP V3 Access Entry

Use this command to configure an SNMP V3 Access entry. Up to 10 V3 Access Entries can be configured.

To add an SNMP V3 Access Entry, type the following:

Snmp:0 >>`v3 access <number> name <string>`

An *number* value is the entry in the access table being configured. The *`string`* identifies the name assigned to the entry.

To remove an SNMP V3 Access Entry, type the following; for example:

Snmp:0 >>`no v3 access 3`

SNMP V3 Access Configuration Examples

Snmp:1 >>`v3 access 3 name grpAll`

Snmp:1 >>`v3 access 3 readview <word>`

Snmp:1 >>`v3 access seclevel <security_level>`

Snmp:1 >>`v3 access 3 writeview <word>`

Adding or Removing an SNMP V3 View Entry

Use this command to configure an SNMP V3 view entry. Up to 10 V3 View Entries can be configured.

To add an SNMP V3 View Entry, type the following:

Snmp:0 >>`v3 view <number> name <string>`

An *number* value is the entry in the view table being configured. The *`string`* identifies the name assigned to the entry.

To remove an SNMP V3 View Entry, type the following; for example:

Snmp:0 >>`no v3 view 3`

SNMP V3 View Configuration Examples

Snmp:1 >>`v3 view 3 name all`

Snmp:1 >>`v3 view 3 mask FF`

Snmp:1 >>`v3 view 3 subtree 1.3.6.1`

Snmp:1 >>`v3 view 3 type included`

MIB-II System Group Configuration

This section describes how to configure the MIB-II sysContact and sysLocation object values. Type the following commands at the CLI SNMP Config prompt.

Snmp:0 >>`contact <string>`

Snmp:0 >>`location <string>`

SNMP V3 Overview

The LX Series supports SNMP V3. The following structures are used to set up an SNMP V3 entity.

User

This is where the user is defined, as well as the security levels to be applied to this user. A two-tier security level is provided for the user: Authentication security and Privilege (communication) security.

Authentication security defines which secure methods used to encrypt the user/password being sent. The options are MD5, SHA-1, or NONE.

Privilege security defines the secure methods used to encrypt the user datagrams being exchanged between the two devices. The options are NONE, DES, or AES128.

You can define a user with any combination of the above. For example, NoAuth/NoPriv defines a user with both encryptions set to none. Auth/noPriv defines a user who can use authentication encryption, but no datagram encryption.

Group

This is an organization of users, and points to various ACCESS entries.

Access

This defines the abilities available to a GROUP that is bound to a particular access entry. Access defines which VIEW from the VIEW table is used to determine READ/WRITE capabilities.

View

This is where you limit what a user can view. You can specify a certain OID; for example, 1.3.6.1. This means as long as the user request attempts to read or write to a value that has 1.3.6.1 beginning the string, they will be able to do so.

Configuration

For SNMP V3 to function properly, an entry must exist in each of the four tables. Your configuration is a logical linking of table entries in the four different tables:

```
USER ---> GROUP---> ACCESS --->VIEW
```

The following sections consist of examples of how to configure the SNMP V3 feature on the LX.

Accessing SNMP Commands

SNMP V3 is in the Configuration Command Mode. To access it, type the following:

Config:0 >>`snmp enable`

Config:0 >>`snmp`

SNMP:0 >>

SNMP V3 Commands

The LX supports SNMP V3. The SNMP V3 commands are:

- monitor/show snmp v3 access
- monitor/show snmp v3 group
- monitor/show snmp v3 misc
- monitor/show snmp v3 user
- monitor/show snmp v3 view
- v3 access <*number*> name
- v3 access <*number*> readview
- v3 access <*number*> seclevel
- v3 access <*number*> writeview
- v3 group <*number*> user authpass
- v3 group <*number*> user authproto
- v3 group <*number*> user name
- v3 group <*number*> user privpass
- v3 group <*number*> user privproto
- v3 view <*number*> mask
- v3 view <*number*> name
- v3 view <*number*> subtree
- v3 view <*number*> type
- v3 user <*number*> privpass <*0xkey*>
- trap client <*number*> v3 user index <*index*>

Configuring SNMP V3 for No Authentication and No Privilege

To configure SNMP V3 for no authentication and no privilege, do the following:

1. Configure user:

   Snmp:0 >>`v3 user 0 name tim`

2. Configure group:

   Snmp:0 >>`v3 group 0 user tim`

   Snmp:0 >>`v3 group 0 group groupall`

3. Configure access:

   Snmp:0 >>`v3 access 0 name groupall`

   Snmp:0 >>`v3 access 0 readview viewall`

   Snmp:0 >>`v3 access 0 writeview viewall`

4. Configure view:

   Snmp:0 >>`v3 view 0 name viewall`

   Snmp:0 >>`v3 view 0 subtree 1.3.6.1`

Configuring SNMP V3 for Authentication Privileges

This is the most secure configuration. To configure SNMP V3 for authentication privileges, do the following:

1. Configure user:

   Snmp:0 >>`v3 user 1 name tim`

2. Configure group:

   Snmp:0 >>`v3 group 1 user tim`

   Snmp:0 >>`v3 group 1 group groupall`

3. Configure access:

   Snmp:0 >>`v3 access 1 name groupall`

   Snmp:0 >>`v3 access 1 readview viewall`

   Snmp:0 >>`v3 access 1 writeview viewall`

4. Configure view:

   Snmp:0 >>`v3 view 1 name viewall`

   Snmp:0 >>`v3 view 1 subtree 1.3.6.1`

5. Configure protocols and passwords:

   Snmp:0 >>`v3 user 1 privproto des`

   Snmp:0 >>`v3 user 1 privpass` *`privpass`*

   Snmp:0 >>`v3 user 1 authproto md5`

   Snmp:0 >>`v3 user 1 authpass` *`authpass`*

Configuring SNMP V3 for Authentication and No Privilege

To configure SNMP V3 for authentication with no privileges, do the following:

1. Access Security Level 1:

   Snmp:0 >>`v3 access 1 seclevel authAndPriv`

2. Configure user:

   Snmp:0 >>`v3 user 2 name tim`

3. Configure group:

   Snmp:0 >>`v3 group 2 user tim`

4. Configure access:

   Snmp:0 >>`v3 access 2 seclevel authNoPriv`

5. Configure group:

   Snmp:0 >>`v3 group 2 group groupall`

6. Configure access:

   Snmp:0 >>v3 access 2 name groupall

   Snmp:0 >>v3 access 2 readview viewall

   Snmp:0 >>v3 access 2 writeview viewall

7. Configure view:

   Snmp:0 >>v3 view 2 name viewauthnopriv

   Snmp:0 >>v3 view 2 subtree 1.3.6.1

8. Configure protocols and password:

   Snmp:0 >>v3 user 2 authproto md5

   Snmp:0 >>v3 user 2 authpass *authpass*

   Snmp:0 >>v3 access 2 seclevel authNoPriv

Configuring SNMP V3 for Read-Only Authentication and Privilege

To configure SNMP V3 for read-only authentication and privileges, do the following:

1. Configure user:

   Snmp:0 >>v3 user 3 name tim

2. Configure group:

   Snmp:0 >>v3 group 3 user tim

   Snmp:0 >>v3 group 3 group groupall

3. Configure access:

   Snmp:0 >>v3 access 3 name groupall

   Snmp:0 >>v3 access 3 readview viewall

4. Configure view:

   Snmp:0 >>v3 view 3 name viewall

   Snmp:0 >>v3 view 3 subtree 1.3.6.1

5. Configure protocols and passwords:

   Snmp:0 >>`v3 user 3 privproto des`

   Snmp:0 >>`v3 user 3 privpass` *`abcd`*

   Snmp:0 >>`v3 user 3 authproto md5`

   Snmp:0 >>`v3 user 3 authpass` *`authpass`*

   Snmp:0 >>`v3 access 3 seclevel authAndPriv`

Configuring a Trap Client User Index

The Trap Client User Index command has been added. The syntax follows:

Snmp:0 >>`trap client <`*`number`*`> v3userindex <`*`number`*`>`

where:

<*number*> is the number of the client.

<*number*> points to the entry in the v3 user table on whose behalf this trap client is configured. The range is from 0 to 9. Note that you need to set this field only if this entry is for a V3 trap client.

Example

Snmp:0 >>`trap client 4 v3userindex 8`

Configuring a V3 User Passw/Priv Key

The V3 UserPassw/Priv Key command has been added. The syntax follows:

Snmp:0 >>`v3 user <`*`number`*`> privpass <`*`password`*`>`

Snmp:0 >>`v3 user <`*`number`*`> privpass <`*`0xkey`*`>`

where:

<*number*> is the index for the user entry being configured.

<*password*> is the alphanumeric privacy password.

<*0xkey*> is the privacy key, in hex format. To indicate that a key value is being entered, the value must begin with "`0x`."The key must be 32 characters or less.

Example

Snmp:0 >> `v3 user 0 privpass mypassword`

Snmp:0 >> `v3 user 0 privpass 0x01020304`

Displaying SNMP Information

The following sections explain how to access the SNMP Show screens.

Show Whether SNMP is Enabled or Disabled

Use the following command to see whether SNMP is enabled or disabled.

In-Reach:0 >>`show system characteristics`

The "SNMP Feature" field (highlighted in the following screen) indicates whether SNMP is enabled or disabled.

```
Name:                          In-Reach  Time:   Sat, 01 Jan 2005 06:01:49 UTC
Serial Number:      00:a0:9c:00:02:b1  Authenticate Image:          Disabled
Location:
Domain Name suffix:
Maximum Number of Async Ports:     34  Internal Modem on Port:            33
Maximum Number of Subscribers:    100  LX Model Type:            LX-4032-101
Maximum Number of Interfaces:      36  Maximum Number of Ethernet Ports:   1
Primary Domain :              0.0.0.0  Secondary Domain :            0.0.0.0
Gateway :                     0.0.0.0  Default TFTP Server : 120.179.169.188
Timed Daemon:                Disabled  TFTP Retries:                       3
NTP   Daemon:                Disabled  TFTP Timeout:                       3
NTP   Server:                 0.0.0.0  NTP Server Alternate:         0.0.0.0
NTP IPv6 Server:                         3ffe:303:11:2222:220:edff:fe4b:fc67
NTP IPv6 Server Alternate:               3ffe:303:11:2222:220:edff:fe4b:fc68
Finger Daemon:               Disabled  Logging Size :                  64000
Telnet Server:                Enabled  Telnet Client:                Enabled
Web Server:                   Enabled  Web Server Port:                   80
Web Server Timeout:                20  Web JceModule:               JsafeJCE
Web Encrypt:                 Disabled  Web Banner:                   Enabled
Subscriber Debug Option:     Disabled  Trigger-Action Debug Option: Disabled
System Debug Option:         Disabled  Flash Debug Option:          Disabled
Minimum Password Length:            0  SSH Daemon:                   Enabled
Rlogin Client:               Disabled  Message Feature:             Disabled
SNMP Feature:                 Enabled
Modem Pool Enabled Serial Ports:
```

Figure 41 - Show System Characteristics Display

Show the SNMP Characteristics

Use the following command to display the SNMP configuration for the LX unit:

In-Reach:0 >>`show snmp characteristics`

Example

In-Reach:0 >>`show snmp characteristics`

```
Time:   Sat, 01 Jan 2005 01:58:49 UTC  Name:                    In-Reach
Debug Logging:               Enabled  Port:                         161
Contact:
Location:
```

Figure 42 - Show SNMP Characteristics Display

Show the SNMP Clients

Use the following command to display the SNMP client information:

In-Reach:0 >>`show snmp client [`*number* `| all]`

A *number* value is any valid client number from 0 to 9.

Example

In-Reach:0 >>`show snmp client all`

```
Get Client:                      1  Address:             140.111.222.111
Version:                        v1  NetMask:             255.255.255.255
Community:                                                       public

Set Client:                      1  Address:             140.111.222.111
Version:                        v1  NetMask:             255.255.255.255
Community:                                                      private

Trap Client:                     1  Address:             140.111.222.111
Version:                        v1  UDP Port:                       162
Community:                                                       public
Retransmit Count:                0  Retransmit Interval:             0
V3 User Index:                   0
```

Figure 43 - Show SNMP Client Display

Show the SNMP V3 Settings

The following sections explain how to access the SNMP V3 Show screens.

Show All SNMP V3 Users

Use the `show snmp v3 user all` command to display information on characteristics at either of the following command modes; for example:

Cluster:0 >>`show snmp v3 user [0 | 1, 2, 3 |all]`

InReach:0 >>`show snmp v3 user [0 | 1, 2, 3 |all]`

Figure 44 shows an example of the SNMP V3 User All Screen.

```
userEntry:                          0
userName:                noauthnopriv
authProtocol:                  none  authPassword:
privProtocol:                  none  privPassword:
status:                        active
userEntry:                          1
userName:                    authpriv
authProtocol:                   md5  authPassword:              authpass
privProtocol:                   des  privPassword:              privpass
status:                        active
userEntry:                          2
userName:                  authnopriv
authProtocol:                   md5  authPassword:              authpass
privProtocol:                  none  privPassword:
status:                     notReady
userEntry:                          3
userName:                  authprivRO
authProtocol:                   md5  authPassword:              authpass
privProtocol:                   des  privPassword:              privpass
 status:                                                         notReady
privPassword (Key):
```

Figure 44 - SNMP V3 User All Screen

Showing All SNMP V3 Access

Use the `snmp v3 access all` command to display information on snmp at either of the following command modes; for example:

Cluster:0 >>`show snmp v3 access all`

InReach:0 >>`show snmp v3 access all`

```
accessEntry:                      0
groupName:         groupnoauthnopriv
secModel:                     usm  secLevel:              noAuthNoPriv
readView:          viewnoauthnopriv  writeView:          viewnoauthnopriv
ctxPrefix:                        ctxMatch:                      exact
status:                      active
accessEntry:                      1
groupName:             groupauthpriv
secModel:                     usm  secLevel:               authAndPriv
readView:              viewauthpriv  writeView:              viewauthpriv
ctxPrefix:                        ctxMatch:                      exact
status:                      active
accessEntry:                      2
groupName:           groupauthnopriv
secModel:                     usm  secLevel:               authNoPriv
readView:            viewauthnopriv  writeView:            viewauthnopriv
ctxPrefix:                        ctxMatch:                      exact
status:                    notReady
accessEntry:                      3
groupName:           groupauthprivRO
secModel:                     usm  secLevel:               authAndPriv
readView:            viewauthprivRO  writeView:
ctxPrefix:                        ctxMatch:                      exact
status:                    notReady
```

Figure 45 - SNMP V3 Access All Screen

Showing All SNMP V3 View

Use the `snmp v3 view all` command to display information on snmp at either of the following command modes; for example:

Cluster:0 >>`show snmp v3 view all`

InReach:0 >>`show snmp v3 view all`

```
viewEntry:                          0
 viewName:            viewnoauthnopriv
 subTree:                  .1.3.6.1  mask:
 type:                    included  status:                    active
 viewEntry:                         1
 viewName:               viewauthpriv
 subTree:                  .1.3.6.1  mask:
 type:                    included  status:                    active
 viewEntry:                         2
 viewName:             viewauthnopriv
 subTree:                  .1.3.6.1  mask:
 type:                    included  status:                  notReady
 viewEntry:                         4
 viewName:             viewauthprivRO
 subTree:                  .1.3.6.1  mask:
 type:                    included  status:                  notReady
```

Figure 46 - SNMP V3 View All Screen

Show the SNMP V3 Access Settings

Use the following command to display the V3 settings for a Version-3 SNMP entry:

In-Reach:0 >>`show snmp v3 access` *`entry_number`*

An *entry_ number* value is any valid SNMP V3 entry number from 0 to 9.

Example

In-Reach:0 >>`show snmp v3 access 0`

```
accessEntry:0
groupName:       grpAll
secModel:        usm        secLevel:     authAndPriv
readView:        all        writeView:    all
ctxPrefix:                  ctxMatch:     exact
status:          active
```

Figure 47 - V3 Access Screen

Show the SNMP V3 Group Settings

Use the following command to display the V3 settings for a Version-3 SNMP group:

In-Reach:0 >>`show snmp v3 group` *`entry_number`*

An *entry_ number* value is any valid SNMP V3 entry number from 0 to 9.

Example

In-Reach:0 >>`show snmp v3 group 0`

```
Entry       secModel     userName      groupName     status
0           usm          bob           grpAll        active
```

Figure 48 - SNMP V3 Group Screen

Show the SNMP V3 Miscellaneous Settings

Use the following command to display miscellaneous SNMP V3 settings:

In-Reach:0 >>`show snmp v3 misc`

Example

In-Reach:0 >>`show snmp v3 misc`

```
EngineId:      800000210100000000
EngineBoots:   1
```

Figure 49 - SNMP V3 Miscellaneous Screen

Show the SNMP V3 User Settings

Use the following command to display the V3 settings for a Version-3 SNMP user:

In-Reach:0 >>`show snmp v3 user`

An *entry_ number* value is any valid SNMP V3 entry number from 0 to 9.

Example

In-Reach:0 >>`show snmp v3 user 0`

```
userEntry:                        0  status:                      active
userName:                                                         bob
authProtocol:                   md5   privProtocol:                des
authPassword:                                                Configured
privPassword (Key):                                          Configured
```

Figure 50 - SNMP V3 User Screen

Show the SNMP V3 View Settings

Use the following command to display the V3 settings for a Version-3 SNMP view:

In-Reach:0 >>`show snmp v3 view` *`entry_number`*

An *entry_ number* value is any valid SNMP V3 entry number from 0 to 9.

Example

In-Reach:0 >>`show snmp v3 view 0`

```
Entry    viewName    subTree     viewMask    viewType    status
0        all         .1.3.6.1    FF          included    active
```

Figure 51 - SNMP V3 View Screen

Dual Power Supply SNMP Traps

The LX now supports SNMP traps to notify you of a Power Supply state change (on/off).

References

- *Understanding SNMP MIBs* - by Dave Perkins, Prentice Hall.
- *The Simple Book*, by Marshall Rose, Prentice Hall.
- RFC 1213, "MIB-II", IETF
- RFC 1902, "Structure of Management Information for Version 2 of SNMP", IETF
- RFC 1903, "Textual Conventions for Version 2 of SNMP", IETF
- RFC 1905, "Protocol Operations for Version 2 of SNMP", IETF
- RFC 1907, "Management Information Base for Version 2 of SNMP", IETF

Chapter 14

Configuring the High Density Alarm Manager (HDAM)

IMPORTANT

The IR-7104 HDAM is compatible only with the LX-Series. It is no longer compatible with In-Reach legacy products.

This chapter describes how to configure the IR-7104 and Option Modules.

Configuring the IR-7104

The configuration tasks for the IR-7104 include the following:

- Configuring the HDAM port
- Updating the IR-7104 Firmware
- Rebooting the IR-7104

Configuring the HDAM Port

The IR-7104 and Option Modules are managed from a port on the LX Master Unit that is configured as an HDAM port. All ports on an LX-Series unit other than port 0 (diagnostic/management port) can be configured as HDAM ports. Only four total ports can be HDAM ports at one time.

Use the following command to configure ports as HDAM ports:

Config:0 >>`port async <port_number> access hdam`

Where	Means
port_number	Specifies the port you want to use to control the HDAM. You can use any LX-Series port other than port 0 (diagnostic/ management port).

Press <RETURN> to configure the port as an HDAM port.

Example

```
Config:0 >>port async 6 access hdam
```

Updating the IR-7104 Firmware

Use this command to launch an attempt to update the firmware on the 7104 connected to a specific HDAM port. The LX attempts to download the `hdam.img` file and copy it into 7104 flash memory. Use the following commands to update the IR-7104 firmware:

`hdam <port_number> update <ip_address>|<domain_name>`

`hdam <port_number> update`

Where	Means
port_number	The number of the LX port connected to the HDAM on which you want to update firmware. For example, a value of 5 means that the IR-7104 connected to port 5 of the Master LX Unit will have its firmware updated.
ip_address	Specifies the IP address of the TFTP server from which the firmware update will be obtained. If no IP address is given, the LX unit's default TFTP server address is used.
domain_name	Specifies the domain name of the TFTP server from which the firmware update will be obtained. If no domain name is given, the LX unit's default TFTP server address is used.

The IR-7104 reboots automatically after the firmware is successfully updated. This ensures that the updated firmware will take effect immediately.

Example

```
hdam 5 update 130.155.110.55
hdam 28 update local_host_foo
```

Rebooting the IR-7104

Use the following command to reboot the IR-7104:

`hdam <port_number> reset`

Where	Means
port_number	Specifies one HDAM port. The IR-7104 unit that is managed from this HDAM port will be rebooted. For example, a value of 5 means that the IR-7104 connected to port 5 of the Master LX Unit will be rebooted.

