LX-Series Configuration Examples

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

451-0322B

All rights reserved. No part of this publication may be reproduced without the prior written consent of MRV Communications, Inc. The information in this document is subject to change without notice and should not be construed as a commitment by MRV Communications, Inc. MRV Communications, Inc. reserves the right to revise this publication and to make changes in content from time to time, without obligation to provide notification of such revision or changes. MRV Communications, Inc. assumes no responsibility for errors that may appear in this document.

Copyright © 2004 by MRV Communications, Inc.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptosoft.com).

This product includes software written by Tim Hudson (tjh@cryptosoft.com).

Service Information

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

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

Secure Shell Disclaimer

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

Table of Contents

Figures

Preface

This book contains examples of how to configure the LX CLI for various applications.

How This Book is Organized

This guide is organized as follows:

- **Chapter 1** – Provides server-level configuration examples. The examples in this chapter include the following: Loading a Configuration File, Saving and Editing Configuration Files, Specifying the IP Address of the LX Unit, Configuring Network Security with IP Filter Rules, Configuring SNMP, and configuring SSH.
- **Chapter 2** – Provides examples of how to set up server-based authentication and accounting. This chapter includes examples of setting up RADIUS Authentication and Accounting, setting up TACACS+ Authentication and Accounting, and setting up SecurID Authentication.
- **Chapter 3** – Provides port-configuration examples for the LX unit. This chapter includes examples of customizing asynchronous port settings and configuring asynchronous ports for Data Buffering, Pattern Matching, Console Management, Power Management, Sensor Management, and PPP (Point-to-Point Protocol) Sessions.
- **Chapter 4** – Provides configuration examples for the Notification Feature. This chapter includes an example of configuring syslogd messages and examples of configuring the Notification Feature for each of the eight Service Types (Protocols).
- **Chapter 5** – Provides a configuration example for the Menu Feature. This chapter includes an example that shows how to create a menu for a subscriber.

- **Chapter 6** – Provides Subscriber configuration examples. This chapter includes examples of assigning a Menu to a subscriber, configuring the Dialback Feature for a subscriber, and configuring a Trusted Key for a subscriber.
- **Chapter 7** – Provides configuration examples for IP Interfaces and Broadcast Groups. This chapter includes examples that show how to create an IP Interface, assign Broadcast Groups to an IP Interface, and configuring an IP Interface as a Rotary.
- **Appendix A** - Explains advanced features, such as Multi-level command execution.

Conventions

The following conventions are used throughout this guide:

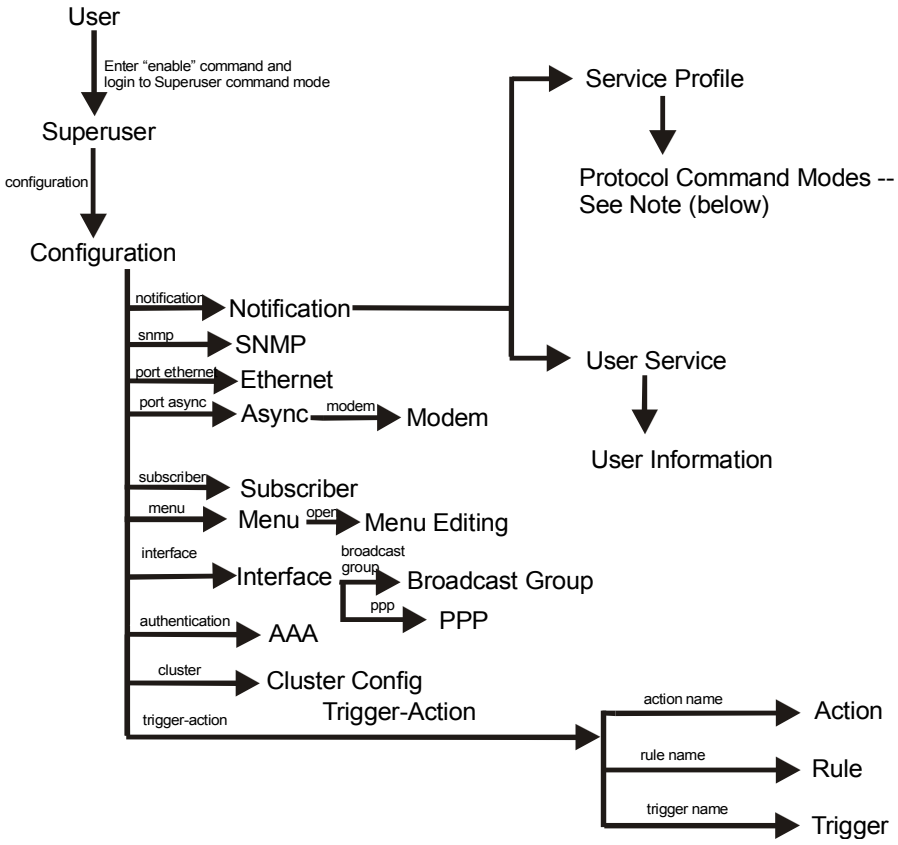
- **Command execution –** Unless otherwise specified, commands are executed when you press <RETURN>.
- **Command syntax –** Where command options or command syntax are shown, keywords and commands are shown in lowercase letters.
- **Keyboard characters (keys)** – Keyboard characters are represented using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

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 rest of this 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*.

Cluster Command Mode – Contains commands for configuring, sharing parameters, 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*.

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*.

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
cluster            Superuser cluster commands
configuration      Enter configuration mode
```

```
connect            Connect to a remote access port  async
                   on this LX unit
control           Control port async output signals
debug             Set debug options
dial              Dial a dialout modem
exit              Exit up one level
logout             Logout device, port, process or user
menu              Menu utility
message           Send a message to a logged on user
monitor           Monitor running system information
no                Negate a command
notify            Send message to syslog
outlet            Manipulate outlets
pause             Set the page mode
ping              Send echo messages
reload            Restart the Unit
restart           Restart notification
rlogin            Open a rlogin connection
save              Save configuration
script            Run a script file
send              Send an snmp trap message
setup             Run Quick Start configurator
shell             Run a shell as Superuser
show              Show running system information
ssh               Secure Shell
telnet            Open a telnet connection
terminal          Set the terminal type
update            Update software or ppciboot
zero              Clear statistics and logs
```

- 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 using the LX unit, refer to the *LX-Series Configuration Guide* (P/N 451-0311).

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

Server-level Configuration Examples

This chapter provides server-level configuration examples. The examples in this chapter include the following:

Loading a Configuration File

This example shows how to load a configuration file from a TFTP server. For background information on this task, refer to "Creating and Loading a Default Configuration File" in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisite for this task is the following:

- Install and configure the LX unit as described in the *LX Quick Start Instructions* (451-0312G).

Procedure

To load a configuration file from a TFTP server, do the following:

1. Connect a terminal to the Diag port and press <Enter> one or two times.

   The ppciboot Main Menu is displayed (see Figure 2).

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

Figure 2 - ppciboot Main Menu

2. At the Main menu, enter 5 to open the IP Configuration menu (see Figure 3).

```
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:
```

Figure 3 - IP Configuration Menu

3. Choose option 8 to define the TFTP Server IP address.
4. Enter S to save the configuration.
5. Enter R to return to the Main Menu.
6. Enter B to reboot.
7. Once the unit has loaded, access the CLI Config level.

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

8. Define the TFTP server IP address:

Config:0 >>`ppciboot tftp server 10.10.10.1`

9. Specify that the LX unit will be booted from the TFTP server that you specified in step 8:

   Config:0>>`boot config from network 10.10.10.1 filename`

10. Go to the Superuser Command Mode:

    Config:0 >>`end`

11. Save the configuration file to flash:

    InReach:0 >>`save config flash`

12. Boot the LX unit:

    InReach:0 >>`reload`

13. After the LX unit has rebooted, log on to it and verify that the LX unit has rebooted from the proper place:

    InReach:0 >`show system status`

The following System Status screen shows that the LX unit rebooted from the TFTP server that was specified in step 8 (`10.10.10.1`) and the filename that was specified in step 9 (`filename`).

```
Time:   Mon, 23 Jun 2004 20:17:20 UTC  System Uptime:                0 8:7:50

Software Load From                 :                      Local Flash Memory
Active System Gateway              :                            102.19.169.1
Configuration Load From            :                      Local Flash Memory
Network file Name                  :
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

CPU usage (0.10 = 10%):                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

PowerFail Log:  Feb 24 21:54:33 2003
```

Figure 4 - System Status Screen

Specifying the IP Address of the LX Unit

This example shows how to specify an IP address for the LX unit from the LX CLI.

Prerequisites

The prerequisites for this task are the following:

- Install and configure the LX unit as described in the *LX Quick Start Instructions* (451-0312G).

Procedure

To specify the IP address of the LX unit, do the following:

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. Enter the Interface Command Mode for Interface 1:

   Config:0 >>`interface 1`

   NOTE: Interface 1 is the default IP interface for the LX unit.

3. Specify an IP address for Interface 1 (add mask here as well if you need to change it):

   Intf 1-1:0>>`address 10.240.10.234 mask 255.255.255.0`

4. Verify the IP configuration of Interface 1:

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