Example

```
Config:0 >>hdam 5 reset
```

Using the Alarm Input Commands

This section explains how to configure the alarm input commands, including the following:

- Naming Alarm Inputs
- Enabling and Disabling Audible Alarms
- Configuring an Alarm Input Description String
- Configuring an Alarm Input Default Description
- Renaming an Alarm Input
- Configuring the Debounce Interval for an Alarm
- Configuring the Fault State for Alarm Inputs
- Configuring a Severity Level for Alarm Inputs
- Defaulting a Single Named Alarm

- Resetting the Alarm Input Name to the Default
- Resetting Alarm Inputs to the Defaults

Naming Alarm Inputs

NOTE: You can use each point name once on the LX. You cannot use the same name on multiple ports, slots, or points.

The default name for an alarm input is canonically derived from the port number, slot number and point number. For example, the default name for the 8th alarm input on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.

You can configure by the default name (if known), or by the physical location on the HDAM (see examples below).

You can configure a descriptive name (all names across the Master LX Unit must be unique) for any Alarm Input in the IR-7104 by issuing the following Privileged command:

`hdam alarm <alarm_name_1> name <alarm_name_2>`

`hdam alarm port <port_number> slot <slot_number> point <point_number> name <new_name>`

Where	Means
alarm_name_1	The name of the alarm input you want to rename.
alarm_name_2	The new alarm name you want to assign to the alarm input. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.
port_number	Specifies the individual LX port number to which the IR-7104 is attached.
slot_number	Specifies a specific Slot for which you want to configure a name.

point_number	Specifies a specific Points for which you want to configure a name.
new_name	The new name for the point.

Example

Config:0 >>hdam alarm 5_4_20 name BankVaultDoor

Config:0 >>hdam alarm port 5 slot 4 point 20 name BankVaultDoor

InReach:0 >>config hdam alarm port 5 slot 4 point 20 name BankVaultDoor

Enabling and Disabling Audible Alarms

Use the following commands to enable and disable the audible alarm for a specific alarm, or to configure the audible alarm for multiple alarms:

hdam alarm <*alarm_name*> audible enable

hdam alarm <*alarm_name*> no audible

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] audible enable

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] no audible

Where	Means
alarm_name	The name of the alarm on which you want to enable/disable the audible alarm. This entry is in the order port_slot_alarm (e.g., 5_2_31, or BankVaultDoor).
enable	The Audible Alarm will sound when a fault condition is detected on an Alarm Input of an IR-7104 unit specified in *alarm_name*.
no audible	The Audible Alarm will *not* sound when a fault condition is detected on an Alarm Input of an IR-7104 unit specified in *alarm_name*. This is the default setting.
port_number	Specifies the HDAM port managing the IR-7104.

slot_list	Specifies a list of Slots on which you want to enable the audible alarm. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4).
point_list	Specifies a list of Points on which you want to enable the audible alarm. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-32)
all	Specifies that all Alarm Inputs managed by the LX Master Unit will be as specified in this command.

Examples

Config:0 >>hdam alarm BankVaultDoor audible enable

Config:0 >>hdam alarm 5_2_31 no audible

Config:0 >>hdam alarm port 2 slot 1,2 point 1,2,3,4 no audible

Config:0 >>hdam alarm port 2 slot 1-20 point 6-18 no audible

Config:0 >>hdam alarm port 2 slot all point all audible enable

Config:0 >>hdam alarm port 2 slot 1-20 point 6-18 audible enable

Configuring an Alarm Input Description String

Use the following commands to configure an Alarm Description String for a specific alarm, or to configure an Alarm Description String for multiple alarms:

hdam alarm <*alarm_name*> description <*string*>

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] description <*string*>

Where	Means
alarm_name	Specifies an Alarm Input Name. The default name for an alarm input or control output is canonically derived from the port number, slot number and point number. For example, the default name for the 31st control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_31.

port_number	Specifies the HDAM port managing the 7104.
slot_list	Specifies a list of Slots on which you want to configure a description string. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points on which you want to configure a description string. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-32), or a combination.
all	Specifies that all Slots or Points managed by the LX Master Unit will be as specified in this command.
string	The description of the alarm input (a maximum of 63 characters long).

Examples

Config:0 >>hdam alarm 5_4_8 description lab door 1

Config:0 >>hdam alarm 3_1_8 description lab door 2

Config:0 >>hdam alarm port 2 slot 1,2 point 1-4 description lab1

Config:0 >>hdam alarm port 2 slot all point all description library second floor

Defaulting the Description for an Alarm Input

Use the following commands to default an Alarm Input Description for a specific alarm or for multiple alarms:

hdam alarm <*alarm_name*> default description

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] default description

Where	Means
alarm_name	Specifies an Alarm Input Name. The default name for an alarm input or control output is canonically derived from the port number, slot number and point number. For example, the default name for the 31st control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_31.
port_number	Specifies the HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to configure a description for. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points for which you want to configure a description. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	Specifies that all Slots or Points managed by the LX Master Unit will be as specified in this command.

Examples

Config:0 >>`hdam alarm 5_4_8 default description`

Config:0 >>`hdam alarm 3_1_8 default description`

Config:0 >>`hdam alarm port 2 slot 1,2 point 1-4 default description`

Config:0 >>`hdam alarm port 2 slot all point all default description`

Renaming an Alarm Input

Use the following command to rename a given alarm, or to configure a name for an Alarm Input:

`hdam alarm <`*`alarm_name`*`> name <`*`new_name`*

`hdam alarm port <`*`port_number`*`> slot <`*`slot_number`*`> point <`*`point_number`*`> name <`*`new_name`*`>`

Where	Means
alarm_name	The name of the alarm you want to rename.
new_name	The new alarm name you want to assign to alarm name 1. The name must be unique across the Master LX Unit. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.
port_number	Specifies the HDAM port managing the 7104.
slot_number	Specifies the number of the slot on whose point you want to give the new name.
point_number	Specifies the number of the point you want to give the new name.

Examples

Config:0 >>hdam alarm BankVaultDoor name SafedepositDoor

Config:0 >>hdam alarm 5_2_31 name AuxACDown

Config:0 >>hdam alarm port 2 slot 1 point 1 name lab1

Config:0 >>hdam alarm port 2 slot 4 point 18 name library

NOTE: You cannot list multiple slots or points, because point names must be unique.

Enabling and Disabling SNMP Traps for Alarm State Changes

Use the following commands to enable or disable the sending of an SNMP trap for a change in Alarm states for a specific alarm or for multiple alarms:

hdam alarm <*alarm_name*> trap enable

hdam alarm <*alarm_name*> no trap

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] trap enable

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] no trap

Where	Means
alarm_name	Specifies an Alarm Input Name. The value of *name* can be a descriptive name or a default name.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points about which you want to send SNMP traps. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points about which you want to send SNMP traps. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	Specifies that Slots or Points managed by the LX Master Unit will be as specified in this command.
trap enable	This is the default setting. An SNMP trap will be sent when the Alarm Input specified changes state.

Examples

```
Config:0 >>hdam alarm SafedepositDoor trap enable
Config:0 >>hdam alarm 5_2_31 no trap
Config:0 >>hdam alarm port 2 slot all point all trap enable
Config:0 >>hdam alarm port 2 slot 1-3 point 1,2,6-18 trap enable
Config:0 >>hdam alarm port 2 slot all point 6-18 no trap
```

Configuring the Debounce Interval for an Alarm

An Alarm Input can be configured to stop receiving alarms for up to 1800 seconds after an alarm comes in. The period during which the Alarm Input does not receive alarms is called the "debounce interval". For example, if you have a door with a timer attached with a debounce setting of 5 seconds, and the door stays open more than 5 seconds after opening, an alarm message is sent. If the door closes within 5 seconds, no alarm message is sent and everything appears normal. Use the following command to configure the debounce interval for an Alarm Input:

```
hdam alarm <alarm_name> debounce <time>

hdam alarm port <port_number> slot [<slot_list>|all] point [<point_list>|all]
debounce <time>
```

Where	Means
alarm_name	Specifies an Alarm Input Name. The value of *name* can be a descriptive name or a default name.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots on which you want to set the debounce interval. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points on which you want to set the debounce interval. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	The debounce interval specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.
time	Specifies the debounce interval, in seconds. The allowable values are 0 - 1800 seconds. The default value is 0.

Examples

Config:0 >>`hdam alarm 5_2_31 debounce 30`

Config:0 >>`hdam alarm port 2 slot 1-4 point 1,2,6-18 debounce 45`

Configuring the Fault State for Alarm Inputs

Use the following commands to configure the fault state for Alarm Inputs for a specific alarm or for multiple alarms:

```
hdam alarm <alarm_name> fault state [open|closed]

hdam alarm port <port_number> slot [<slot_list>|all] point [<point_list>|all]
fault state [open|closed]
```

Where	Means
alarm_name	Specifies an Alarm Input Name. The value of *name* can be a descriptive name or a default name.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots on whose points you want to change the fault state. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or combination.
point_list	Specifies a list of Points on which you want to change the fault state. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	The fault state specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.
open	The point will be in Alarm when it is open. This is the default setting.
closed	The point will be in Alarm when it is closed.

Examples

Config:0 >>`hdam alarm SafedepositDoor fault state open`

Config:0 >>`hdam alarm 5_2_31 fault state closed`

Config:0 >>`hdam alarm port 2 slot 1,2 point 1,2,3,4 fault state open`

Config:0 >>`hdam alarm port 2 slot 1-4 point 6-18 fault state closed`

Configuring a Severity Level for Alarm Inputs

Use the following commands to configure a Severity Level for Alarm Inputs for a specific alarm or for multiple alarms:

`hdam alarm <`*`alarm_name`*`> trap severity <`*`severity_level`*`>`

`hdam alarm port <`*`port_number`*`> slot [<`*`slot_list`*`>|all] point [<`*`point_list`*`>|all] trap severity <`*`severity_level`*`>`

Where	Means
name	Specifies an Alarm Input Name. The value of *name* can be a descriptive name or a default name.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to set trap severity on. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points on which you want to set trap severity. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	The fault severity specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.
severity_level	The SNMP Trap Severity Level used when SNMP Traps are sent for faults detected by the specified Alarm Inputs. The allowable values are Information, Warning, Minor, Major, and Critical. The default value is Minor.

Examples

```
Config:0 >>hdam alarm SafedepositDoor trap severity critical
Config:0 >>hdam alarm 5_2_31 trap severity information
Config:0 >>hdam alarm port 2 slot 1,2 point 1,2,3,4 trap severity minor
Config:0 >>hdam alarm port 2 slot 1-4 point 6-18 trap severity major
```

Defaulting a Single Named Alarm

Use the following command to default a single named alarm:

```
hdam alarm <alarm_name> default point
```

Where	Means
alarm_name	The name of the alarm you want to default. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.

Examples

Config:0 >>hdam alarm BankVaultDoor default point

Config:0 >>hdam alarm 3_1_22 default point

Resetting the Alarm Input Name to its Default

Use the following commands to reset alarm inputs to their default names for a specific alarm or for multiple alarms:

hdam alarm <*alarm_name*> default name

hdam alarm port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] default name

Where	Means
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to reset to the default name. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points you want to reset to the default name. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-32), or a combination.
all	The default names specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

Config:0 >>hdam alarm port 2 slot 1,2 point 1,2,3,4 default name

Config:0 >>hdam alarm port 2 slot 1-4 point 6-18 default name

Config:0 >>hdam alarm port 2 slot all point all default name

Config:0 >>hdam alarm port 2 slot 1-4 point 6-18 default name

Config:0 >>hdam alarm fan_window default name

Resetting Alarm Inputs to the Defaults

Use the following command to reset alarm inputs to the default settings:

`hdam alarm port <port_number> slot [<slot_list>|all] point [<point_list>|all] default point`

Where	Means
port_number	Specifies the HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to default. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points you want to default. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-32`), or a combination.
all	The default settings specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

Config:0 >>`hdam alarm port 2 slot 1,2 point 1,2,3,4 default point`

Config:0 >>`hdam alarm port 2 slot 1-4 point 6-18 default point`

Config:0 >>`hdam alarm port 2 slot all point all default point`

Config:0 >>`hdam alarm port 2 slot 1-4 point 6-18 default point`

Using the Control Output Commands

This section explains how to configure the control output commands, including the following:

- Naming Control Outputs
- Configuring a Control Output Name as Opened or Closed
- Configuring a Control Output Description String
- Configuring a Control Output Default Description

- Configuring a Name for a Control Output
- Setting the Active State of a Named Control
- Configuring the Default Point for a Named Control Output
- Resetting Control Outputs to Default Settings

Naming Control Outputs

The default name for a control output is canonically derived from the port number, slot number and point number. For example, the default name for the 8th control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.

You can configure by the default name (if known), or by the physical location on the HDAM (see examples below).

You can configure a descriptive name for any Control Output in the IR-7104 by issuing the following Privileged command:

`hdam control <control_name_1> name <control_name_2>`

Where	Means
control_name_1	Specifies that the point being named is a Control Output.
control_name_2	The new control name you want to assign to the control output. The names must be unique across the Master LX Unit. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.

Example

Config:0 >>`hdam control 3_1_8 name AuxACUnitON`

Configuring Control Output Name as Open or Closed

Use the following commands to configure IR-7104 Control Output signals as Open or Closed for a specific control or for multiple controls:

`hdam control <control_name> set [open|closed]`

```
hdam control port <port_number> slot [<slot_list>|all] point
[<point_list>|all] set [open|closed]
```

Where	Means
port_number	The number of the port to which the HDAM is connected.
control_name	Specifies a Control Output Name. The default name for an alarm input or control output is canonically derived from the port number, slot number and point number. For example, the default name for the 8th control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.
slot_list	The list of the slots whose points you want to configure as open or closed. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	The list of the points whose state you want to set open or closed. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-8`), or a combination.
`open|closed`	Set the specified Control Output signals to Open|Closed. Closed is the default setting.

Examples

```
Config:0 >>hdam control 5_4_8 set open
Config:0 >>hdam control 3_1_8 set closed
Config:0 >>hdam control port 2 slot all point 1-4 set open
```

Configuring a Control Output Description String

Use the following commands to configure a Control Output Description String for a specific control or for multiple controls:

```
hdam control <control_name> description <string>
```

```
hdam control port <port_number> slot [<slot_list>|all] point
[<point_list>|all] description <string>
```

Where	Means
control_name	Specifies a Control Output Name. The default name for an alarm input or control output is canonically derived from the port number, slot number and point number. For example, the default name for the 8th control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to configure a description for. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points you want to configure a description for. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-8`), or a combination.
all	Specifies that all Slot or control outputs managed by the LX Master Unit will be as specified in this command.
string	The description of the control output (a maximum of 63 characters long).

Examples

```
Config:0 >>hdam control Floor2Lab description lab door 1
Config:0 >>hdam control 3_1_8 description lab door 2
Config:0 >>hdam control port 2 slot 1,2 point 1-4 description lab1
Config:0 >>hdam control port 2 slot all point all description library
second floor
```

Configuring a Control Output Default Description

Use the following commands to configure a Control Output Description for a specific control or for multiple controls:

```
hdam control <control_name> description

hdam control port <port_number> slot [<slot_list>|all] point
[<point_list>|all] description
```

Where	Means
control_name	Specifies a Control Output Name. The default name for an alarm input or control output is canonically derived from the port number, slot number and point number. For example, the default name for the 8th control output on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.
port_number	Specifies the HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to configure a description for. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points for which you want to configure a description. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-8`), or a combination.
all	Specifies that all Slot or control outputs managed by the LX Master Unit will be as specified in this command.

Examples

```
Config:0 >>hdam control Temp_AC default description
Config:0 >>hdam control 3_1_8 default description
Config:0 >>hdam control port 2 slot 1,2 point 1-4 default description
Config:0 >>hdam control port 2 slot all point all default description
```

Configuring a Name for a Control Output

Use the following commands to configure a name for a Control Output for a specific control or for multiple controls:

```
hdam control <control_name_1> name <control_name_2>
```

```
hdam control port <port_number> slot <slot_number> point <point_number>
name <new_name>
```

Where	Means
control_name_1	The name of the control output you want to rename.

control_name_2	The new control output name. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.
port_number	Specifies the HDAM port managing the 7104.
slot_number	Specifies a specific Slot whose point you want to give a new name.
point_number	Specifies a specific Point to which you want to give a new name.
new_name	The unique name of the control output.

NOTE: You cannot list multiple slots or points, because point names must be unique across the Master LX Unit.

Examples

```
Config:0 >>hdam control 5_2_31 name DoorAlarm
Config:0 >>hdam control DoorAlarm name AuxACDown
Config:0 >>hdam control port 2 slot 1 point 1 name lab1
Config:0 >>hdam control port 2 slot 4 point 8 name library
```

Setting the Active State of a Named Control

Use the following commands to set the active state of a named control to open or closed, or to set the active state of one or more control outputs to open or closed:

```
hdam control <control_name> active state [open|closed]
```

```
hdam control port <port_number> slot [<slot_list>|all] point
[<point_list>|all] active state [open|closed]
```

Where	Means
control_name	The name of the control output whose active state you want to set open or closed.
port_number	Specifies the HDAM port managing the 7104.

slot_list	Specifies a list of Slots whose points you want to configure as open or closed. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points whose active state you want to set open or closed. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	The Active State specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

Config:0 >>hdam control AuxAcDown active state open

Config:0 >>hdam control 5_2_8 active state closed

Config:0 >>hdam control port 2 slot 4 point 5 active state open

Config:0 >>hdam control port 2 slot 5 point 5-8 active state closed

Configuring the Default Point for a Named Control Output

Use the following command to default a named control output, or to reset a range of control outputs to their defaults:

hdam control <*control_name*> default point

hdam control port <*port_number*> slot <*slot_list*>|all point <*point_list*>|all default point

Where	Means
control_name	The name of the control output you want to default.
port_number	Specifies the HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to reset to defaults. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points you want to reset to defaults. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.

all	The defaults specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

```
Config:0 >>hdam control AuxAcDown default point
Config:0 >>hdam control 6_1_8 default point
Config:0 >>hdam control port 2 slot 1,2 point 1,2,3,4 default point
Config:0 >>hdam control port 2 slot 1-4 point 6-8 default point
Config:0 >>hdam control port 2 slot all point all default point
Config:0 >>hdam control port 2 slot 1-4 point 6-8 default point
```

Resetting Control Outputs to Default Settings

Use the following commands to reset control outputs to their defaults for a specific control or for multiple controls:

`hdam control <control_name> default name`

`hdam control port <port_number> slot [<slot_list>|all] point [<point_list>|all] default name`

Where	Means
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to reset to the default name. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-4`), or a combination.
point_list	Specifies a list of Points you want to reset to the default name. The list can contain single items (e.g., `1,3,4`) or ranges (e.g., `1-8`), or a combination.
all	The defaults specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

```
Config:0 >>hdam control port 2 slot 1,2 point 1,2,3,4 default name
```

```
Config:0 >>hdam control port 2 slot 1-4 point 6-8 default name
Config:0 >>hdam control port 2 slot all point all default name
Config:0 >>hdam control Door_Sign default name
```

Using the Analog Input Commands

This section explains how to configure the analog input commands, including the following:

- Naming Analog Inputs
- Configuring an Analog Input Description String
- Resetting Analog Inputs to the Defaults
- Resetting the Analog Input Name to Its Default
- Enabling and Disabling Analog Input
- Configuring Analog Calibration

Naming Analog Inputs

NOTE: You can use each point name once on the LX. You cannot use the same name on multiple ports, slots, or points.

The default name for an analog input is canonically derived from the port number, slot number and point number. For example, the default name for the 8th analog input on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.

You can configure by the default name (if known), or by the physical location on the HDAM (see examples below).

You can configure a descriptive name (all names across the Master LX Unit must be unique) for any analog input in the IR-7104 by issuing the following Privileged command:

```
hdam analog <analog_name> name <new_name>
```

```
hdam analog port <port_number> slot <slot_number> point
<point_number> name <new_name>
```

Where	Means
analog_name	The name of the analog input you want to rename.
new_name	The new analog name you want to assign to the analog input. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.
port_number	Specifies the individual LX port number to which the IR-7104 is attached.
slot_number	Specifies a specific Slot for which you want to configure a name.
point_number	Specifies a specific Point for which you want to configure a name.

Example

Config:0 >>`hdam analog 5_4_8 name BankVaultDoor`

Config:0 >>`hdam analog port 5 slot 4 point 8 name BankVaultDoor`

InReach:0 >>`config hdam analog port 5 slot 4 point 8 name BankVaultDoor`

Configuring an Analog Input Description String

Use the following commands to configure an Analog Input Description String:

`hdam analog <analog_name> description <string>`

`hdam analog port <port_number> slot [<slot_list>|all] point [<point_list>|all] description <string>`

Where	Means
analog_name	Specifies an Analog Input Name. The default name for an analog input is canonically derived from the port number, slot number and point number. For example, the default name for the 8th analog input on the 2nd slot of the HDAM being managed by port 5 is 5_2_8.
port_number	Specifies the HDAM port managing the 7104.

slot_list	Specifies a list of Slots on which you want to configure a description string. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points on which you want to configure a description string. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	Specifies that all Slots or Points managed by the LX Master Unit will be as specified in this command.
string	The description of the analog input (a maximum of 63 characters long).

Examples

Config:0 >>hdam analog 5_4_8 description lab door 1

Config:0 >>hdam analog 3_1_8 description lab door 2

Config:0 >>hdam analog port 2 slot 1,2 point 1-4 description lab1

Config:0 >>hdam analog port 2 slot all point all description library second floor

Resetting Analog Inputs to the Defaults

Use the following commands to reset analog inputs to the default settings:

hdam analog <*analog_name*> default point

hdam analog port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] default point

Where	Means
analog_name	Specifies an Analog Input Name. The name of the analog input you want to default. The name must start with a letter, and the remainder of the name can contain only letters and/or numbers and/or underscores.
port_number	Specifies the HDAM port managing the 7104.

slot_list	Specifies a list of Slots whose points you want to default. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points you want to default. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	The default settings specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

```
Config:0 >>hdam analog BankVaultDoor default point
Config:0 >>hdam analog 3_1_8 default point
Config:0 >>hdam analog port 2 slot 1,2 point 1,2,3,4 default point
Config:0 >>hdam analog port 2 slot 1-4 point 6-8 default point
Config:0 >>hdam analog port 2 slot all point all default point
```

Resetting the Analog Input Name to Its Default

Use the following commands to reset analog inputs to their respective default names:

hdam analog <*analog_name*> default name

hdam analog port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] default name

Where	Means
analog_name	The name of the analog input you want to reset to the default name.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots whose points you want to reset to the default name. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.

point_list	Specifies a list of Points you want to reset to the default name. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	The default names specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

Config:0 >>hdam analog port 2 slot 1,2 point 1,2,3,4 default name

Config:0 >>hdam analog port 2 slot 1-4 point 6-8 default name

Config:0 >>hdam analog port 2 slot all point all default name

Config:0 >>hdam analog fan_window default name

Enabling and Disabling the Analog State

Use the following commands to configure the state of analog inputs:

hdam analog <*analog_name*> state [enable|disable]

hdam analog port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] state [enable|disable]

Where	Means
analog_name	The name of the analog input on which you want to change the state.
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots on whose points you want to enable the state. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points on which you want to enable the state. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	The default names specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.

Examples

Config:0 >>hdam analog port 2 slot 1,2 point 1,2,3,4 state enable

Config:0 >>hdam analog port 2 slot 1-4 point 6-8 state enable

Config:0 >>hdam analog port 2 slot all point all state disable

Config:0 >>hdam analog fan_window state enable

Configuring Analog Calibration

Use the following commands to calibrate analog inputs:

hdam analog <*analog_name*> calibrate minimum <*minimum_value*> maximum <*maximum_value*> units <*unit_name_string*> [margin <*margin_value*>]

hdam analog port <*port_number*> slot [<*slot_list*>|all] point [<*point_list*>|all] calibrate minimum <*minimum_value*> maximum <*maximum_value*> units <*unit_name_string*> [margin <*margin_value*>]

Where	Means
analog_name	The name of the analog input you want to calibrate .
port_number	Specifies the LX HDAM port managing the 7104.
slot_list	Specifies a list of Slots on whose points you want to calibrate values. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-4), or a combination.
point_list	Specifies a list of Points on which you want to calibrate values. The list can contain single items (e.g., 1,3,4) or ranges (e.g., 1-8), or a combination.
all	The default names specified in this command will apply to all Slots or Points (or both) managed by this LX Master Unit.
minimum_value	The minimum calibration setting. The range is -9999.9999 to 9999.9999. **Refer to your Sensor documentation for this information.**
maximum_value	The maximum calibration setting. The range is -9999.9999 to 9999.9999. **Refer to your Sensor documentation for this information.**

unit_name_string	The string representing the attached sensor's native units. For example, "DegF" or "DegC" for a temperature sensor. This can be up to 8 characters long.
margin_value	Indicates the optional margin value. The range is -9999.9999 to 9999.9999.

Examples

Config:0 >>hdam analog 5_2_8 calibrate minimum 5 maximum 140 units DegF

Config:0 >>hdam analog 5_2_7 calibrate minimum 5 maximum 95 units %RH

Config:0 >>hdam analog port 2 slot 1,2 point 1,2,3,4 calibrate minimum 20.8 maximum 32.0 units Hg

Config:0 >>hdam analog port 2 slot 3-4 point 6-8 calibrate minimum 5 maximum 140 units TempF margin 1.2

Sending a User-generated Message to the LCD Panel

Use the following command to send a message to the LCD Panel of the IR-7104:

hdam <*port_number*> banner <*string*>

Where	Means
port_number	Specifies one HDAM port. The IR-7104 unit that is managed from this port will display the given string.
string	Specifies the message text that is to be displayed on the LCD Panel of the IR-7104. The maximum size of the message is 32 characters.

The contents of *string* will be displayed on the LCD Panel of the IR-7104 when all alarm notices have been cleared.

In the following example, the message PUSH MASTER ALARM CLEAR SWITCH is displayed on the LCD Panel of the IR-7104 that is attached to port 6. Use this to set your own banner, if necessary.

Example

Config:0 >>hdam 5 banner PUSH MASTER ALARM CLEAR SWITCH

Setting the Banner on the LCD Panel to Defaults

Use the following command to set the banner on the LCD Panel of the IR-7104 to defaults:

`hdam <port_number> default banner`

Where	Means
port_number	Specifies the HDAM port. The IR-7104 unit that is managed from this port will display the default banner.

Example

Config:0 >>`hdam 5 default banner`

Displaying HDAM Information

This section explains how to display HDAM show screens.

Viewing HDAM Alarm Input Characteristics Using the Alarm Name

Use the `show hdam alarm <alarm_name> characteristics` command to display alarm characteristics using a specific alarm name; for example:

Config:0 >>`show hdam alarm 5_4_20 characteristics`

InReach:0 >>`show hdam alarm 5_2_31 characteristics`

Figure 52 shows an example of the HDAM Alarm Name Characteristics Screen.

```
                                                    Fault  Debounce   Trap     Trap
Port Slot Point       Name          Audible         State  Interval   Setting  Severity

 1    2    5          8_2_5         Disabled        Open   3          Enabled  Minor
   Description:
```

Figure 52 - HDAM Alarm Name Characteristics Screen

Use the `show hdam alarm <alarm_name> status` command to display alarm status information using a specific alarm name at either of the following command modes; for example:

Config:0 >>`show hdam alarm 5_4_20 status`

InReach:0 >>`show hdam alarm 5_2_31 status`

Figure 53 shows an example of the HDAM Alarm Name Status Screen

```
                                        Current    Fired    Last Time
Port Slot Point       Name              State      Count    Fired

1     2     5         8_2_5             Faulted    5        Wed,20 Oct 2004 11:47:24 UTC
```

Figure 53 - HDAM Alarm Name Status Screen

Viewing HDAM Port Characteristics Information

Use the `show hdam <port_number> characteristics` command to display alarm and analog input, and control output characteristics at either of the following command modes; for example:

Config:0 >>`show hdam 4 characteristics`

InReach:0 >>`show hdam 1 characteristics`

Figure 54 shows an example of the HDAM Port Characteristics Screen.

```
Time:                                        Thu, 21 Oct 2004 09:10:18 UTC
Device Number:                      8  Firmware:                    V2.0.B6
Banner:                                       HDAM 7104 Series SW Ver. 2.0
Number of Resets:                   1
Slot  Type      Points
 1    Control     8
 2    Alarm       32
 3    Alarm       32
 4    Sensor      8

Port Slot Point   Name                                Active State

 1    1     1     8_1_1                               Opened
Description:

 1    1     2     8_1_2                               Opened
Description:

 1    1     3     8_1_3                               Opened
Description:

 1    1     4     8_1_4                               Opened
Description:

                                          Fault    Debounce  Trap     Trap
Port Slot Point                  Audible  State    Interval  Setting  Severity

 1    2     1    labdoor          Disabled  Open      3        Enabled  Informational
Description:

 1    2     2    8_2_2            Disabled  Closed    3        Enabled  Informational
Description:

 1    2     3    8_2_3            Disabled  Open      3        Enabled  Minor
Description:      this point is on port 8 slot 2 point 3 for my cellar door
Type a key to continue, q to quit.
```

Figure 54 - HDAM Port Characteristics Screen

Viewing HDAM Control Name Information

Use the `show hdam control <control_name> characteristics` command to display control output characteristics using a specific control name at either of the following command modes; for example:

Config:0 >>`show hdam control 5_4_8 characteristics`

InReach:0 >>`show hdam control 5_2_8 characteristics`

Figure 55 shows an example of the HDAM Control Name Characteristics Screen.

```
Port Slot Point        Name                                  Active State

 1    1     5          8_1_5                                 Opened
Description:
```

Figure 55 - HDAM Control Name Characteristics Screen

Use the `show hdam control <control_name> status` command to display information for control outputs using a specific control name at either of the following command modes; for example:

Config:0 >>`show hdam control 5_4_8 status`

InReach:0 >>`show hdam control 5_2_8 status`

Figure 56 shows an example of the HDAM Control Name Status Screen.

```
                                                      Current   Operational
Port Slot Point        Name                           State     State

 1    1     5          8_1_5                          Opened    On
```

Figure 56 - HDAM Control Name Status Screen

Viewing HDAM Analog Input Characteristics Using the Analog Name

Use the `show hdam analog <analog_name> characteristics` command to display analog characteristics using a specific analog name; for example:

Config:0 >>`show hdam analog 10_1_1 characteristics`

InReach:0 >>`show hdam analog 10_1_1 characteristics`

Figure 57 shows an example of the HDAM Analog Name Characteristics Screen.

```
Port Slot Point   Name            State          Min        Max         Margin     Units

 10   1    1      OfficeTemp      Enabled        5.0000     140.0000    1.0000     TempinF
Description:
```

Figure 57 - HDAM Analog Name Characteristics Screen

Use the `show hdam analog <analog_name> status` command to display analog status information using a specific analog name at either of the following command modes; for example:

Config:0 >>`show hdam analog 5_4_8 status`

InReach:0 >>`show hdam analog 10_1_8 status`

Figure 58 shows an example of the HDAM Analog Name Status Screen.

```
Port Slot Point    Name                            Native Units Value      MilliAmp Value

 10   1    8       TemperatureInMyOfficeWithEWSRH  83.4203   TempinF       13.2942   mA
```

Figure 58 - HDAM Analog Name Status Screen

Viewing HDAM Mapping Information

Use the `show hdam mapping all|<port_name>` command to display mapping information on HDAM ports at either of the following command modes; for example:

Config:0 >>`show hdam mapping 5_2_31`

InReach:0 >>`show hdam mapping all`

Figure 59 shows an example of the HDAM Mapping Screen.

```
Name                                Port  Slot  Point

8_1_1                                8     1     1
8_1_2                                8     1     2
8_1_3                                8     1     3
8_1_4                                8     1     4
8_1_5                                8     1     5
8_1_6                                8     1     6
8_1_7                                8     1     7
8_1_8                                8     1     8
```

Figure 59 - HDAM Mapping Screen

Viewing HDAM Port/Slot/Point Characteristics

Use the `show hdam <port_number> slot <slot_list> point <point_list> characteristics` command to display alarm, analog, and/or control characteristics on HDAM ports at either of the following command modes; for example:

Config:0 >>`show hdam 6 slot 6 point 12 characteristics`

InReach:0 >>`show hdam 8 slot 1 point 1-6 characteristics`

Figure 60 shows an example of the HDAM Port/Slot/Point Characteristics Screen, if Slot 1 contains a Control Card.

```
Port Slot Point       Name                                Active State

1     1     1         8_1_1                               Opened
Description:

1     1     2         8_1_2                               Opened
Description:

1     1     3         8_1_3                               Opened
Description:

1     1     4         8_1_4                               Opened
Description:

1     1     5         8_1_5                               Opened
Description:

1     1     6         8_1_6                               Opened
Description:
```

Figure 60 - HDAM Port/Slot/Point Characteristics Control Card Screen

Figure 61 shows an example of the HDAM Port/Slot/Point Characteristics Screen, if Slot 2 contains an Alarm Card.

```
                                          Fault   Debounce  Trap     Trap
Port Slot   Point      Name       Audible   State   Interval  Setting  Severity

1     2     3          8_2_3      Disabled  Open    3         Enabled  Minor
Description:      this point is on port 8 slot 2 point 3 for my cellar door

1     2     4          8_2_4      Disabled  Open    3         Enabled  Minor
Description:

1     2     5          8_2_5      Disabled  Open    3         Enabled  Minor
Description:

1     2     6          8_2_6      Disabled  Open    3         Enabled  Minor
Description:

1     2     7          8_2_7      Disabled  Open    3         Enabled  Minor
Description:
```

Figure 61 - HDAM Port/Slot/Point Characteristics Alarm Card Screen

Figure 62 shows an example of the HDAM Port/Slot/Point Characteristics Screen, if Slot 1 contains an Analog Card

```
Port Slot Point   Name             State       Minimum      Maximum       Margin    Units

 1    1    1      OfficeTemp       Enabled     5.0000       140.0000      1.0000    TempinF
Description:

 1    1    2      NothingConnected Disabled    -14.0000     100.0000      0.5000    PSI
Description:

 1    1    3      NothingConnected Disabled    20.8000      0.0000        2.5000    Undefined
Description:
```

Figure 62 - HDAM Port/Slot/Point Characteristics Analog Card Screen

Viewing HDAM Port/Slot/Point Status

Use the `show hdam <port_number> slot <slot_list> point <point_list> status` command to display alarm, analog, and/or control status on HDAM ports at either of the following command modes; for example:

Config:0 >>show hdam 8 slot 6 point 8 status

InReach:0 >>show hdam 8 slot 1 point 1-8 status

InReach:0 >>show hdam 8 slot 2 point 3-15 status

Figure 63 shows an example of the HDAM Port/Slot/Point Status Screen, if Slot 1 contains a Control Card.

```
                                                  Current   Operational
 Port Slot Point       Name                       State     State

 1     1     1         1_1_1                      Opened    On
 1     1     2         1_1_2                      Opened    On
 1     1     3         1_1_3                      Opened    On
 1     1     4         1_1_4                      Opened    On
 1     1     5         1_1_5                      Opened    On
 1     1     6         1_1_6                      Opened    On
 1     1     7         1_1_7                      Opened    On
 1     1     8         1_1_8                      Opened    On
```

Figure 63 - HDAM Port/Slot/Point Status Control Card Screen

Figure 64 shows an example of the HDAM Port/Slot/Point Status Screen, if Slot 2 contains an Alarm Card.

```
                                          Current   Fired   LastTime
Port Slot Point      Name                 State     Count   Fired

 1    2     3         1_2_3                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     4         1_2_4                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     5         1_2_5                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     6         1_2_6                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     7         1_2_7                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     8         1_2_8                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     9         1_2_9                  Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     10        1_2_10                 Faulted    13      Wed,20 Oct 2004 12:17:21 UTC
 1    2     11        1_2_11                 Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     12        1_2_12                 Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     13        1_2_13                 Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     14        1_2_14                 Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
 1    2     15        1_2_15                 Faulted    5       Wed,20 Oct 2004 11:47:24 UTC
```

Figure 64 - HDAM Port/Slot/Point Status Alarm Card Screen

Figure 65 shows an example of the HDAM Port/Slot/Point Status Screen, if Slot 1 contains an Analog Card.

```
Port Slot Point    Name                          Native Units Value      MilliAmp  Value

 1    1    1       Officetemp                     N/A                     0.0000    mA
 1    1    2       NothingConnectedToPoint2       N/ A                    N/A
 1    1    3       NothingConnectedToPoint3       N/A                     N/A
 1    1    4       NothingConnectedToPoint4       N/A                     N/A
 1    1    5       NothingThere                   N/A                     0.0195    mA
 1    1    6       BarometricPressureInMyOffice   29.7128   Hg            16.7326   mA
 1    1    7       HumidityInMyOfficeWithEWSRH    43.1318   %R            10.7789   mA
 1    1    8       TemperatureInMyOfficeWithEWSRH 83.4203   TempinF       13.2942   mA
```

Figure 65 - HDAM Port/Slot/Point Status Analog Card Screen

Viewing HDAM Status Information

Use the `show hdam <port_number> status` command to display both alarm, analog, and control status information on an HDAM port at either of the following command modes; for example:

Config:0 >>`show hdam 4 status`

InReach:0 >>`show hdam 1 status`

Figure 66 shows an example of the HDAM Port Status Screen.

```
Time:                                        Thu, 21 Oct 2004 09:10:06 UTC
 Device Number:                      8  Temperature (Celsius):           23.0

                                                      Current   Operational
 Port Slot Point       Name                           State     State

 1    1     1          1_1_1                          Opened    On
 1    1     2          1_1_2                          Opened    On
 1    1     3          1_1_3                          Opened    On
 1    1     4          1_1_4                          Opened    On
 1    1     5          1_1_5                          Opened    On
 1    1     6          1_1_6                          Opened    On
 1    1     7          1_1_7                          Opened    On
 1    1     8          1_1_8                          Opened    On

 Port Slot Point    Name                           Native Units Value      MilliAmp  Value

  1    2    1       Officetemp                     N/A                     0.0000    mA
  1    2    2       NothingConnectedToPoint2       N/ A                    N/A
  1    2    3       NothingConnectedToPoint3       N/A                     N/A
  1    2    4       NothingConnectedToPoint4       N/A                     N/A
  1    2    5       NothingThere                   N/A                     0.0195    mA
  1    2    6       BarometricPressureInMyOffice   29.7128   Hg            16.7326   mA
  1    2    7       HumidityInMyOfficeWithEWSRH    43.1318   %R            10.7789   mA
  1    2    8       TemperatureInMyOfficeWithEWSRH 83.4203   TempinF       13.2942   mA

                                          Current  Fired       LastTime
Port Slot Point                           State    Count       Fired

 1    3     1          n2345               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     2          1_2_2               Normal     0
 1    3     3          1_2_3               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     4          1_2_4               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     5          1_2_5               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     6          1_2_6               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     7          1_2_7               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     8          1_2_8               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
 1    3     9          1_2_9               Faulted    5         Wed,20 Oct 2004 11:47:24 UTC
```

Figure 66 - HDAM Port Status Screen

Chapter 15

Configuring PPP

This chapter describes how to configure PPP features.

Configuring an IP Interface for PPP

You can bind an IP interface to PPP and specify a dedicated asynchronous port for the IP interface to use for PPP Links.

In addition, you can configure CHAP or PAP authentication, CCP negotiation, IPCP and LCP parameters, the PPP Mode, and the Remote IP address for PPP Links on an IP interface.

The LX unit also supports PPP routing via static routing. With PPP routing, you can manage serially connected devices on remote LX units that do not have Ethernet connectivity. For more information on the LX implementation of PPP Routing, refer to "PPP Routing on the LX" on page 327.

Do the following to configure PPP on an IP interface:

1. Execute the `interface` command, in the Configuration Command Mode, to access an IP interface; for example:

   Config:0 >>`interface 2`

   This enters the Interface Command Mode for the specified interface (i.e., Interface `2`). The Interface Command prompt (e.g., `Intf 2-2:0 >>`) is displayed.

2. Execute the `bind port async protocol ppp` command to bind the IP interface to PPP, and to specify the asynchronous port that the IP interface will use for its PPP Links; for example:

   Intf 2-2:0 >>`bind port async 4 protocol ppp`

   In the above example, IP interface 2 is bound to PPP, and asynchronous port 4 is specified as the port that IP interface `2` will use for its PPP Links.

3. Execute the `ppp` command to access the PPP Command Mode for the IP interface; for example:

   Intf 2-2:0 >>`ppp`

4. Execute the `authentication` command to specify CHAP or PAP as the authentication method for PPP Links on the IP interface. In the following example, CHAP is specified as the authentication method:

   Ppp 2-2:0 >>`authentication chap`

5. Execute the `outbound secret` command to specify the outbound secret for PPP Links on the IP interface; for example:

   Ppp 2-2:0 >>`outbound chap secret wtrrrbbbba`

   NOTE: Because CHAP is the authentication method specified in step 4, an outbound CHAP secret is specified in the above command.

6. Execute the `outbound username` command to specify the outbound client username for PPP Links on the IP interface; for example:

   Ppp 2-2:0 >>`outbound username HenryW`

7. Execute the `remote address` command to specify the remote partner for PPP Links on the IP interface; for example:

   Ppp 2-2:0 >>`remote address 129.27.172.19`

Re-binding an IP Interface to Eth0

When you bind an IP interface to PPP, that IP interface can only be used for PPP connections; the asynchronous port that is specified for PPP Links on the IP interface can only be used for PPP sessions on that interface.

If you want to use the PPP-bound IP interface (or its dedicated asynchronous port) for any other purpose, you must re-bind the IP interface to Eth0. Use the `default bind` command, in the Interface Command Mode, to re-bind the IP interface to Eth0. In the following example, IP interface 2 is re-bound to Eth0:

```
Intf 2-2:0 >>default bind
```

The above `default bind` command also unbinds the asynchronous port that had been specified as a dedicated port for PPP Links on Interface 2. This port is now available for other purposes.

Setting Optional PPP Parameters

The LX supports several optional parameters for PPP sessions, including Compression Control Protocol (CCP) negotiation and several settings for the Link Control Protocol (LCP) and Internet Protocol Control Protocol (IPCP). This section describes how to specify values for these parameters.