```
Time:                                          Mon, 24 May 2004 16:14:27
Interface Name:          Interface_1  Bound to :                     eth0
IP MTU Size:                1500  Unnumbered Interface: First Available
IP Address   :            0.0.0.0  Learned IP Address  :         0.0.0.0
IP Mask      :            0.0.0.0  Learned IP Mask     :         0.0.0.0
IP Broadcast :            0.0.0.0  Learned IP Broadcast:         0.0.0.0
Interface Status:           In Use  Learned IP Gateway  :         0.0.0.0
Interface Banner:            Local  Learned IP DNS      :         0.0.0.0
Authentication:              Local  Radius Accounting:           Disabled
Authentication FallBack:  Disabled  Tacacs+ Accounting:          Disabled
SSH port:                       22  Telnet port:                       23
SSH Keepalive Interval:          0  SSH Keepalive Count:                3
```

Figure 5 - Interface Characteristics Screen

Saving and Editing Configuration Files

This example shows how to create a configuration file which you can load on multiple units.

1. Create an empty `.zip` file on the TFTP server with write permissions. The prefix of the zip filename consists of the last six digits of the LX mac address appended to `lx` (e.g., `lx12ab9f`):

   ```
   -rw-rw-rw- 1 root other lx12ab9f.zip
   ```

2. Save the configuration to the TFTP server:

   ```
   InReach:0>>save configuration network lx12ab9f 10.10.10.1
   ```

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

3. Next move the file to its own directory and unzip the zip file.

4. You can edit the configuration files for other LX units.

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

   ```
   zip -o lx12ab9f.prm file1 file2 file3
   ```

   where `lx12ab9f.prm` is automatically named filename.zip. The filename.zip file is the archive you are writing the files to, and file1, file2, and file3 are the files you are adding to the archive.

6. In Windows, select the files you want to add to the zip file by clicking on them while holding down the **Ctrl** key.

   Right click on the selected files and select **Add to Zip**.

7. You can use this .zip 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.

Configuring Network Security (IP Filter Rules)

This example shows how to configure IP filter rules for the LX unit. For background information on this example, refer to Chapter 10 ("Configuring Packet Filters with the `iptables` Command") and Appendix D ("Details of the `iptables` Command") in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisites for this task are the following:

- This task must be performed in a subscriber account that has a security level of `shell` or `superuser`.

Procedure

The following steps would typically be performed to create IP Filter rules for the LX unit:

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

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

2. Enter the Linux shell:

```
InReach:0>>shell
```

   The Linux command prompt (e.g., **InReach:/#**) is displayed in the shell.

   NOTE: The commands that are executed in the Linux shell are case-sensitive and can not be abbreviated.

3. Display the existing IP Tables chains:

```
InReach:/# iptables -L
```

4. Create an INPUT rule that will drop any packets coming to the LX from the source address 10.240.10.240:

   InReach:/# `iptables -A INPUT -s 10.240.10.240 -j DROP`

5. Create an OUTPUT rule that will drop any packets originating from the LX that are destined for the IP address 10.128.1.13:

   InReach:/# `iptables -A OUTPUT -d 10.128.1.13 -j DROP`

6. Verify the IP Tables configuration:

   InReach:/# `iptables -L`

   Figure 6 shows an example of the screen that the `iptables -L` command displays.

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.240.10.240        anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             10.128.1.13

Chain tcp_allow (0 references)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere          tcp flags:SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere             anywhere          state RELATED,ESTABLISHED
DROP       tcp  --  anywhere              anywhere
```

Figure 6 - IP Tables Configuration Display

Figure 6 contains the following entry for the INPUT Filter Chain, which prove that the rule created in step 4 was added to the IP Tables configuration:

```
DROP       all  --  10.240.10.240        anywhere
```

Figure 6 contains the following entry for the OUTPUT Filter Chain, which proves the rule created in step 5 was added to the IP Tables configuration:

```
DROP       all  --  anywhere             10.128.1.13
```

7. Save the changes to the `/config/iptables.conf` file.

   InReach:/# `iptables-save -f /config/iptables.conf`

8. Execute the `exit` command to return to the Superuser Command Mode:

   InReach:/# `exit`

9. Save the modified `iptables.conf` file to flash:

   InReach:0>>`save configuration flash`

   NOTE: If you have a TFTP server configured, you can save the modified `iptables.conf` file to the TFTP server. The following command could be used to save the modified `iptables.conf` file to the TFTP server:

   InReach:0>>`save config network unit1 119.25.42.37`

   where unit1 is the filename.