NOTE: If you do not specify values for the optional parameters, the LX unit will use default values. The default values are sufficient to support most PPP Links.

Inactivity Timeout

The Inactivity Timeout is the length of time the PPP link will wait for an LCP echo reply before closing the link. Use the `inactivity timeout` command, in the PPP Command Mode, to specify the Inactivity Timeout; for example:

```
Ppp 2-2:0 >>inactivity timeout 6
```

CCP Negotiation

By default, an IP interface does *not* negotiate CCP use with its remote partner. However, you can execute the `ccp enable` command, in the PPP Command Mode, to configure the IP interface to negotiate CCP use with its remote partner; for example:

```
Ppp 2-2:0 >>ccp enable
```

To disable CCP negotiation on an IP interface, execute the `no ccp` command in the PPP Command Mode; for example:

```
Ppp 2-2:0 >>no ccp
```

IPCP Accept Address

Execute the `ipcp accept address enable` command, in the PPP Command Mode, to configure the PPP link to accept negotiation of local, or remote, addresses; for example:

```
Ppp 2-2:0 >>ipcp accept local address enable
```

```
Ppp 2-2:0 >>ipcp accept remote address enable
```

By default, an LX IP interface does not accept the negotiation of local or remote addresses. Use the `no ipcp accept address` command to disable address negotiation on PPP Links; for example:

```
Ppp 2-2:0 >>no ipcp accept local address
```

```
Ppp 2-2:0 >>no ipcp accept remote address
```

IPCP Compression

By default, an IP interface will try to negotiate the use of Van Jacobson (VJ) compression over a PPP link. Use the `no ipcp compression` command, in the PPP Command Mode, to disable VJ compression over a PPP link; for example:

```
Ppp 2-2:0 >>no ipcp compression
```

Execute the `ipcp compression enable` command, in the PPP Command Mode, to re-enable the negotiation of VJ compression over a PPP link; for example:

```
Ppp 2-2:0 >>ipcp compression enable
```

IPCP Failure Limit

The IPCP Failure Limit is the number of attempts at IPCP option negotiation that can be made by the IP interface. Use the `ipcp failure limit` command, in the PPP Command Mode, to specify the IPCP Failure Limit; for example:

```
Ppp 2-2:0 >>ipcp failure limit 6
```

IPCP Timeout

The IPCP Timeout is the length of time that the IP interface has for IPCP option negotiation. Use the `ipcp timeout` command, in the PPP Command Mode, to specify the IPCP Timeout; for example:

```
Ppp 2-2:0 >>ipcp timeout 30
```

PPP Mode

NOTE: The default mode for the LX is *passive*. When configuring PPP between two LX units, one side must be set to active.

In PPP active mode, the port that is bound to the IP interface for PPP Links will periodically send PPP LCP negotiation packets. In PPP passive mode, the port that is bound to the IP interface for PPP Links is in listening mode; the port listens for incoming PPP LCP negotiation packets.

Use the `mode` command, in the PPP Command Mode, to specify the PPP Mode; for example:

```
Ppp 2-2:0 >>mode active
```

```
Ppp 2-2:0 >>mode passive
```

NOTE: When using mode, demand, or backup, the LCP negotiations will always assume *active* mode.

LCP Compression

By default, an IP interface will *not* try to negotiate the use of LCP compression over a PPP link. Use the `lcp compression enable` command, in the PPP Command Mode, to enable the negotiation of LCP compression over a PPP link; for example:

```
Ppp 2-2:0 >>lcp compression enable
```

Execute the `no lcp compression` command, in the PPP Command Mode, to disable the negotiation of LCP compression over a PPP link; for example:

```
Ppp 2-2:0 >>no lcp compression
```

LCP Echo Failure

The LCP Echo Failure setting is the number of times that the IP interface can send an LCP echo request. Use the `lcp echo failure` command, in the PPP Command Mode, to specify the LCP Echo Failure setting; for example:

```
Ppp 2-2:0 >>lcp echo failure 6
```

LCP Echo Interval

The LCP Echo Interval is the interval between the sending of LCP echo requests. Use the `lcp echo interval` command, in the PPP Command Mode, to specify the LCP Echo Interval; for example:

```
Ppp 2-2:0 >>lcp echo interval 20
```

LCP Failure Limit

The LCP Failure Limit is the number of attempts at LCP option negotiation that can be made by the IP interface. Use the `lcp failure limit` command, in the PPP Command Mode, to specify the LCP Failure Limit; for example:

```
Ppp 2-2:0 >>lcp failure limit 6
```

LCP Timeout

The LCP Timeout is the length of time that the IP interface has for LCP option negotiation. Use the `lcp timeout` command, in the PPP Command Mode, to specify the LCP Timeout; for example:

```
Ppp 2-2:0 >>lcp timeout 30
```

PPP Routing on the LX

PPP Routing makes it possible to access remote LX units that do not have Ethernet connections. PPP is established when the router dials your LX and pre-configured routes are activated to allow your NOC to manage the remote LX.

In Figure 67, the NOC telnets to 197.168.1.1 2100-2300 to manage the serial devices.

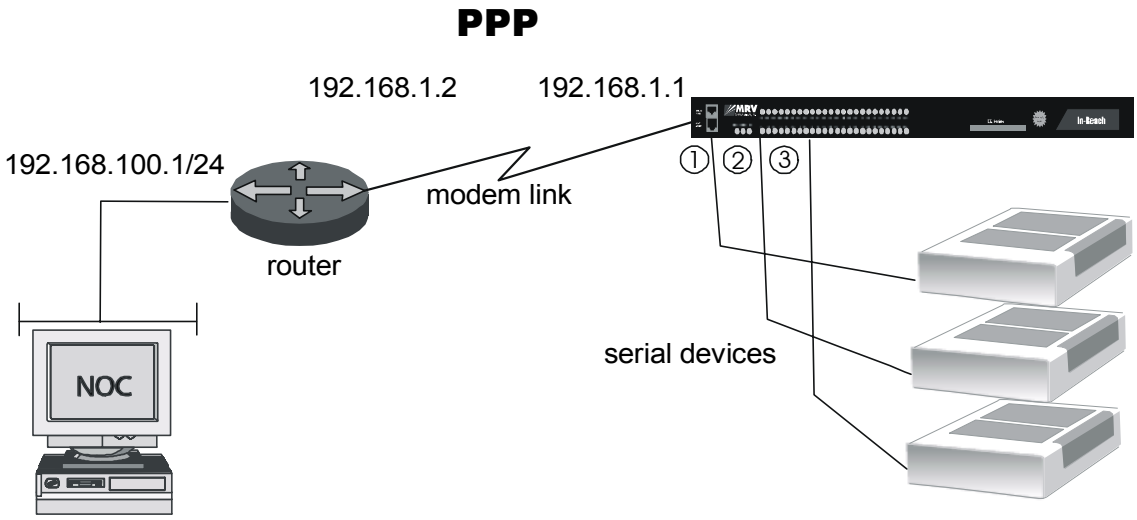


Figure 67 - LX PPP Routing

In order to implement PPP Routing on an LX, do the following:

1. Configure an IP interface for PPP as described in “Configuring an IP Interface for PPP” on page 321.

NOTE: You must specify the IP address of your NOC as the remote partner for PPP Links with the `remote address` command in the PPP Command Mode.

2. Access the Configuration Command Mode. (Refer to page 26 for information on accessing the Configuration Command Mode.)

3. Configure a static route to the NOC by executing the `route` command; for example:

```
Config:0 >>route address 192.168.100.0 mask 255.255.255.0
gateway 192.168.1.2
```

The above example is a static route from the LX unit in Figure 67 on page 327 to the router at IP address 192.168.1.2.

Using PPP Routing for Backup Connectivity

You can configure a Rule to implement PPP routing as a backup method for maintaining the connectivity of the LX unit to the NOC. PPP connectivity would take over connectivity when the local Ethernet for the LX went down. To configure such a rule, do the following:

1. Access the Trigger-Action Command Mode. (Refer to page 33 for information on accessing the Trigger-Action Command Mode.)

2. Use the `trigger name` command, in the Trigger-Action Command Mode, to create a trigger; for example:

```
Trigger-Action:0 >>trigger name NOCLinkIsDown
```

3. In the Trigger Command Mode, configure a trigger with a trigger condition that will be true when the NOC ping status is Down; for example:

```
Trigger_NOCLinkIsDown:0 >>ping address 192.168.100.0
Trigger_NOCLinkIsDown:0 >>ping interval 30
Trigger_NOCLinkIsDown:0 >>ping status down
```

The above commands specify that a ping test will be sent every 30 seconds to the NOC at 192.168.100.0. If the ping status of the NOC is Down, the trigger condition is true.

4. Execute the `exit` command to return to the Trigger-Action Command Mode; for example:

   Trigger_NOCLinkIsDown:0 >>`exit`

5. Use the `action name` command, in the Trigger-Action Command Mode, to create an action; for example:

   Trigger-Action:0 >>`action name ReachNOCbyPPPdial`

6. In the Action Command Mode, use the `command` to configure an action that dials the PPP Routing gateway for the NOC; for example:

   Action_ReachNOCbyPPPdial:0 >>`command dial ppp number 1234567878 interface 3`

7. Execute the `exit` command to return to the Trigger-Action Command Mode; for example:

   Action_ReachNOCbyPPPdial:0 >>`exit`

8. Use the `rule name` command, in the Trigger-Action Command Mode, to create a rule; for example:

   Trigger-Action:0 >>`rule name BackupByPPPdial`

9. In the Rule Command Mode, specify the action and trigger for the rule, and enable the rule; for example:

   Rule_BackupByPPPdial:0 >>`trigger NOCLinkIsDown`
   Rule_BackupByPPPdial:0 >>`action ReachNOCbyPPPdial`
   Rule_BackupByPPPdial:0 >>`enable`

In the above example, the rule `BackupByPPPdial` is a backup method that the NOC can use to access the LX when the Ethernet is down for the LX.

Displaying PPP Characteristics

Use the `monitor/show interface ppp characteristics` command to display the PPP characteristics for an IP interface; for example:

Ppp 2-2:0 >>`show interface 2 ppp characteristics`

In the above example, the PPP characteristics are displayed for IP interface 2. Use the following syntax to show the PPP characteristics of *all* IP interfaces on the LX unit:

Ppp 2-2:0 >>`show interface all ppp characteristics`

Figure 68 shows an example of the PPP Settings Screen.

```
Time:                                          Thu, 27 May 2004 12:29:53 UTC
Interface Name:          Interface_10  PPP Debug:                    Disabled
PPP Mode:                      Active  PPP Dialback Mode:
PPP Authent:                     None  PPP Authent. Retry:                 3
PPP CCP:                     Disabled  PPP Authent. Timeout:              60
PPP Backup Feature:               N/A  PPP Backup Ping Host:             N/A
PPP Backup Ping Interface:        N/A  PPP Backup Ping Interval:         N/A
PPP Remote IP Address:        0.0.0.0  PPP Inactivity Timeout:             0
PPP LCP Compress.:           Disabled  PPP IPCP Compress.(VJ):      Disabled
PPP LCP Failure Limit:             10  PPP IPCP Failure Limit:            10
PPP LCP Echo Failure Limit:         0  PPP IPCP Timeout:                   4
PPP LCP Echo Interval:              0  PPP IPCP Accept Remote:       Enabled
PPP LCP Timeout:                    4  PPP IPCP Accept Local:        Enabled
Outbound CHAP Secret:  Not configured  Outbound PAP Secret:   Not Configured
Outbound Username:        Configured
In-Reach
```

Figure 68 - PPP Settings Screen

Displaying the PPP Status of an IP Interface

Use the `monitor/show interface ppp status` command to display PPP status information for IP interfaces; for example:

Ppp 2-2:0 >>`show interface 2 ppp status`

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

```
Ppp 2-2:0 >>show interface all ppp status
```

Figure 69 shows an example of the PPP Status Screen.

```
Time:                                    Wed, 27 Aug 2003 03:29:41 UTC
Interface Name:        Interface_1
Learned Remote Addr.:      0.0.0.0
Lcp Link Status:            Closed  Ipcp Link Status:             Closed
PPP Transmit Bytes:              0  PPP Receive Bytes:          831262792
PPP Transmit Frames:             0  PPP Receive Frames:             17905
PPP Transmit Errors:             0  PPP Receive Errors:                 0
```

Figure 69 - PPP Status Screen

Configuring PPP Dial-On-Demand

Circuits can reduce line charges by using bandwidth only when needed. When data must be forwarded across a switched circuit, the LX automatically activates the connection, transfers the data, and then based on inactivity, tears down the connection.

There are two main reasons to use PPP Dial-On-Demand:

- If you do not have a LAN connection to the site you want to use. Use PPP demand to bring up a PPP link, to send traps and notification events, and to alert administrators to problems in remote locations.
- Use PPP Dial-On-Demand in conjunction with Trigger Action as a backup network connection in case your LAN goes down.

The following procedure gives an example of how to configure PPP Dial-On-Demand. Figure 70 on page 332 illustrates the sample used in the procedure.

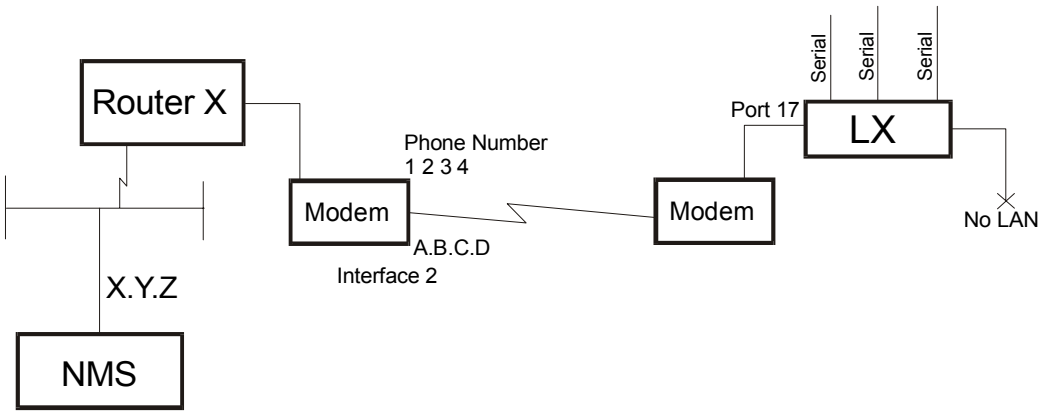


Figure 70 - PPP Dial-On-Demand Diagram

Do the following to configure PPP Dial-On-Demand:

1. Enable the modem on the port and define a dialout number:

   Config:0 >> `port async 17 modem dial number 1234`

2. Enter the Interface Mode:

   Config:0 >> `interface 2`

3. Bind async port 17 to this interface and use ppp17 for the device name. This changes the access on port async 17 to PPP.

   Intf 2-2:>> `bind async port 17 protocol ppp`

4. Enter a remote address. The remote address is an address on the peer network. This remote address is required to define the link as a PPP demand.

   Intf 2-2:>> `ppp remote address A.B.C.D`

5. Put the port into Dial on Demand mode using the existing mode. When you do this, the port only attempts to dial a modem and negotiate PPP when there is a demand to do so, such as when IP network traffic matching the interface's PPP Remote IP Address appears on the unit.

   Intf 2-2:>> `ppp mode demand`

6. When a timeout is set, the PPP link is up and no data packets are being sent or received across the link. Under these conditions, the LX tears down the PPP/dialup connection. This is typically used when the PPP mode is in "demand", but may also be useful in non-demand modes.

   Intf 2-2:>>`ppp inactivity timeout`

7. As the LX does not have a LAN connection, go to the **Config:0 >>** mode and set the system gateway to the remote PPP address, thereby directing all IP traffic to that address:

   Config:0 >>`gateway A.B.C.d`

PPP Backup

This enhancement allows an LX to dial a "backup" PPP connection if contact to a given host is lost. The PPP connection is enabled as a dial-on-demand, and thus is only active as needed. The PPP backup system uses the trigger-action-rule subsystem to detect when contact to the ping host is lost, and then activate the dial-on-demand service.

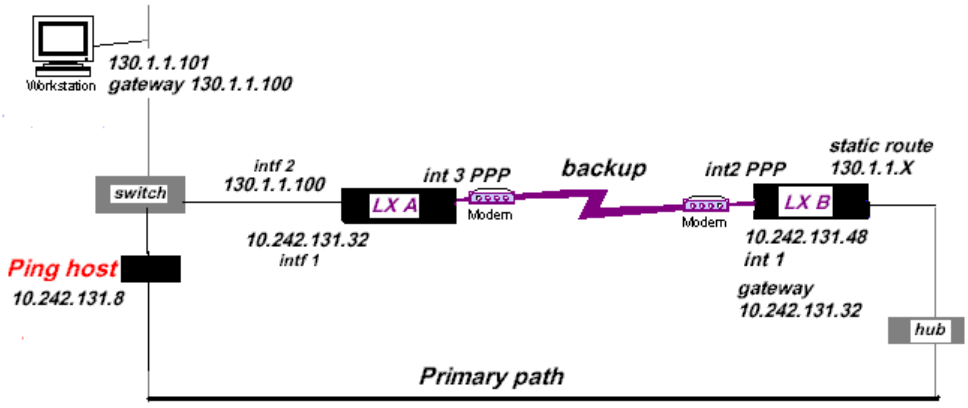


Figure 71 - PPP Dial Backup Diagram

PPP backup becomes a Demand Circuit when LX B cannot ping its ping host 10.242.131.8 because the primary path is down. The connection will not dial unless traffic is destined for a device across the PPP link.

The appropriate settings for the diagram shown in Figure 71 are as follows:

LX A

InReach:0 >> `config inter 1 address 10.242.131.32 mask 255.255.255.0`

InReach:0 >> `config inter 2 address 130.1.1.100 mask 255.255.255.0`

InReach:0 >> `config int 3 bind port async 33 protocol ppp`

InReach:0 >> config int 3 ppp remote address 10.242.131.48

LX B

InReach:0 >>config gateway 10.242.131.32

InReach:0 >>config int 1 address 10.242.131.48 mask 255.255.255.0

InReach:0 >>config int 2 bind port Async 49 protocol ppp

InReach:0 >>config int 2 ppp remote address 10.242.131.32

InReach:0 >>config int 2 ppp mode backup

InReach:0 >>config int 2 ppp backup ping host 10.242.131.8

InReach:0 >>config int 2 ppp backup ping interface 1

InReach:0 >>config int 2 ppp inactive time 30 *(seconds)*

InReach:0 >>config int 2 ppp backup enable

InReach:0 >>config po as 49 modem dialout number 2760 *(phone# of LX A)*

InReach:0 >>config route address 130.1.1.0 mask 255.255.255.0 gateway 10.242.131.32 int 2

Displaying PPP Backup Information

Use the `show interface <interface_number> ppp characteristics` command to display the PPP Settings Screen. An example of this screen follows, with the pertinent entries highlighted:

```
Time:                                        Thu, 27 May 2004 12:29:53 UTC
Interface Name:          Interface_10  PPP Debug:                   Disabled
PPP Mode:                      Active  PPP Dialback Mode:
PPP Authent:                     None  PPP Authent. Retry:                3
PPP CCP:                    Disabled  PPP Authent. Timeout:              60
PPP Backup Feature:              N/A  PPP Backup Ping Host:             N/A
PPP Backup Ping Interface:       N/A  PPP Backup Ping Interval:         N/A
PPP Remote IP Address:       0.0.0.0  PPP Inactivity Timeout:             0
PPP LCP Compress.:          Disabled  PPP IPCP Compress.(VJ):      Disabled
PPP LCP Failure Limit:             10  PPP IPCP Failure Limit:            10
PPP LCP Echo Failure Limit:         0  PPP IPCP Timeout:                   4
PPP LCP Echo Interval:              0  PPP IPCP Accept Remote:       Enabled
PPP LCP Timeout:                    4  PPP IPCP Accept Local:        Enabled
Outbound CHAP Secret:  Not configured  Outbound PAP Secret:   NotCconfigured
Outbound Username:        Configured
In-Reach
```

Figure 72 - PPP Settings

The new "Backup Link Status" field has been added to the PPP Status screen. Use the `show interface <interface_number> ppp status` command to display the PPP Status Screen. An example of this screen follows, with the new entry highlighted:

```
Time:                                    Fri, 08 Oct 2004 11:22:15 US/EASTERN
 Interface Name:          Interface_1  Backup Link Status:              Active
 Learned Remote Addr.:        0.0.0.0
 Lcp Link Status:              Closed  Ipcp Link Status:                Closed
 PPP Transmit Bytes:                0  PPP Receive Bytes:                7312
 PPP Transmit Frames:               0  PPP Receive Frames:               5617
 PPP Transmit Errors:               0  PPP Receive Errors:                  0
```

Figure 73 - PPP Status

PPP Dialback

PPP Dialback provides a level of security by forcing the LX to call back to a specific phone number. It also helps you centralize billing from one location. This feature allows you to configure PPP dialback on both the server and client sides.

Do the following to configure PPP Dialback:

1. At the Interface mode, enable PPP Dialback on the server side:

   Intf 2-2:>> `ppp dialback enable`

2. Enter a PPP outbound number for the server to call back on.

   Intf 2-2:>> `ppp outbound dialback <telephone_number>`

Displaying PPP Dialback Information

Use the `show interface <interface_number> ppp characteristics` command to display the PPP Settings Screen. An example of this screen follows, with the pertinent entry highlighted:

```
Time:                                        Thu, 27 May 2004 12:29:53 UTC
Interface Name:          Interface_10  PPP Debug:                   Disabled
PPP Mode:                      Active  PPP Dialback Mode:              server
PPP Authent:                     None  PPP Authent. Retry:                 3
PPP CCP:                     Disabled  PPP Authent. Timeout:              60
PPP Backup Feature:               N/A  PPP Backup Ping Host:             N/A
PPP Backup Ping Interface:        N/A  PPP Backup Ping Interval:         N/A
PPP Remote IP Address:        0.0.0.0  PPP Inactivity Timeout:             0
PPP LCP Compress.:           Disabled  PPP IPCP Compress.(VJ):      Disabled
PPP LCP Failure Limit:             10  PPP IPCP Failure Limit:            10
PPP LCP Echo Failure Limit:         0  PPP IPCP Timeout:                   4
PPP LCP Echo Interval:              0  PPP IPCP Accept Remote:       Enabled
PPP LCP Timeout:                    4  PPP IPCP Accept Local:        Enabled
Outbound CHAP Secret:  Not configured  Outbound PAP Secret:   NotCconfigured
Outbound Username:        Configured
In-Reach
```

Figure 74 - PPP Settings Screen with PPP Dialback

Chapter 16

Configuring Redundant Ethernet

This chapter describes how to configure Redundant Ethernet.

Redundant Ethernet

NOTE: This feature applies only to the LX-8000.

MRV now supports use of the Ethernet 2 port on a LX-8000 series unit. The second Ethernet port may be used as a normal network interface or to provide fault tolerance for Ethernet 1. If used as a second network interface, the LX-8000 can be connected to two IP networks at the same time and accept connections on either interface. When in fault-tolerant mode, the Ethernet 2 will take on the MAC address and IP information of Ethernet 1 after a link failure occurs.

Two types of link failure may be detected: physical and logical. A physical link failure is triggered when link integrity is lost. A logical link failure occurs when no traffic is received in a defined interval. ARP is used for traffic generation in case no other network traffic is present. Fail-over is automatic. The backup link now becomes the primary link, even if connectivity is restored to the original "primary". Refer to the *LX-Series Commands Reference Guide* and the *LX-Series Configuration Guide* for further information.

Some configuration examples follow:

Configuring Ethernet 2 as a Second Network Interface

NOTE: This capability is not intended to replace a LAN router. Dynamic protocols such as RIP and OSPF are not supported, nor are other routing features such as UDP forwarding. Additionally, LAN routing performance is limited on the LX-8000 Series due to hardware limitations. Routing between ethernet segments is not a supported configuration, due to the above mentioned limitations.

To configure Ethernet 2 as a second ethernet port, do the following:

1. Since Interface 1 is already configured, create Interface 2:

   InReach:0 >> `conf interface 2`

2. Change interface 2 to use eth1:

   Intf 2-2:>> `bind port ethernet 2`

3. Configure an IP address and Mask:

   Intf 2-2:>> `address 192.168.10.1 mask 255.255.255.0`

4. Configure a Broadcast Address:

   Intf 3-3:>> `broadcast 192.168.10.255`

Configuring Ethernet 2 as a Redundant Ethernet Link for Ethernet 1

Use this procedure if you want a redundant link in case the primary link fails. A concept diagram follows:

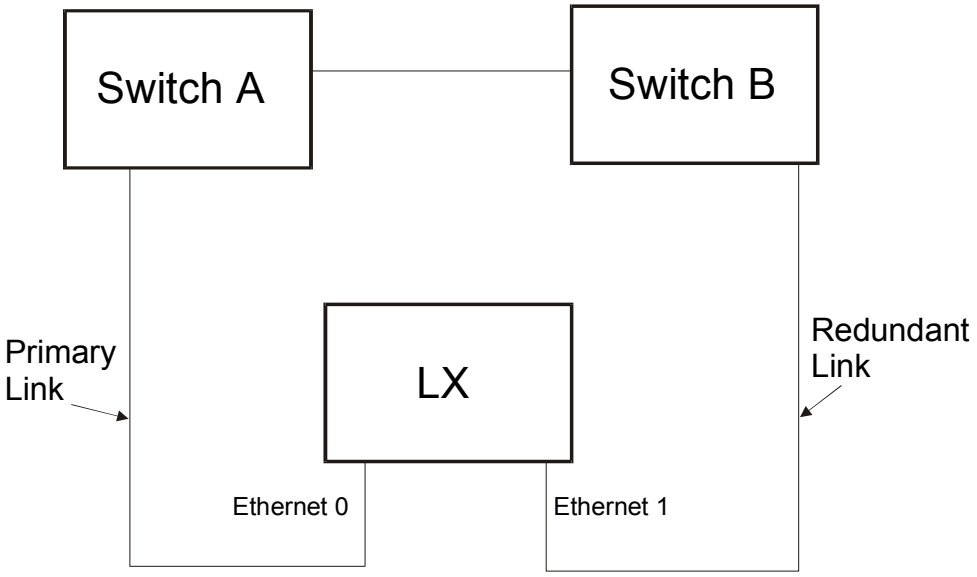


Figure 75 - Primary Link/Redundant Link

NOTE: Because only one link is active at one time, the IP address and the MAC address are mapped to the active link. Therefore, in a fail over condition, the MAC address will change locations on your network. Older switches have difficulty with this dynamic change, and require time to age out the old MAC address. Use some caution when doing this.

To configure Ethernet 2 as a redundant ethernet link for Ethernet 1, do the following:

1. Create the interface:

   InReach:0 >> `conf interface 3`

2. Bond the ethernet ports together:

   Intf 3-3:>> `bind port ethernet 1 2`

3. Configure an IP address and Mask:

   Intf 3-3:>> `address 192.168.10.1 mask 255.255.255.0`

4. Configure a Broadcast Address:

   Intf 3-3:>> `broadcast 192.168.10.255`

There are two mechanisms by which you can detect a primary link fault: physical link detection and logical link detection. Use the `bonding link` command for physical link detection, and the `bonding link arp address` and `bonding link arp interval` commands for logical link detection.

You can access the bonding commands in the Interface Mode.

Bonding Link

This command monitors the physical link of the primary ethernet port if it goes down and the secondary ethernet port comes up. When the secondary ethernet port comes up, the Mac address and the IP address are shifted to the secondary link.

Use the `bonding link` command to monitor the link by the physical connection, and to send a poll every second.

Intf:1-1>> `bonding link <number_of_milliseconds>`

Example

Intf:1-1>> `bonding link 1000`

Bonding Link ARP Address

This command monitors the primary link via ARP to a defined address on the network. ARP is used to generate traffic and receive a response, so the primary link will receive traffic in case no other network traffic is present. If the ARP target fails to respond, the primary link will only fail over if no traffic is received within twice the length of the ARP interval. The redundant link assumes the primary role. The MAC and IP addresses are shifted to the redundant link.

Use the `bonding link arp address` command to monitor the link integrity using ARP. If the ARP fails, the link is presumed to be down and the LX will switch over to the redundant link.

Intf:1-1>> `bonding link arp address <A.B.C.D>`

Example

Intf:1-1>> `bonding link arp address 119.255.255.255`

Bonding Link ARP Interval

Use the `bonding link arp interval` command to configure an ARP interval of one second.

Intf:1-1>> `bonding link arp interval <number_of_milliseconds>`

Example

Intf:1-1>> `bonding link arp interval 1000`

The new Bonding Characteristics screen has been added. Use the `show interface <interface_number> bonding characteristics` command to display the Bonding Characteristics Screen. An example of this screen follows:

```
Time:                                  Tue, 11 Jan 2005 10:51:10 US/EASTERN
 Interface Name:          Interface_2  Bound to :                    eth0:1
 Mode:                           N/A  Link Polling Interval:           N/A
 Arp Address:                    N/A  Arp Polling Interval:            N/A
```

Figure 76 - Bonding Characteristics Screen

The new Bonding Status screen has been added. Use the `show interface <interface_number> bonding status` command to display the Bonding Status Screen. An example of this screen follows:

```
Bonding Mode: fault-tolerance (active-backup)
ARP IP Target: 10.242.131.230 ARP Interval 1000

Interface eth1: STANDBY
MII Status: UP
Redundant Fail-over count: 0

Interface eth0: ACTIVE
MII Status: UP
Redundant Fail-over count: 0
```

Figure 77 - Bonding Status Screen

NOTE: The second ethernet port is inactive during boot, whether it is being used as a second segment or as a redundant connection. Booting the image or parameters over the second segment is not supported.

Defaulting the Binding

If you want to delete a current binding, do the following:

1. At the Interface level, enter:

   Intf 10-10:0 >> `default bind`

2. Save the configuration.

3. Perform reboot.

Reboot is necessary in this software version, but will not be in a future release.

Chapter 17

Internal Modem

This chapter describes how to configure the internal modem.

Configuring the Internal Modem for Dial-Out

If you use this modem for either dial-in/dial-out circuit data, you do not need to configure anything on the LX other than port access. However, if you are using the modem for a dial-out IP GPRS connection to a subscribed ISP via PPP, you must perform the following:

1. Configure the interface:

   InReach>>`config interface <interface_number>`

2. Bind the port with the GPRS modem on it to the PPP Protocol:

   Intf 10-10:0 >>`bind port async <port_number> protocol ppp`

   where <*port_number*> is the internal modem port (port 5).

3. Enter the PPP Mode:

   Intf 10-10:0 >>`ppp`

4. Configure the PPP mode active:

   Ppp 10-10:0 >>`mode active`

5. Enable the remote address:

   Ppp 10-10:0 >>`ipcp accept remote address enable`

6. Enable the local address:

   Ppp 10-10:0 >>`ipcp accept local address enable`

Your ISP may require you to pass in PAP. If so, do the following:

1. Enter an outbound user name:

   Ppp 10-10:0 >>`outbound username <username>`

2. Enter an outbound PAP secret:

   Ppp 10-10:0 >>`outbound pap secret <password>`

Use the `show interface <interface_number> ppp characteristics` command to display the PPP Settings Screen. An example of this screen follows:

```
Time:                                        Thu, 27 May 2004 12:29:53 UTC
Interface Name:          Interface_10  PPP Debug:                   Disabled
PPP Mode:                      Active  PPP Dialback Mode:
PPP Authent:                     None  PPP Authent. Retry:                3
PPP CCP:                     Disabled  PPP Authent. Timeout:              60
PPP Backup Feature:               N/A  PPP Backup Ping Host:             N/A
PPP Backup Ping Interface:        N/A  PPP Backup Ping Interval:         N/A
PPP Remote IP Address:        0.0.0.0  PPP Inactivity Timeout:             0
PPP LCP Compress.:           Disabled  PPP IPCP Compress.(VJ):      Disabled
PPP LCP Failure Limit:             10  PPP IPCP Failure Limit:            10
PPP LCP Echo Failure Limit:         0  PPP IPCP Timeout:                   4
PPP LCP Echo Interval:              0  PPP IPCP Accept Remote:       Enabled
PPP LCP Timeout:                    4  PPP IPCP Accept Local:        Enabled
Outbound CHAP Secret:  Not configured  Outbound PAP Secret:   Not Configured
Outbound Username:        Configured
In-Reach
```

Figure 78 - PPP Settings Screen

NOTE: Your ISP may require a different Modem Init String. Consult your ISP for the proper Modem Init String. Typos in the Modem Init String will return an error.

Viewing Internal Modem Characteristics

NOTE: The new fields appear on the Port Async Modem screen only if a GSM/GPRS Internal Modem is installed.

The new "`Modem Type`", "`GSM/GPRS Received Signal Strength`", and "`GSM/GPRS Channel Bit Error Rate`" fields have been added to the Show Port Async Modem screen. The new fields show the modem type, as well as the Received Signal Strength and Channel Bit Error Rate of the modem. Use the `show port async <port_number> modem` command to display the Port Async Modem Screen. An example of this screen follows, with the new entries highlighted:

```
Time:                              Mon 24 Mar 2005 12:50:42 UTC
Banner:                              /config/banner.default
Device Name:             /dev/pts/0   Port Number:           7
Port Type:                  Virtual   Port Name:             5
Modem Control:             Disabled   Modem Timeout:        40
Modem Retry:                      6   Modem Pool:     Disabled
Modem Dialout Num.:     19785558371
Modem Init String:  AT S7=45 S0=1 L1 V1 X4 &C1 &1 Q0 &S1
Modem Type: GSM/GPRS
GSM/GPRS: Received Signal Strength: 9
GSM/GPRS: Channel Bit Error Rate: 0
```

Figure 79 - Port Async Modem Screen

Chapter 18

Alarm Input/Control Output Points

This chapter describes how to configure control output.

The LX Series can be configured to provide two low voltage/low current Control Output signals per port using the DTR and RTS signals. By using a customer specialized interface design, you can control facility equipment on the LX-Series product.

Configuring Control Output

This feature allows you to configure exclusive control over DTR and/or RTS output signals.

1. Dedicate the port to the use of controlling DTR/RTS:

   InReach>>`config port async <port_number> access control`

   This disables modem control, flow control, autohangup, and autobaud. Telnet and SSH connections to the port will be denied, and you cannot log out of the port.

2. Raise or lower the DTR signal:

   InReach>>`control port async <port_number> dtr high`

   InReach>>`control port async <port_number> dtr low`

   If the port's access is not "control", or DTR is already in the state you are configuring, the command is not performed. The default state is low.

3. Raise or lower the RTS signal:

   InReach>>`control port async <port_number> rts high`

   InReach>>`control port async <port_number> rts low`

If the port's access is not "control", or RTS is already in the state you are configuring, the command is not performed. The default state is low.

Use the `show port async <port_number> characteristics` command to display the Port Async Characteristics Screen. The word `Control` is displayed in the `Access` field when this feature is enabled. An example of this screen follows:

```
Time:                                        Fri, 02 Jan 1970 01:09:56 UTC
Banner:        /config/banner.default  Banner Display:                  Both
Port Number:                     1     Transparent Mode:            Disabled
Access:                    Control     Flow Control:                     Xon
Port Name:                  Port_1     Stop Bits:                          1
Port Type:                 Physical    Parity:                          None
Device Name:           /dev/ttyGN0     Bits per Character:                 8
Port Prompt String:          Login     Autobaud:                    Disabled
Break:                     Enabled     Autobaud Retry:                     5
Special Break String:
Inbound Authentication:      Local     Autohangup:                  Disabled
Outbound Authentication:     Local     Radius Accounting:           Disabled
Authentication FallBack:  Disabled     Tacacs+ Accounting:          Disabled
Auth. FallBack Attempts:         0     Data Buffer Display:           Prompt
Data Buffer Size:             1024     Data Buffer Time Stamp:      Disabled
Data Buffer Syslog:       Disabled
Signal Notif. CTS High:   Disabled     Signal Notif. DSR-DCD High:  Disabled
Signal Notif. CTS Low:    Disabled     Signal Notif. DSR-DCD Low:   Disabled
Port Debug Option:        Disabled     IdleBuffer:                   Enabled
Connect Command:
```

Figure 80 - Port Async Characteristics Screen

Viewing DTR/RTS States

Use the `show port async <port_number> status` command to display the Port Async Status Screen. The `Output Signals: RTS` and the `Output Signals: DTR` fields display the current setting. An example of this screen follows, with the entries highlighted:

```
Time:                                    Mon 24 Mar 2003 13:19:01 UTC
Port Device:              /dev/ttyGN7    Port Number:                8
Remote Partner Host IP Address:                                0.0.0.0
Locally Connected by IP Address:                               0.0.0.0
Autobaud:                      Enabled    Speed:                   9600
Port Lock Status:               In Use    Port Name:              Port_8
Transmit Bytes:                 137260    Receive Bytes:            8728
Frame Errors:                        0    Overrun Errors:              0
Parity Errors:                       0    Break Signals:               2
Buffer Overruns:                     0
Last Transmit Char:                0x0    Last Receive Char:         0x0
Last Control DTR State:            Low    Last Control RTS State:    Low
Tcppipe Connection Status:  Suspended
Input Signals:                          Output Signals:
 CTS=                   Up               RTS=                     Down
 DSR=                   Up               DTR=                     Down
```

Figure 81 - Port Async Status Screen

Configuring Alarm Inputs via Trigger Action Rules

You can configure the LX-Series unit using the console CLI or by utilizing the Graphical User Interface. You can configure the Alarm Inputs function using *Signal-Notice* or by using the CLI commands *Trigger-Action-Rule*. The following examples set up an Alarm Input using CTS and utilize the port DTR Control Output as the controlling voltage on Port 10. Additionally, when the Trigger events occur an SNMP message is generated. A sample procedure follows:

1. Create a trigger:

   InReach:0 >> `config`

```
Config:0 >> trigger
Trigger-Action:0 >> trigger name pa10ctsh
Trigger-pa10ctsh:0 >> signal port 10 cts high
Trigger-pa10ctsh:0 >> exit
Trigger-Action:0 >> trigger name pa10ctsl
Trigger-pa10ctsl:0 >> signal port 10 cts low
Trigger-pa10ctsl:0 >> end
InReach:0 >>
```

NOTES:

- Refer to the Signal-Notice Example for additional simplification.
- Names of the form pa#ctsup, pa#ctsdn are reserved for Signal Notice setup.

2. Create an action:

```
InReach:0 >> config
Config:0 >> trigger
Trigger-Action:0 >> action name pa10ctsh
Action_pa10ctsh:0 >> command notify facility user priority
notice message CTS is H on port name Lab1
Action_pa10ctsh:0 >> exit
Trigger-Action:0 >> action name pa10ctsl
Action_pa10ctsl:0 >> command notify facility user priority
notice message CTS is L on port name Lab1
Action_pa10ctsl:0 >> end
InReach:0 >>
```

3. Create rules to bind the trigger and the action

```
InReach:0 >> config
```

```
Config:0 >> trigger
Trigger-Action:0 >> rule name pa10ctsh
Rule_pa10ctsh:0 >> trigger pa10ctsh
Rule_pa10ctsh:0 >> action pa10ctsh
Rule_pa10ctsh:0 >> exit
Trigger-Action:0 >> rule name pa10ctsl
Rule_pa10ctsl:0 >> trigger pa10ctsl
Rule_pa10ctsl:0 >> action pa10ctsl
Rule_pa10ctsl:0 >> end
InReach:0 >>
```

NOTE: The rules must be enabled. This will be shown later in the setup sequence.

4. Create the SNMP Trap Client:

```
InReach:0 >> config
Config:0 >> snmp
Snmp:0 >> get client 0 x.x.x.x
Snmp:0 >> set client 0 x.x.x.x
Snmp:0 >> trap client 0 x.x.x.x
Snmp:0 >> exit
Config:0 >> snmp enable
Config:0 >> exit
InReach:0 >>
```

NOTE: x.x.x.x is the target SNMP management system IP address.

5. Create the Notification Profile for the Service:

```
InReach:0 >> config
```

```
Config:0 >> notification
Notification:0 >> profile service ricksnmp snmp
Notification:0 >> end
InReach:0 >>
```

NOTES:

- The LX Unit must have a trap client configured.
- Additional service profiles can be created.
- Refer to the LX-Series Configuration Guide for more information.

6. Create the Notification Profile for the user:

```
InReach:0 >> config
Config:0 >> notification
Notification:0 >> profile user ricksnmp service ricksnmp
Noti_User_Info:0 >> facility user
Noti_User_Info:0 >> priority notice
Noti_User_Info:0 >> exit
Notification:0 >> end
InReach:0 >>
```

7. Enable the Rules:

NOTE: Each rule can be enabled when it is created with the single command `enable`. In this step we will enable all rules configured in one step.

```
InReach:0 >> config
Config:0 >> trigger rule all enable
Config:0 >> exit
InReach:0 >>
```

8. Select DTR or RTS as the controlling voltage for the Alarm Input signal. In this example DTR is used to provide the controlling voltage and the port # is port 10.

9. Set the selected signal up as a Control Output with a default High state:

   InReach:0 >> `config port async 10 access control`

   InReach:0 >> `control port async 10 dtr high`

NOTE: The `control port` command can be used to test the functionality of the configuration.

Using Signal Notice to Set Up a Trigger-Action-Rule

The Trigger-Action-Rule setup can be simplified through the use of the Signal-Notice capability; for example:

Create the Trigger, Rule and Action:

InReach:0 >> `config`

Config:0 >> `port async 10 signal cts enable`

Config:0 >> `exit`

InReach:0 >>

NOTES:

- The above command creates two Triggers, two Rules and two Actions for the target signal on the target port with the form pa10ctsup and pa10ctsdn. A port range can be specified.
- Signal-Notice defaults to logging messages in `syslog` at a default level of `notice`.

If the alarm circuit that is attached to the port in the above example is a *normally closed* contact and everything is setup correctly the user will receive an SNMP message when the DTR signal is transitioned via the software commands. In normal use the DTR signal will remain in the High state and changes at the physical contact will cause the messages to be generated.

LX Signal Notice Ease-of-Use

This feature allows you to use substitution characters for port, signal, and current state within the action command. It is an automated way of creating up to 192 trigger actions and rules using one or two simple commands. The % character is now reserved for character substitutions.

- %p for port number
- %s for signal (CTS, DSR-DCD)
- %c for current state (high or low)
- %% translates to %

The syntax follows:

Async 1-2:0 >>`signal action notify message signal %s is %c on port %p`

The substitution is translated into the correct command message for the applicable port, signal, and state. For this action command to function, notification profiles must be configured.

The following is an ease-of-use example:

1. Enter the range of ports on which you want to configure signal notification:

   Config:0 >>`port async 1 2`

2. Enable which signal to monitor (`CTS`, `DSR-DCD`, or `all`) for all ports within the port range:

   Async 1-2:0 >>`signal cts enable`

   Where `all` will monitor both `CTS` and `DSR-DCD` for High and Low rates.

3. Enter the signal action `action` command, using substitute characters:

   Async 1-2:0 >>`signal action send trap message signal %s is %c on port %p`

   This command generates the following action commands; for example:

   ```
   send trap message signal CTS is HIGH on port 1
   ```

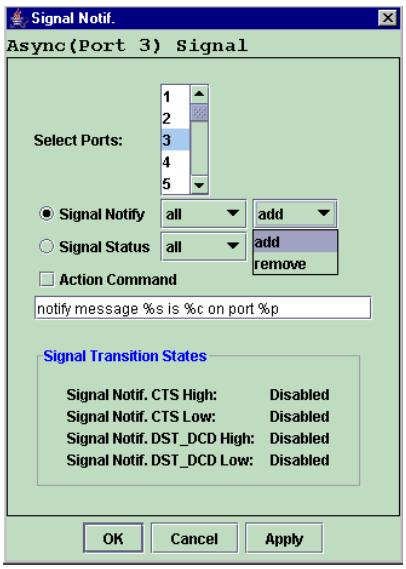
```
send trap message signal CTS is LOW on port 2
```

NOTE: For the `send trap` command to function, the LX requires a configured SNMP trap client, and that SNMP be enabled.

Port Async Signal Notice GUI Configuration

Several changes were made to the Port Async Signal Notice Configuration window. To access the window, do the following:

1. Go to **Port: Async** and then choose a Port tab.
2. At the Console window, click on the **Signal Notif** button at the bottom of the window. The Signal Notif window appears.
3. Select the number of the port(s) on which you want to configure or remove Signal Notification.
4. Select **Signal Notify**. After you select the signals you want to track or remove, choose the options **add** and **remove**, or select the **enable** and **disable** options under **Signal Status**.



5. Click **OK** or **Apply** to save your changes.

If necessary, you can check the **Action Command** box to change the default option command, then click on **Apply** for your configuration to take affect.

Running Signal Notice

You can now run signal notice on a port of access type “control”.

Chapter 19

Configuring IPv6

This chapter describes how to configure IPv6.

IPv6 Internet Protocol

The major changes from IPv4 to IPv6 fall primarily into the following categories:

- Scope-Global Addressing
- Scope-Local Addressing
- 6to4 Tunneling

Configuring IPv6 Stateless Autoconfiguration

Use the following commands to enable or disable stateless auto-configuration of the IPv6 Scope-Global Address.

Intf 1-1:0 >>`ipv6 stateless autoconfiguration`

Intf 1-1:0 >>`no ipv6 stateless autoconfiguration`

Examples

Intf 1-1:0 >>`ipv6 stateless autoconfiguration`

Intf 1-1:0 >>`no ipv6 stateless autoconfiguration`

Configuring the Number of IPv6 Addresses On an Interface

Use the following command to define the maximum number of IPv6 addresses assigned to an ethernet interface. The range is 1-4.

Intf 1-1:0 >>`ipv6 maximum addresses <number_of_addresses>`

Example

Intf 1-1:0 >>`ipv6 maximum addresses 4`

Setting the Number of IPv6 Addresses On an Interface to the Default

Use the following command to set the maximum number of IPv6 addresses assigned to an ethernet interface to the default (4).

Intf 1-1:0 >>`ipv6 default maximum addresses`

Example

Intf 1-1:0 >>`ipv6 default maximum addresses`

Configuring the Number of Duplicate Address Detection Probes to Send

Use the following command to define the number of duplicate address detection probes to send when attempting to configure an IPv6 address on an interface. The range is 1-5.

Intf 1-1:0 >>`ipv6 probes <number_of_probes>`

Example

Intf 1-1:0 >>`ipv6 probes 5`

Setting the Number of Duplicate Address Detection Probes to the Default

Use the following command to set the number of duplicate address detection probes to the default (1).

Intf 1-1:0 >>`ipv6 default probes`

Example

Intf 1-1:0 >>`ipv6 default probes`

Configuring or Deleting a Scope-Global IPv6 Address

Use the following commands to configure or delete a Scope-Global IPv6 address if there are no routers advertising addresses, or if you want to configure another address on an interface.

Intf 1-1:0 >>ipv6 address <*ipv6_address/prefixLength*> device <*ethernet_device*>

Intf 1-1:0 >>no ipv6 address <*ipv6_address/prefixLength*> device <*ethernet_device*>

Examples

Intf 1-1:0 >>ipv6 address 3ffe:303:14:42a0:9cff:fe00:8ad/64 device eth0

Intf 1-1:0 >>no ipv6 address 3ffe:303:14:42a0:9cff:fe00:8ad/64 device eth0

Configuring or Deleting a Route

Use the following commands to configure or delete a route for the *ipv6_address/prefixLength* via the ipv6_address of the specified ethernet device.

Config:0 >>ipv6 route address <*ipv6_address/prefixLength*> device <*ethernet_device*> via <*ipv6_address*>

Config:0 >>no ipv6 route address <*ipv6_address/prefixLength*> device <*ethernet_device*> via <*ipv6_address*>

Examples

Config:0 >>ipv6 route address 3ffe:303:14:42a0:9cff:fe00:8ad/64 device eth0 via 3ffe:303:14:42a0:9cff:fe00:8ac

Config:0 >>no ipv6 route address 3ffe:303:14:42a0:9cff:fe00:8ad/64 device eth0 via 3ffe:303:14:42a0:9cff:fe00:8ac

Configuring or Deleting a Neighbor Entry

Use the following commands to configure or delete a neighbor entry for the destination *ipv6_address* whose ethernet address is the <*ethernet_address*> of the specified ethernet device.

Config:0 >>ipv6 neighbor address <*ipv6_address_of_neighbor*> lladdr <*eth_address_of_neighbor*> device <*ethernet_device*>

Config:0 >>no ipv6 neighbor address <*ipv6_address_of_neighbor*> lladdr <*eth_address_of_neighbor*> device <*ethernet_device*>

Examples

Config:0 >>ipv6 neighbor address fe80::220:edff:febe:3cae lladdr 00:20:ed:be:3c:ae device eth0

Config:0 >>no ipv6 neighbor address fe80::220:edff:febe:3cae lladdr 00:20:ed:be:3c:ae device eth0

Configuring Standard On-Link Tunneling

Use the following commands to configure Standard On-Link tunneling on an interface going to any remote IPv4 host supporting tunneling on your local link. The command word "any" generates the tunnel's local IPv6 address automatically.

Config:0 >>ipv6 tunnel <*tunnel_name*> remote any local <*ipv4_address_of_eth0*> enable

Examples

Config:0 >>ipv6 tunnel 6to4local remote any local 140.179.100.50 enable

- The maximum amount of tunnels per interface that can be configured is 4 (non-configurable).
- The tunnel name can be up to 10 characters in length.
- The tunnel names must be unique.
- If you reconfigure the IPv4 address on the "ethx" interface and a matching tunnel exists, the LX **must** dynamically reconfigure the existing 6to4 tunnel interface accordingly and present you with a message to that effect.

- If you delete the IPv4 address on the “ethx” interface and a matching tunnel exists, the LX **must** delete the existing 6to4 tunnel interface accordingly and present you with a message to that effect.

Configuring a Remote Tunnel Via a Tunnel Broker

Use the following commands to configure a remote tunnel via a tunnel broker.

NOTE: MRV Communications is not responsible for acquiring the broker service for the end user. It is up to the user to subscribe to a tunnel broker who will provide the necessary configuration information.

Config:0 >>`ipv6 tunnel <tunnel_name> remote <ipv4_address> ipv6 address <ipv6_address/prefixLength> local <ipv4_address_of_eth0> enable`

Examples

Config:0 >>`ipv6 tunnel rem-6to4 remote 3ffe:303:14:42a0:9cff:fe00:8ad/64 ipv6 address 3ffe:303:14:42a0:9cff:fe00:8ad/65 local 140.179.100.50 enable`

- The maximum amount of tunnels per interface that can be configured is 4 (non-configurable).
- The tunnel name can be up to 10 characters in length.
- The tunnel names must be unique.
- If you reconfigure the IPv4 address on the “ethx” interface and a matching tunnel exists, the LX **must** dynamically reconfigure the existing 6to4 tunnel interface accordingly and present you with a message to that effect.
- If you delete the IPv4 address on the “ethx” interface and a matching tunnel exists, the LX **must** delete the existing 6to4 tunnel interface accordingly and present you with a message to that effect.

Deleting a Tunnel

Use the following command to delete a tunnel, or all tunnels.

Config:0 >>`no ipv6 tunnel all|<tunnel_name>`

Examples

Config:0 >>`no ipv6 tunnel all`

Config:0 >>`no ipv6 tunnel rem-6to4`

Configuring the Tunnel Packet TTL

Use the following command to define the value for the packet TTL. The range is 0-255.

Config:0 >>`ipv6 tunnel <tunnel_name> ttl <ttl_value>`

Example

Config:0 >>`ipv6 tunnel rem-6to4 ttl 60`

Setting the Tunnel Packet TTL to the Default

Use the following command to set the value of the packet TTL to the default (255).

Config:0 >>`ipv6 tunnel <tunnel_name> default ttl`

Example

Config:0 >>`ipv6 tunnel rem-6to4 default ttl`

Configuring IPv6 on Network Time Protocol (NTP)

Use the following command to configure or delete an NTP Server IPv6 address:

Config:0 >>`ntp server ipv6 address <ipv6_address>`

Config:0 >>`no ntp server ipv6 address <ipv6_address>`

Example

Config:0 >>`ntp server ipv6 address 3ffe:303:14:4:2a0:9cff:fe00:8ad/64`

Configuring an Alternate IPv6 Address on Network Time Protocol (NTP)

Use the following command to configure or delete an alternate NTP Server IPv6 address:

Config:0 >>`ntp server alternate ipv6 address <ipv6_address>`

Config:0 >>`no ntp server alternate ipv6 address <ipv6_address>`

Example

Config:0 >>`ntp server alternate ipv6 address 3ffe:303:14:4:2a0:9cff:fe00:8ad/65`

Configuring a Service Name and Address

Use the following command to configure an IPv6 Service Name and Address.

Config:0 >>`service name <name> ipv6 address <ipv6_address>`

Example

Config:0 >>`service name Finance_Server ipv6 address 3ffe:303:14:4:2a0:9cff:fe00:8ad/64`

To view the Service, enter the `show service` command.

Viewing IPv6 Characteristics

Use the `show interface <interface_number> ipv6 characteristics` command to display the Interface IPv6 Configured Characteristics Screen. An example of this screen follows:

```
Time:                                          Mon, 26 Aug 2002 09:56:22 UTC
Interface Name:              Interface_1   Bound to :                    eth0
Stateless Autoconfig:            Enabled   Maximum Addresses:               4
Maximum DAD Probes:                    1
Global Address/Prefix:                      3ffe:303:14:4:2a0:9cff:fe00:8ad/64
Global Address/Prefix:                     3ffe:405:22:14:2a0:9cff:fe00:8ad/64
```

Figure 82 - Interface IPv6 Characteristics Screen

Viewing IPv6 Status

Use the `show interface <interface_number> ipv6 status` command to display the Interface IPv6 Status Screen. An example of this screen follows:

```
Time:                                    Mon, 26 Aug 2002 12:10:36 UTC
Interface Name:           Interface_1    Bound to :                  eth0

3: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qlen 1000
   inet6 fe80::2a0:9cff:fe00:8ad/64 scope link
     valid_lft forever preferred_lft forever
   inet6 fe80::2a0:9cff:fe00:8ad/64 scope global dynamic
     valid_lft 258935sec preferred_lft 602345sec
```

Figure 83 - Interface IPv6 Status Screen

Viewing IPv6 Tunnel Information

Use the `show ipv6 tunnel all|<tunnel_name>` command to display the IPv6 Tunnel Information Screen. Use `show ipv6 tunnel all` to display information on all current tunnels. Use `show ipv6 tunnel <tunnel_name>` to display information on a specific tunnel. An example of the screen follows:

```
Tunnel Name                      6to4local
Tunnel Address:                                        2002:8cb3:a940::1/16
Tunnel Local Address:                                        140.179.100.50
Tunnel Remote Address:                                                  any
Tunnel TTL:                                                             244

Tunnel Name                       rem-6to4
Tunnel Address:                                    2001:560:1f01:ffff::840/127
Tunnel Local Address:                                        140.179.100.26
Tunnel Remote Address:                                                  any
Tunnel TTL:                                                             255
```

Figure 84 - IPv6 Tunnel All Information Screen

Viewing the IPv6 NTP Address

Use the `show system characteristics` command to display the NTP IPv6 Address on the System Characteristics Screen. An example of this screen follows, with the new field highlighted:

```
Name:                          In-Reach  Time:   Sat, 01 Jan 2005 06:01:49 UTC
Serial Number:      00:a0:9c:00:02:b1  Authenticate Image:          Disabled
Location:
Domain Name suffix:
Maximum Number of Async Ports:     34  Internal Modem on Port:            33
Maximum Number of Subscribers:    100  LX Model Type:            LX-4032-101
Maximum Number of Interfaces:      36  Maximum Number of Ethernet Ports:   1
Primary Domain :              0.0.0.0  Secondary Domain :            0.0.0.0
Gateway :                     0.0.0.0  Default TFTP Server : 120.179.169.188
Timed Daemon:                Disabled  TFTP Retries:                       3
NTP   Daemon:                Disabled  TFTP Timeout:                       3
NTP   Server:                 0.0.0.0  NTP Server Alternate:         0.0.0.0
NTP IPv6 Server:                        3ffe:303:11:2222:220:edff:fe4b:fc67
NTP IPv6 Server Alternate:              3ffe:303:11:2222:220:edff:fe4b:fc68
Finger Daemon:               Disabled  Logging Size :                  64000
Telnet Server:                Enabled  Telnet Client:                Enabled
Web Server:                   Enabled  Web Server Port:                   80
Web Server Timeout:                20  Web JceModule:               JsafeJCE
Web Encrypt:                 Disabled  Web Banner:                   Enabled
Subscriber Debug Option:     Disabled  Trigger-Action Debug Option: Disabled
System Debug Option:         Disabled  Flash Debug Option:          Disabled
Minimum Password Length:            0  SSH Daemon:                   Enabled
Rlogin Client:               Disabled  Message Feature:             Disabled
SNMP Feature:                 Enabled
Modem Pool Enabled Serial Ports:
```

Figure 85 - System Characteristics Screen with NTP IPv6 Address

Viewing IPv6 Routes

Use the `show ipv6 routes device <interface_name>` command to display the IPv6 route information. An example of this screen follows:

```
3ffe:303:11:2::/64  proto kernel  metric 256  mtu 1280 advmss 1220 metric 10 64
fe80::/64  metric 256  mtu 1280 advmss 1220 metric 10 64
ff00::/8  metric 256  mtu 1280 advmss 1220 metric 10 1
default via fe80::220:edff:febe:3caf  proto kernel  metric 1024  expires 29sec
mtu 1280 advmss 1220 metric 10 64
```

Figure 86 - IPv6 Routes Screen

Viewing IPv6 Neighbors

Use the `show ipv6 neighbor device <interface_name>` command to show the IPv6 neighbor information:

```
fe80::220:edff:febe:3caf lladdr 00:20:ed:be:3c:af PERMANENT
fe80::220:edff:febe:3cae lladdr 00:20:ed:be:3c:ae router STALE
```

Figure 87 - IPv6 Neighbors Screen

IPv6 Enhancement to Ping, SSH, and Telnet

The User level and Superuser level commands ping, ssh, and telnet now support IPv6. The syntax follows:

Ping IPv6

The syntax follows:

InReach:0 >>`ping [IPv6] [<ip_address or ipv6_address>|NAME]`

Example

InReach:0 >>`ping ipv6 fe80::220:edff:fe4B:sc67`

SSH IPv6

The syntax follows:

InReach:0 >>`ssh [IPv6] [<ip_address or ipv6_address> [NUMBER]]|[NAME [NUMBER]] [LOGIN NAME]`

Example

InReach:0 >>`ssh ipv6 fe80::220:edff:fe4B:sc67`

Telnet IPv6

The syntax follows:

InReach:0 >>`telnet [IPv6] [<ip_address or ipv6_address> [NUMBER]]|[NAME [NUMBER]] [<window_size>]`

Example

InReach:0 >>`telnet ipv6 fe80::220:edff:fe4B:sc67`

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 88 shows an example of the RADIUS authentication process.

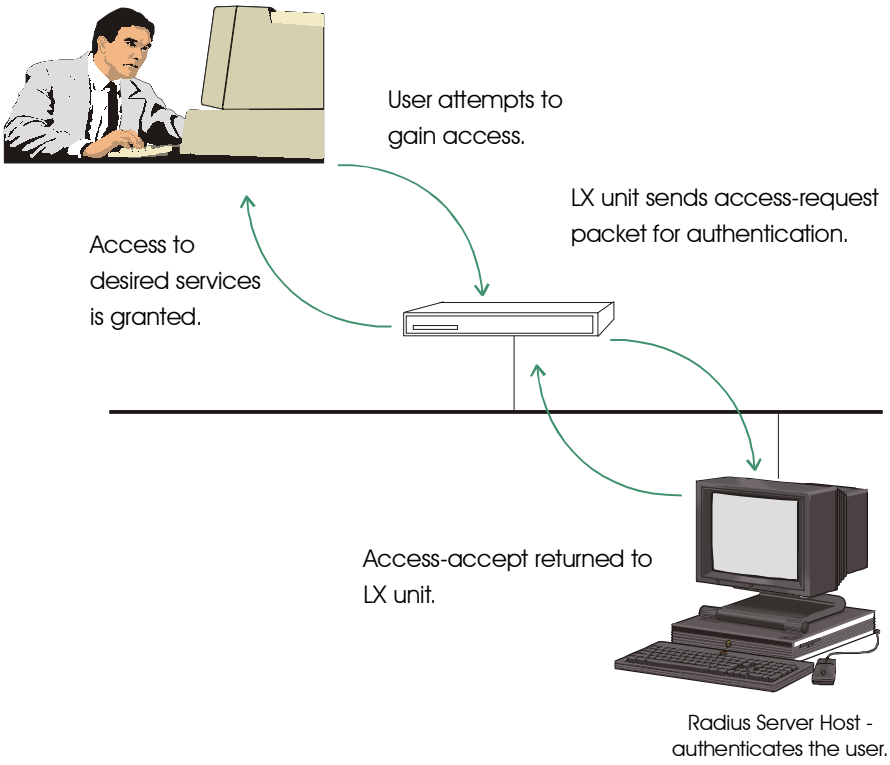


Figure 88 - RADIUS Authentication Process

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.
04	NAS-IP-Address	IP address associated with the LX unit.
05	NAS-Port	Port or circuit number associated with the request.
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.
	Callback-NAS-Prompt	After a Dialback connection is completed, the user will *not* have Superuser privileges.
	Callback-Administrative	After a Dialback connection is completed, the user will have Superuser privileges.
	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.

13	Framed-Compression	The compression protocol for the circuit.
19	Callback - Number	The Callback number in the packet will be used to call back the subscriber for a Callback (Dialback) connection.
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.
25	Class	Sent by the server , and then sent unmodified by the client to the accounting server.
28	Idle Timeout	The amount of time (in seconds) before the idle user is disconnected. The minimum is 60 seconds (seconds are converted to minutes on the LX and rounded to the nearest minute).
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.
60	CHAP-Challenge	

61	NAS-Port-Type	The type of port being used. The valid values are: 0 - Asynchronous

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 379 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 and Authorization

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 89 shows an example of the TACACS+ authentication process.

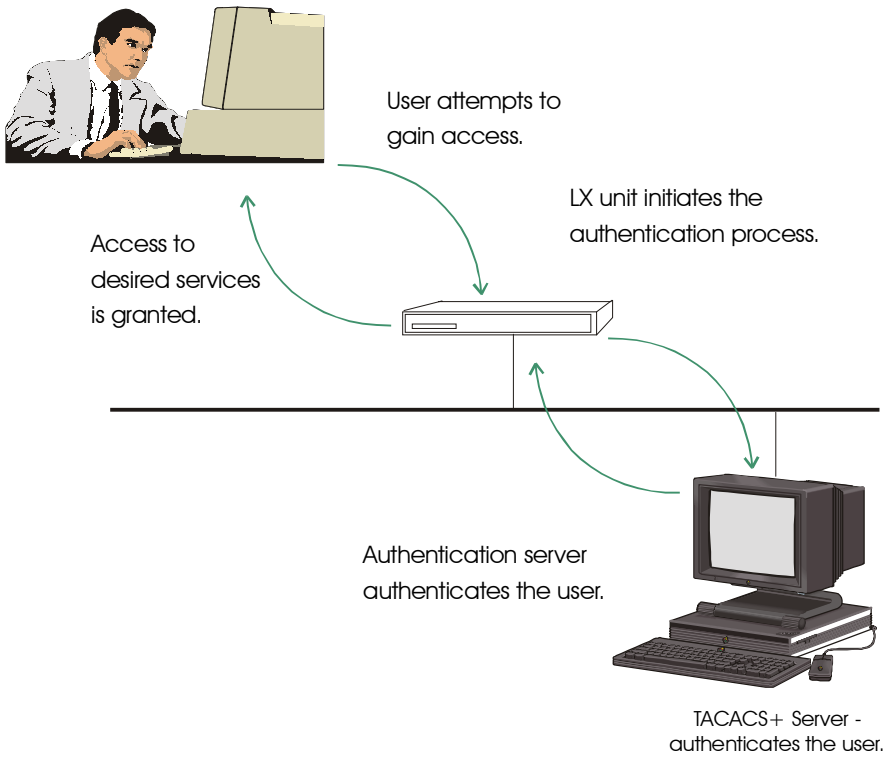


Figure 89 - TACACS+ Authentication Process

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.

TACACS+ Authorization Attributes

Table 13 lists the TACACS+ Authorization Attributes that are supported on the LX unit.

Table 13 - Supported TACACS+ Authorization Attributes

	Attribute Name	Description
01	Auto-cmd	Sends an auto-command.
02	Priv-level	Set this value to 15 to enable rights.

Auto Command

The only valid command is "`menu <menuname>`". The filename must already exist as a valid LX menu on the LX in the `/config` directory. If the menu does not exist, you are logged off after you are authenticated. If the menu does exist, you are prompted with the menu and will not be able to access the CLI. This attribute only applies if you are accessing the CLI (either remotely or locally).

Example

Enter the following in the TACACS+ configuration file on the TACACS+ server if you want to be presented with a menu:

```
user bob {
  login = cleartext bob
  service = exec {
    autocmd = "menu demo_menu"}
}
```

where `user bob` is the username, `cleartext bob` is the password, `exec` is the login mode, and `menu demo_menu` is the menu file.

Privilege Level

You must set this value to the Superuser level. The level must be set to 15.

Example

Enter the following in the TACACS+ configuration file on the TACACS+ server if you want enable rights:

```
user InReach {
login = cleartext access
service = exec {
priv-lvl = 15}
}
```

where `user InReach` is the username, `cleartext access` is the password, `exec` is the login mode, and `priv-lvl` is the authorized level.

Appendix D

Details of the iptables and ip6tables Commands

This appendix contains the Linux man pages for the **iptables** command and the **ip6tables** command. Refer to the man pages in this appendix for detailed information on the **iptables** command, which is introduced in "Configuring iptables and ip6tables" on page 201.

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.
```

Refer to the man pages in this appendix for detailed information on the **ip6tables** command, which is introduced in "Configuring iptables and ip6tables" on page 201.

ip6tables man Pages

```
IP6TABLES(8)                                              IP6TABLES(8)

NAME
       ip6tables - IPv6 packet filter administration

SYNOPSIS
      ip6tables [-t table] -[AD] chain rule-specification [options]
      ip6tables [-t table] -I chain [rulenum] rule-specification
      [options]
      ip6tables [-t table] -R chain rulenum rule-specification
      [options]
      ip6tables [-t table] -D chain rulenum [options]
      ip6tables [-t table] -[LFZ] [chain] [options]
      ip6tables [-t table] -N chain
      ip6tables [-t table] -X [chain]
      ip6tables [-t table] -P chain target [options]
      ip6tables [-t table] -E old-chain-name new-chain-name

DESCRIPTION
             Ip6tables  is  used to set up, maintain, and inspect
```

the tables of IPv6 packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains 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 determine the fate of the packet.

TABLES

There are currently two independent tables (which tables are present at any time depends on the kernel configuration options and which modules are present), as nat table has not been implemented yet.

-t, --table 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 (if no -t option is passed. 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).

mangle: This table is used for specialized packet alteration. Until kernel 2.4.17 it had two built-in chains: PREROUTING (for altering incoming packets before routing) and OUTPUT (for altering locally-generated packets before routing). Since kernel 2.4.18, three other built-in chains are also supported: INPUT (for packets coming into the box itself), FORWARD (for altering packets being routed through the box),and POSTROUTING (for altering packets as they are about to go out).

OPTIONS

The options that are recognized by ip6tables 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 ip6tables can differentiate it from all other options.

-A, --append chain rule-specification

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 chain rule-specification

-D, --delete chain rulenum

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.

-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.

-R, --replace chain rulenum rule-specification
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.

-L, --list [chain]
List all rules in the selected chain. If no chain is selected, all chains are listed. As every other iptables command, it applies to the specified table (filter is the default), so mangle rules get listed by ip6tables -t mangle -n -L Please note that it is often used with the -n option, in order to avoid long reverse DNS lookups. 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. The exact rules are suppressed until you use ip6tables -L -v

-F, --flush [chain]
Flush the selected chain (all the chains in the table if none is given). This is equivalent to deleting all the rules one by one.

-Z, --zero [chain]
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 chain
            Create  a  new user-defined chain by the given name.
            There must be no target of that name already.

       -X, --delete-chain [chain]
            Delete the optional user-defined chain specified.
            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 chain target
            Set the policy for the chain to the given target.  See
            the  section  TARGETS  for  the legal targets.  Only
            built-in (non-user-defined) chains can have  policies,
            and  neither  built-in  nor user-defined chains can be
            policy targets.

       -E, --rename-chain old-chain new-chain
            Rename the user specified chain to the user supplied
            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, ipv6-
            icmp|icmpv6, or all, or it can be a numeric value, rep-
            resenting 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 omitted.

-s, --source [!] address[/mask]
Source specification. Address can be either a hostname (please note that specifying any name to be resolved with a remote query such as DNS is a really bad idea), a network IPv6 address (with/mask), or a plain IPv6 address. (the network name isn't supported now). The mask can be either a network mask or a plain number, specifying the number of 1â€™s at the left side of the network mask. Thus, a mask of 64 is equivalent to ffff:ffff:ffff:ffff:0000:0000:0000:0000. A "!" argument before the address specification inverts the sense of the address. The flag --src is an 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 counters on the rule will be incremented.

-i, --in-interface [!] name
Name of an interface via which a packet is going to be received (only for packets entering the INPUT, FORWARD and PREROUTING 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, any interface name will match.

-o, --out-interface [!] name
Name of an interface via which a packet is going to be sent (for packets entering the FORWARD and OUTPUT 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, any interface name will match.

-c, --set-counters PKTS BYTES
This enables the administrator 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 name, the rule options (if any), and the TOS masks. The packet and byte counters are also listed, with the suffix “K”, “M” or “G” for 1000, 1,000,000 and 1,000,000,000 multipliers 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 program will try to display them as host names, network 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 (multiples 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 beginning 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
ip6tables 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 specified. 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  a  conve-
          nient  alias  for  this option.

     --destination-port [!] port[:port]
          Destination  port or port range specification.  The
          flag --dport is a convenient 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 examine, writ-
          ten 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
          ip6tables -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 RST 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.

ipv6-icmp
   This  extension  is  loaded  if  '--protocol  ipv6-icmp' or
   '--protocol icmpv6' is specified. It provides the following
   option:

     --icmpv6-type [!] typename
          This allows specification of the  ICMP  type,  which
          can  be  a numeric IPv6-ICMP type, or one of the IPv6-
          ICMP type names shown by the command
          ip6tables -p ipv6-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 coming from an Ethernet device
          and entering the PREROUTING, FORWARD or INPUT chains.

limit
   This  module  matches at a limited rate using a token bucket
   filter.  A rule using this extension  will  match  until
   this  limit  is  reached (unless  the "!" flag is used).  It
   can be used in combination with the LOG target to give lim-
   ited logging, for example.

     --limit rate
          Maximum average matching rate: specified as a  number,
          with  an optional  '/second',  '/minute',  '/hour', or
          '/day' suffix; the default is 3/hour.

     --limit-burst number
          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-ports port[,port[,port...]]
            Match if the source port is one of the given  ports.
            The  flag --sports is a convenient alias for this
            option.

       --destination-ports port[,port[,port...]]
            Match  if  the  destination port is one of the given
            ports.  The flag --dports is a convenient alias for
            this option.

       --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
            mask 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.  This is regarded as experimental.

       --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.

TARGET EXTENSIONS
      ip6tables 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  IPv6
      IPv6-header fields) via the kernel log (where it can be read
      with dmesg or syslogd(8)).  This is a "non-terminating  tar-
      get", i.e. rule traversal continues at the next rule.  So if
      you want to LOG the packets you refuse, use two separate
      rules with the same matching criteria, first using target
      LOG then DROP (or REJECT).

       --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 mes-
            sages 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 IPv6 packet header.

MARK
   This  is  used  to  set  the  netfilter  mark value associ-
   ated 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 so
   it is a terminating TARGET, ending rule traversal.  This tar-
   get is only valid  in  the  INPUT, FORWARD  and  OUTPUT
   chains,  and  user-defined  chains which are only called from
   those chains.  The following option controls the nature  of
   the error packet returned:

     --reject-with type
          The type given can be
          icmp6-no-route
          no-route
          icmp6-adm-prohibited
          adm-prohibited
          icmp6-addr-unreachable
          addr-unreach
          icmp6-port-unreachable
          port-unreach
          which  return  the  appropriate  IPv6-ICMP  error mes-
          sage (port-unreach is the default). 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  (113/tcp)  probes  which  frequently
          occur when sending mail to broken mail hosts (which
```

won't accept your mail otherwise).

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

Bugs? What's this? ;-) Well... the counters are not reliable on sparc64.

COMPATIBILITY WITH IPCHAINS

This ip6tables is very similar to ipchains by Rusty Russell. 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 respectively. Hence every packet only passes through one of the three chains (except loopback traffic, which involves both INPUT and OUTPUT 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. There are several other changes in ip6tables.

SEE ALSO

ip6tables-save(8), ip6tables-restore(8), iptables(8), iptables-save(8),iptables-restore(8).

The packet-filtering-HOWTO details iptables usage for packet filtering, the NAT-HOWTO details NAT, the netfilter-extensions-HOWTO details the extensions that are not in the standard distribution, and the netfilter-hacking-HOWTO details the netfilter internals. See http://www.netfilter.org/.

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, Martin Josefsson, Jozsef Kadlecsik, James Morris, Harald Welte and Rusty Russell.

ip6tables man page created by Andras Kis-Szabo, based on iptables man page written by Herve Eychenne <rv@wallfire.org>.

Mar 09, 2002

IP6TABLES(8)

Appendix E

Advanced Features

Multi-Level Command Execution

Multi-Level Command Execution is the ability to execute a command that resides in a command mode other than the current command mode. A command that is executed in this way is called a **target command**, and it must reside in a command mode that is nested in the current one. Figure 1 on page 24 shows the nesting of command modes in the LX CLI.

For example, a target command in the Interface command mode can be executed in the Configuration command mode. In the following example, the target command `broadcast 123.43.34.34` is executed from the Configuration command mode:

```
Config:0 >>interface 1 broadcast 123.43.34.34
```

The command that precedes the target command is known as the **mode-access** command. The mode-access command is used to reach the command mode in which the target command resides. In the above example, the mode-access command is `interface 1`.

You can have more than one mode-access command before a target command, depending on the number of command modes that must be traversed to execute the target command. In the following example, two mode-access commands are used to execute the `open mark1` command from the Superuser command mode:

```
InReach:0 >>configuration menu open mark1
```

In the above example, the mode-access commands are `configuration` and `menu`.

Executing Multi-Level Commands from the User Command Mode

You can execute multi-level commands in the User command mode if you are logged in with an account that gives you access to the Configuration commands.

When you execute a multi-level command from the User command mode, the command string must begin with `enable system`. This is an **access-mode** command that consists of the `enable` command and the Superuser password (**system**). In the following example, the target command is `ssh v1`:

```
InReach:0 >enable system configuration ssh v1
```

Configuring the Notification Feature with Multi-Level Commands

You need to execute the `restart notification` command, in the Superuser command mode, after you execute a multi-level command that effects the Notification Feature. The commands that effect the Notification Feature are those that reside in the Notification command mode and in its subordinate command modes.[1]

The `restart notification` command regenerates the notification configuration and re-starts syslogd. It is necessary to do this when you configure the Notification Feature from outside of the Notification context. (You are outside of the Notification context when you configure the Notification Feature from outside of the Notification command mode or one of its subordinate command modes.) For more information, refer to the `restart notification` command in the *LX-Series Commands Reference Guide*.

1. The subordinate command modes of the Notification command mode are User Service, User Information, Service Profile, Async Profile, Localsyslog Profile, Remotesyslog Profile, SMTP Profile, SNPP Profile, TAP Profile, and WEB Profile. Figure 1 on page 24 shows the nesting of command modes in the Notification command mode.

You must specify the Service Profile type (protocol) in multi-level commands that affect the settings of Service Profiles. The commands that affect the settings of Service Profiles are those in the Async Protocol, Localsyslog Protocol, Remotesyslog Protocol, SMTP Protocol, SNPP Protocol, TAP Protocol, and WEB Protocol Command Modes. The format for such a multi-level command is as follows:

<mode-access-cmd> <protocol> <target-cmd>*

Where	Means
mode-access-cmd	The mode-access commands that are necessary to access the target command.
protocol	The Service-Profile type (protocol) of the Service Profile for which the command is being executed.
target-cmd	The target command.

The following are examples of multi-level commands in which the Service-Profile type (protocol) is specified before the target command:

```
Config:0 >>notification profile service email smtp server
140.179.169.20
```

```
Config:0 >>notification profile service onboard async port 2
```

```
Config:0 >>notification profile service pager tap smsc 3776809977
```

Examples of Multi-Level Commands

The following are examples of multi-level commands. Note that the following is not an exhaustive list of multi-level commands. The following is a list of examples of some of the multi-level commands that could be executed from the User and Configuration command modes.

Examples of Multi-Level Commands in the User Command Mode

```
InReach:0 >enable system zero all
```

```
InReach:0 >enable system configuration secondary dns
119.20.112.3
```

```
InReach:0 >enable system configuration port async 4
break enable

InReach:0 >enable system configuration port async 4
default port

InReach:0 >enable system configuration interface 1 mtu 1200

InReach:0 >enable system enable system ssh
```

Examples of Multi-Level Commands in the Configuration Command Mode

```
Config:0 >>interface 1 broadcast group 4 slave port
async 2

Config:0 >>subscriber mark command log enable

Config:0 >>menu open mark1

Config:0 >>subscriber mark access console enable

Config:0 >>snmp get client 4 125.65.45.34
```

Appendix F

Enabling/Disabling TCP Ports/IR Listener Ports

Open Ports on the LX

Table 14 lists the ports that can be open on the LX. An asterisk (*) indicates the port is open by default

Table 14 - Open LX Ports

Listener Port	Setting
fingerd---79	Disable fingerd to close port.
snmp---161	Disable SNMP to close port.
*ssh---22	Disable SSH to close port.
*telnet---23	Disable telnet to close port.
*http---80	Disable web to close port.
*GUI---5040	Closes if 80 is disabled.
Cluster---8100	Remove cluster secret to close port.
Telnet---2100 - 6800 SSH---2122 - 6822	Port async TCP listener ports. The number of ports on your particular unit will determine the range of ports opened. For example, an 8-port unit contains ports 2100 - 2800. Refer to “Changing the Default TCP Listener Ports” on page 430 for information on changing TCP Port defaults.

Changing the Default TCP Listener Ports

To change the default async TCP listener port settings, do the following:

1. Go to the Interface Command Mode and enter:

   Intf 1-1:0 >>`serial 1 telnet` *`port_number`*

   where `1` is the async port, and where *`port_number`* is the open TCP port you want to switch to.

2. To change the SSH port, enter:

   Intf 1-1:0 >>`serial 1 ssh` *`port_number`*

   where `1` is the async port, and where *`port_number`* is the open TCP port you want to switch to.

Appendix G

RADIUS Vendor Dictionary Files

IMPORTANT!

The following example may not fit your specific RADIUS format. Refer to your RADIUS server manual for further information. The standard `MRV.dict` file is available on your LX CD-ROM.

The RADIUS server uses a *dictionary* file to convert between the numeric attributes and values used in RADIUS packets and human-readable ones. Most RADIUS packages uses a modular dictionary, consisting of the file named **dictionary** and vender specific files in su*b-dictionaries*.

Each RADIUS attribute is assigned a unique number and name, which is than contained in a *dictionary* file on the RADIUS server. Currently, the RADIUS Authentication RFC defines approximately 95 attributes. The remaining values (up to 255) are reserved for future use.

Vendor-specific attributes are additional attributes made by vendors to customize how RADIUS works with their products. One benefit of vendor-specific attributes is that it allows you to obtain a login menu without having to create an LX subscriber.

Most RADIUS packages require you to add your vendor's attributes and values to a sub-dictionary. MRV uses vendor code 33. MRV provides a prepared sub-dictionary that specifies which attributes and values correspond to which numeric codes. Some RADIUS package formats are different and must be modified to work in their format.

To get started, you must have your vendor's ID, and the list of attributes with possible values.

Editing the RADIUS File to Include Your Vendor File

1. Edit the list of vendor ID numbers (this file may be named `dict.vendors`). Add a line for MRV; for example:

   ```
   $add vendor 33 MRV
   ```

2. Add the sub-dictionary `MRV.dict` to the `dictionary`. Edit the dictionary file to include your vendor specific file:

   ```
   $include MRV.dict
   ```

   or cut and paste the `MRV.dict` file into the primary dictionary file. A sample `MRV.dict` file appears below:

```
#  dictionary.mrv
  #
  VENDORMRV33

  # Authentication
  ATTRIBUTE       MRV-Remote-Access-List          1       string          MRV
  ATTRIBUTE       MRV-Port-Access-List            2       string          MRV
  ATTRIBUTE       MRV-Outlet-Access-List          3       string          MRV
  ATTRIBUTE       MRV-Outlet-Group-Access-List    4       string          MRV
  ATTRIBUTE       MRV-Login-Mode                  5       string          MRV
  ATTRIBUTE       MRV-Menu-Name                   6       string          MRV
  ATTRIBUTE       MRV-Web-Menu-Name               7       string          MRV
  ATTRIBUTE       MRV-Security-Level              8       string          MRV
  ATTRIBUTE       MRV-User-Prompt                 9       string          MRV
  ATTRIBUTE       MRV-Command-Logging            10       string          MRV
  ATTRIBUTE       MRV-Audit-Logging              11       string          MRV
  ATTRIBUTE       MRV-Web-Login-Mode             12       string          MRV
  ATTRIBUTE       MRV-Connect-Escape-Char        13       string          MRV

  # Accounting
  ATTRIBUTE       MRV-Acct-Command-Log            1       string          MRV
  ATTRIBUTE       MRV-Acct-Audit-Log              2       string          MRV
```

3. Restart the RADIUS daemon. You can now start using your new vendor configuration.

RADIUS Vendor Specific Attribute Settings

Possible settings for the RADIUS Vendor Specific attribute are:

```
MRV-Remote-Access-List = [Telnet Ssh Web_Server Console]
MRV-Port-Access-List = [# or Range] (example 1-48)
MRV-Outlet-Access-List = [port async # :outlet #] (example: 8:1, 8:4)
MRV-Outlet-Group-Access-List = [group#] (example: 3, 7)
MRV-Login-Mode = [shell]
MRV-Menu-Name = [menu file name] (example: /config/M_demo_menu)
MRV-Web-Menu-Name = [web menu file]
MRV-User-Prompt = [string]
MRV-Command-Logging = [string] (example: [radius syslog])
MRV-Audit-Logging = [string] (example: [radius syslog])
MRV-Web-Login-Mode = [string] (example: [menu])

# Accounting
MRV-Acct-Command-Log = [string]
MRV-Acct-Audit-Log = [string]
```

NOTE: Radius Accounting must be configured on the serial port for the new vendor specific attributes "`MRV-Command-Logging`" and "`MRV-Audit-Logging`" to work.

NOTE: A login mode of "Menu" is required to run a menu on the CLI. A Web login mode of "Menu" is required to run a menu when logging into the GUI.

Some values are mandatory for you to be granted access, and have definable defaults on the host. The mandatory attributes are Username and Password. The more attributes given, the more you can fit the session to your needs.

NOTE: If there is no Service-Type, the session is granted as a "NAS-Prompt-user," not an "administrator".

The following lists some sample attributes:

```
ATTRIBUTE MRV-Remote-Access-List
Example:
"bob" User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Remote-Access-List = "Ssh"

ATTRIBUTE MRV-Port-Access-List (simple user on port 8)
Example:
"bob"  User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Port-Access-List = "8"

ATTRIBUTE MRV-Outlet-Access-List (power unit on port 8)
Example:
"bob" User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Outlet-Access-List = "8:1-8"

ATTRIBUTE MRV-Outlet-Group-Access-List
Example:
"bob" User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Outlet-Group-Access-List = "1"

ATTRIBUTE MRV-Login-Mode
Example:
"bob"  User-Password == "bob"
Service-Type = Administrative-User,
MRV-Login-Mode = "shell"

ATTRIBUTE MRV-Menu-Name (file demo_menu)
Example:
"bob" User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Menu-Name = "/config/M_demo_menu"
MRV-Login-Mode = “menu”
```

```
ATTRIBUTE MRV-Web-Menu-Name
Example:
"bob"  User-Password == "bob"
Service-Type = NAS-Prompt-User,
MRV-Web-Login-Mode = “Menu”,
MRV-Web-Menu-Name = "/config/M_demo_menu"

ATTRIBUTE MRV-Audit-Logging 10 string
Example:
"bob"  User-Password == "bob"
Service-Type = NAS-Prompt-User
MRV-Audit-Logging = “radius syslog”

ATTRIBUTE MRV-Acct-Command-Log 1 string
Example:
"bob"  User-Password == "bob"
Service-Type = NAS-Prompt-User
MRV-Command-Logging = “radius syslog”
```

Appendix H

Configuring rlogin Support

rlogin establishes a remote login session from your terminal on the LX to a remote machine named hostname. Each remote machine may have a file named /etc/hosts.equiv containing a list of trusted hostnames with which it shares usernames. The remote authentication procedure determines whether a user from a remote host should be allowed to access the local system with the identity of a local user. Users with the same username on both the local and remote machine may rlogin from the machines listed in the remote machine's /etc/hosts.equiv file without supplying a password.

The rlogin feature enables a user to log onto a remote host system through a port on the LX, as shown in Figure 90 on page 438.

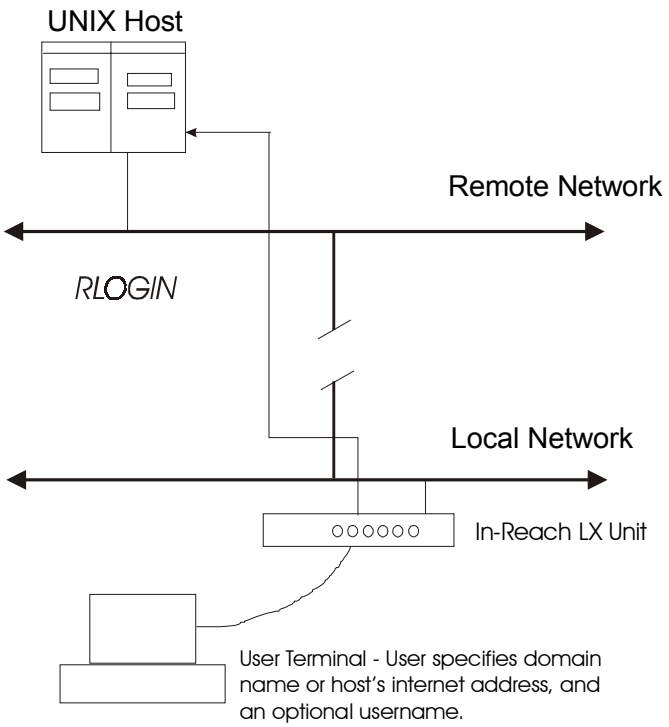


Figure 90 - Connecting to a Host through rlogin

The user enters the domain name or IP address of the host system, and an optional different username, one that the host recognizes. The LX unit passes its IP address to the host, along with the username entered on the CLI rlogin command line or the LX login username.

If the user did not enter a username on the rlogin command line, the LX unit forwards the login username of the port. Depending on the rlogin implementation at the UNIX host, this might be enough to allow the user to bypass the host's login routine.

Considerations

Each user must have an account on the remote host. Additionally, setting up the rlogin feature on the host may require you to modify other files. For example, on some UNIX hosts, you include an entry in /etc/hosts and the /etc/hosts.equiv file and, optionally, each user's .rhosts file. Then, when a user attempts to login to an account – using rlogin from an LX unit that matches an entry in the etc/hosts.equiv file – that user is automatically logged on to the host, as long as the user has a valid user account on the targeted remote host. The user is not prompted for a password.

The rlogin feature is disabled by default on the LX unit. For security reasons, you might not want to use the rlogin feature with sensitive accounts, however, since anyone who knows the right username can log on to the host.

Associated Commands

You can enable/disable rlogin through these commands:

Config:0 >>`rlogin enable`

Config:0 >>`no rlogin`

This command specifies that the user can make a connection using rlogin. The default is disabled.

`rlogin`

Log on to a host by specifying the username and host system.

fred:0>`rlogin 192.168.3.4`

where # username fred will be passed to the target host.

View information about an rlogin session.

InReach:0>`show users`

Displays a list of users, the session numbers, "rlogin", protocol, and the IP address with which the rlogin session was initiated.

Defining rlogin Dedicated Services

NOTE: With dedicated rlogin service, you cannot specify a different username for rlogin. the only valid username is the port's username.

NOTE: When you define a port for dedicated service the user will not be able to access the In-Reach prompt when disconnected from the preferred host. When you define a port as preferred service the user will see the LX prompt when the rlogin session is disconnected.

rlogin With Preferred Services

Use the show port command to display the current preferred service setting for the port subscriber. Use this command to enable a preferred service using rlogin.

NOTE: When you configure a subscriber with a Preferred Service, you set the subscriber's profile to point to a specific host name. Thereafter, when the subscriber enters the protocol rlogin, followed by a carriage return, the LX host automatically fills in the host argument with the configured Preferred Service.

Syntax

```
fred:0>rlogin

fred:0>rlogin username george

where #rlogin will pass along username george.
```

rlogin Transparent Mode

Use this feature to enable the LX to complete a ZMODEM transfer using the rlogin feature.

```
rlogin transparent 192.168.35.4
```

NOTE: Within an rlogin session, characters are passed raw (without interpretation) and transparently. This allows the ZMODEM transfer to complete.

Appendix I

FIPS Support

Overview

This appendix describes how to configure your LX-Series software to run in FIPS mode of operation.

Specific versions of the LX Series Software and associated ppciboot in conjunction with specific LX-Series Models will be FIPS 140-2 validated. MRV LX-Series FIPS approval is software version and hardware platform specific. See product data sheets, MRV FIPS literature, Web information and/or consult you sales representative for details.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

References

More information on the LX-Series FIPS 140-2 is available from the following sources:

- The MRV Communications website (http://www.mrv.com) contains information on the full line of products from MRV. Contact MRV for sales and support information.
- You can find the NIST Validated Modules at the following website: (http://csrc.ncsl.nist.gov/cryptval/)

What is FIPS?

FIPS 140-1 and its successor FIPS 140-2 are U.S. Government standards that provide a benchmark for implementing cryptographic software and hardware. They specify best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. This standard was published by the National Institute of Standards and Technology (NIST), and was adopted by the Canadian government's Communications Security Establishment (CSE), and by the financial community through the American National Standards Institute (ANSI).

When is FIPS a Mandatory Requirement?

FIPS 140-2 validation is required for sale of products implementing cryptography to the Federal Government. Although not all agencies are aware of this, more and more RFPs, contracts, and specifications are requiring FIPS 140-2 certification as a pre-requisite to bid proposals. While it was once possible to get a waiver signed, thus making a product exempt from these requirements for a limited amount of time, that practice was limited by FISMA. Therefore, obtaining a waiver is now rare.

The financial community increasingly specifies FIPS 140-2 as a procurement requirement and is beginning to embrace it, wholly or in part, in its own standards. Finally, the security community values products that have completed this evaluation, as it carries the sanction of an independent third party.

The FIPS 140-2 certification approval is tailored specifically for platforms containing both a Hardware and Software component. The LX-Series software and ppciboot in conjunction with the LX-Series Hardware platforms are the first series to be FIPS 140-2 validated, with other LX-Series platforms to follow.

The FIPS approval is tied to both the specific Hardware platform and Software version. All LX-Series platforms such as the LX-4000 Series and LX-1000 Series can run the FIPS version of LX software (linuxito and ppciboot).

However, it is important to note that the FIPS 140-2 certification will apply only to the FIPS validated version of software specifically configured to run in FIPS mode of operation on MRV LX-Series listed platforms.

Please take the time to review the following “Prerequisites” section.

Prerequisites

The following requirements must be met to be FIPS 140-2 validated:

- You must use the FIPS validated versions of the LX linuxito and ppciboot software. *Only specific versions of the LX software are validated by an independent third party lab.*
- You must be running the software on the FIPS validated LX-Series platform.
- FIPS must be enabled on the LX-Series FIPS validated unit(s).
- If you intend to use SNMP with FIPS, you must use the SNMP V3 version.
- If you intend to use the LX GUI with FIPS, you must use a FIPS validated version of the JRE. Sun Java JRE version 1.4.2 supplies the level of AES encryption required, but has not yet been validated.
- You must place the provided tamper proof labels in the proper locations.

Notes and Restrictions

- The default subscriber InReach password must be changed.
- The default ppciboot password must be changed.
- The default system password must be changed.
- All configured passwords must be greater than or equal to 6 characters in length.
- If using an SNMP NMS or SNMP MIB browser, the application must support SNMPV3 and must support AES encryption. By default SNMP is disabled for security reasons. SNMP V3 must be enabled and configured fully on the LX in order to function with the NMS.

- SSH Clients must support sshV2, AES or 3DES ciphers, and HMAC-SHA1 or HMAC-SHA1-96 message authentication codes.

Applying Tamper Evident Labels

NOTE: To be FIPS compliant, you must apply the tamper-evident labels before you power on and configure the LX unit.

Once the LX has been configured in FIPS mode, the cover cannot be removed without signs of tampering. Applying tamper-evident labels to the LX unit will prevent anyone from opening the unit without your knowledge.

To seal the cover of the LX, apply a tamper-evident label as follows:

1. Clean the LX surface of any grease or dirt before you apply the tamper-evident labels.
2. Apply two labels each to the bottom left and right sides of the unit, as shown in Figure 91.

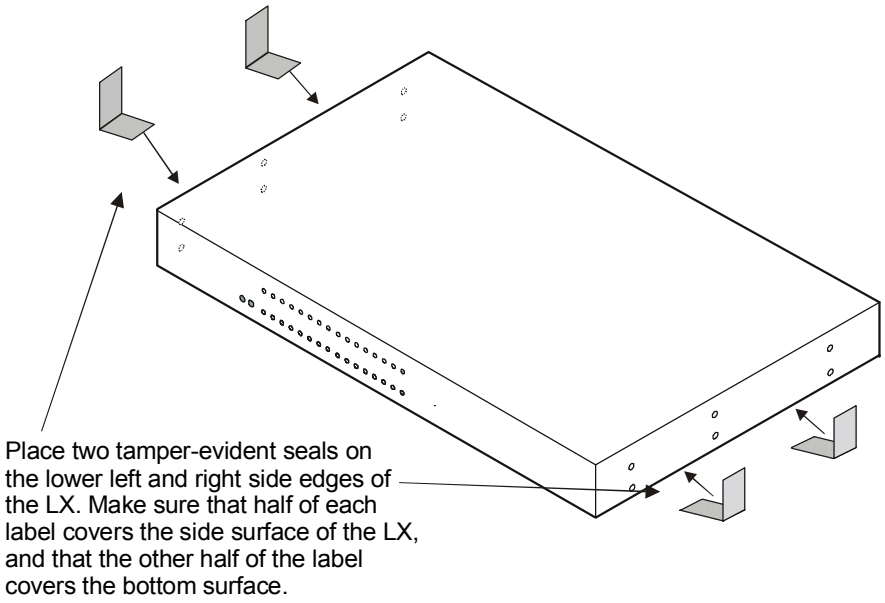


Figure 91 - Location of the Tamper Evident Labels

3. Record the serial numbers of the labels you attached to the LX unit.
4. Allow 24 hours for the adhesive in the tamper-evident labels to cure.

NOTE: You should periodically check the labels to ensure that no one has tampered with the unit.

Making Sure Your Software is FIPS 140-2 Validated

Do the following to determine if the software you are running has been FIPS 140-2 validated:

1. Log into the CLI.
2. Enter the `show version` command at the **InReach:0 >** prompt; for example:

   InReach:0 >`show version`

The Show Version screen appears, with the relevant fields highlighted.

```
Linux Kernel Version:           2.6.11
Linux In-Reach Version:             99
Software Version:                x.x.x (FIPS)
Ppciboot Version:                x.x.x (FIPS)
```

Figure 92 - Show Version Screen

If the software you are running has been validated by an independent lab, the word `(FIPS)` appears to the right of the `Software Version` number and the `Ppciboot Version` number. If `(FIPS)` does not appear, your software has not been validated.

Enabling FIPS Mode of Operation

IMPORTANT!

If you want to configure your unit to run FIPS Mode of Operation, you must do so ***before*** you attempt to configure the unit over and above the default settings. The act of enabling FIPS mode will default the unit's configuration.

When FIPS is enabled, the configuration file is returned to defaults. Therefore, if you fully configured your unit and then turned on FIPS, your configuration will return to factory defaults. FIPS mandates this to ensure that any passwords with fewer than six characters are purged, and that all unsupported applications are disabled.

NOTE: If you enable FIPS Security, option `[1] Boot from Network` is set to `Flash Only` automatically. You can only update from the CLI or GUI while FIPS is enabled. Option `[4] Update ppciboot Firmware` is disabled when FIPS is enabled.

The following passwords must be at least six characters long:

- Subscriber
- Config
- ppciboot
- Radius Secret
- TACACS+ Secret
- PAP/CHAP Outgoing Secret
- SSH Public Key must be at least 1024 bits.

The `FIPS 140-2 Security` option lets you enable or disable FIPS mode of operation.

```
            Welcome to In-Reach ppciboot Version 3.6.0
                        Main Menu
  [1] Boot from network:      Flash
  [2] Time Out, in seconds (0=disabled): 8
  [3] IP Configuration Menu
  [4] Update ppciboot Firmware
  [5] Ethernet Network Link
  [6] Change ppciboot Password
  [7] FIPS 140-2 Security:                                    yes
  [*] Reset to System Defaults
  [S] Save Configuration
  [B] Boot System
  Make a choice:
           __
```

To enable or disable FIPS security:

1. Press the number `7 (FIPS 140-2 Security)`. The following prompt appears:

   ```
   Enabling FIPS security will reset run-time
   configuration to defaults. Are you sure? (y/n):
   ```

2. If you select `y` (this defaults the flash immediately), a `Resetting Linux Configuration` message appears, and the Main Menu reappears after a few seconds. If you select `n`, the Main Menu reappears immediately.

3. If FIPS is already enabled and you want to disable it, press `7 (FIPS 140-2 Security)` from the Main Menu.

4. Press `B` to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration.

Changing the Default ppciboot Password

After enabling FIPS, you must enter a new ppciboot password of greater than six characters.

The `Change ppciboot Password` option lets you change the ppciboot password for the unit. To change the ppciboot password:

1. Press the number `6 (Change ppciboot Password)`. The following prompt is displayed:

   Enter your current ppciboot password:

   Enter the current ppciboot password at the above prompt. After you have entered the current ppciboot password, the following prompt is displayed:

   Enter your NEW password: :

2. Enter the new ppciboot password at the above prompt. The password must be greater than six characters long.

   After you have entered the new ppciboot password, the following prompt is displayed:

   Re-enter your NEW password:

Re-enter the new ppciboot password at the above prompt. A confirmation message is displayed.

Changing the Default Subscriber Password

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 must change the InReach user's password to something other than **access**. The password must be at least six characters long.

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.

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:0 >>`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 Configuration Password

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, you must change this password to something other than **system**. The password must be at least six characters long.

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

1. Access 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: **********

FIPS Mode Console Access

When the LX is in FIPs mode telnet is not allowed. Therefore, you must ssh to the unit in Version 2 mode

```
ssh -l InReach 10.10.10.10
```

If non-FIPS approved algorithms are being used, please see and edit the `/etc/ssh/ssh_config` file on your host system.

Applications Unsupported in FIPS Mode of Operation

Listed below are all the unsupported FIPS protocols and features, which are disabled when FIPS mode of operation is enabled on the LX software.

Table 15 - Unsupported FIPS Protocols and Features

Feature	Impact	Reason
Telnet client/server	Disabled	Passwords are passed in plaintext
rlogin client	Disabled	Passwords are passed in plaintext
Web GUI unencrypted	Disabled	Only AES encryption mode will be supported, customer is required to run FIPS approved JRE on host machine
SNMP v1 & v2	Disabled	Community strings are passed in plaintext
SSH V1 Client / Server	Disabled	Security flaws / known vulnerabilities
Passwords/ Secrets less than 6 characters	Disabled	Due to FIPS max authentication fail attempts
Linux shell access	Restricted	Limited, restricted

Boot or load software image from network	Disabled	FIPS requires DSA signatures on images, units must boot from FLASH
Updating ppci-boot.img from ppci-boot menu	Disabled	FIPS requires ppciboot to be updated from runtime software via CLI or GUI
LDAP	Disabled	Passwords passed in plaintext
Login mode shell	Disabled	Unfettered access
Broadcast Groups	Limited	No support for groups that have a master/ slave of TCP
Fingerd	Disabled	Allows anyone to see who is logged in
Boot config from network (tftp)	Disabled	Configuration sent in plaintext
Save config to network (tftp)	Disabled	Configuration sent in plaintext
No authentication	Disabled	Insecure
Dedicated Services	Disabled	Passwords are passed in plaintext
Port Async Connect	Disabled	Insecure
TCP Pipe	Disabled	In plain text

Upgrading Software

The `ppciboot.img.sign` and `linuxito.img.sign` digital signature files are used to authenticate load images. Place these files on the TFTP server. The LX unit will download them automatically.

Refer to “How to Upgrade the Software” on page 88 for more information on upgrading the software.

FIPS JCE Module Commands

NOTE: These commands apply only if you want to use the GUI in FIPS mode.

NOTE: You can purchase FIPS compliant JCE modules from two vendors. The vendors are listed below, along with the specific JCE Module name.

- IBM – IBMJCEFIPS
- RSA – JSafeJCE

NOTE: These commands are available only when the LX is running in FIPS Mode.

A new FIPS JCE Module command allows you to name the web server FIPS JCE Module. You can access it in the Configuration Command Mode.

Configuring a Web Server FIPS JCE Module Name

Use the following command to configure a Web Server FIPS JCE Module name. The module name is set by the module vendor. For example, if you are using RSA's JSafe cryptology module, the module name would be `JSafeJCE`. Enter `no web_server fips jcemodule` to reset to the default, which is "null". The module name can be up to 16 characters long.

Config:0>>`web_server fips jcemodule <module_name>`

Examples

Config:0>>`web_server fips jcemodule JSafeJCE`

Config:0>>`no web_server fips jcemodule`

Viewing the Web Server FIPS JCE Module Name

Use the `show system characteristics` command to display the System Characteristics Screen. An example of this screen follows, with the new `Web JCEModule` field highlighted:

```
Name:                          In-Reach  Time:   Sat, 01 Jan 2005 06:01:49 UTC
Serial Number:      00:a0:9c:00:02:b1  Authenticate Image:           Enabled
Location:
Domain Name suffix:
Maximum Number of Async Ports:     42  Internal Modem on Port:            41
Maximum Number of Subscribers:    100  LX Model Type:            LX-8040-101
Maximum Number of Interfaces:      86  Maximum Number of Ethernet Ports:   1
Primary Domain :              0.0.0.0  Secondary Domain :            0.0.0.0
Gateway :                     0.0.0.0  Default TFTP Server : 120.179.169.188
Timed Daemon:                Disabled  TFTP Retries:                       3
NTP   Daemon:                Disabled  TFTP Timeout:                       3
NTP   Server:                 0.0.0.0  NTP Server Alternate:         0.0.0.0
NTP IPv6 Server:                         3ffe:303:11:2222:220:edff:fe4b:fc67
NTP IPv6 Server Alternate:               3ffe:303:11:2222:220:edff:fe4b:fc68
Finger Daemon:               Disabled  Logging Size :                  64000
Telnet Server:               Disabled  Telnet Client:               Disabled
Web Server:                   Enabled  Web Server Port:                   80
Web Server Timeout:                20  Web JceModule:               JsafeJCE
Web Encrypt:                  Enabled  Web Banner:                   Enabled
Subscriber Debug Option:     Disabled  Trigger-Action Debug Option: Disabled
System Debug Option:         Disabled  Flash Debug Option:          Disabled
Minimum Password Length:            6  SSH Daemon:                       V2
Rlogin Client:               Disabled  Message Feature:             Disabled
SNMP Feature:                Disabled
Modem Pool Enabled Serial Ports:
```

Figure 93 - Show System Characteristics Screen, with Web JCEModule

INDEX

U

W