   Now your changes will be permanent through a reload from the network.

Configuring SNMP on the LX

This example shows how to configure SNMP on the LX.

Prerequisites

The prerequisites for this task are as follows:

- A client must be on the network.
- A Network Management System (preferably OpenView).

Procedure

To configure SNMP on the LX, do the following:

1. Login and move to the Config level.

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

2. Configure the get client address.

```
Config:0 >>snmp get client 1 10.240.10.100
```

3. Configure the get community for client 1

```
Config:0>>snmp get client 1 community test
```

4. Configure the set client address.

```
Config:0 >>snmp set client 1 10.240.10.100
```

5. Configure the set community for client 1:

```
Config:0>>snmp set client 1 community test
```

6. Configure the trap client address.

```
Config:0 >>snmp trap client 1 10.240.10.100
```

7. Configure the trap community for client 1:

```
Config:0>>snmp trap client 1 community test
```

8. Configure the contact text string for mib object sysContact.

```
Config:0 >>snmp contact Mike Smith
```

9. Configure the location text string for mib object sysLocation.

```
Config:0 >>snmp location Boston MA
```

10. Verify the SNMP settings.

```
Config:0>> end
```

```
InReach :0>> show snmp client 1
```

```
Get Client:                    1  Address:          140.111.222.111
Community:                public  NetMask:            255.255.255.0
Version:                       1

Set Client:                    1  Address:          140.111.222.111
Community:               private  NetMask:            255.255.255.255
Version:                       1

Trap Client:                   1  Address:          140.111.222.111
Community:                public  Version:                        1
UDP Port:                   162
```

Figure 7 - SNMP Client Screen

11. To save the file, enter:

```
InReach :0>> save config flash
```

Configuring SSH On the LX

This example shows how to configure SSH on the LX.

Prerequisites

You must have a Preferred Service configured for your LX unit. (The default SSH server is your Preferred Service.) Refer to the `preferred service` command in the *LX-Series Configuration Guide* for information on configuring a Preferred Service.

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. Enable the LX unit to function as an SSH server:

   Config:0 >>`ssh enable`

3. Access the Interface Command Mode for the default IP Interface (Interface 1) of the LX unit:

   Config:0 >>`interface 1`

4. Specify the UDP port for making an SSH connection to the IP interface:

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

5. Specify the SSH Keepalive Count for the IP interface:

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

6. Specify the SSH Keepalive Interval for the IP interface:

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

7. Specify the SSH Version for the IP interface:

   Intf 1-1:0 >>`ssh v2`

8. Specify unique SSH socket numbers for serial ports on the LX unit:

   Intf 1-1:0 >>`serial 1 ssh 8234`

   Intf 1-1:0 >>`serial 2 ssh 8560`
   Intf 1-1:0 >>`serial 3 ssh 6888`
   Intf 1-1:0 >>`serial 4 ssh 5734`

9. Verify the Port Mapping that you specified in step 8:

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

```
Serial Port   Telnet Port   SSH Port
     0              0          0
     1           2100       8234
     2           2200       8560
     3           2300       6888
     4           2400       5734
     5           2500       2522
     6           2600       2622
     7           2700       2722
     8           2800       2822
```

Figure 8 - Port Mapping Screen

Trigger-Action – Turning Off an Outlet Based on a Temperature Sensor Reading

NOTE: In releases 3.2.0 and higher, pattern matching is no longer configured as a port parameter. It is now configured under Trigger-Action.

The following example explains how to turn off an outlet based on a temperature value via Trigger-Action.

Prerequisites

You must have the port 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 2
   ```

   where 2 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       Errors: 0
                                 Port: 5
                           Hysteresis: +/-2 Celsius
                           Temperature: > 25 Celsius
```

Figure 9 - Show Trigger Action Screen

15. At the `InReach:0>>` prompt, enter:

    `show trigger-action action name temp-ac-power-off`

    The following lines appear:

    `Action Name: temp-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
Action Name: temp-power-off Command: outlet 11:5 off
```

Figure 10 - Show Trigger Rule Name Characteristics Screen

Refer to the *LX-Series Configuration Guide* for more information on Trigger Action.

Cluster Configuration and Control

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.

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 Configuration and Control is in the Configuration Command Mode. To access it, type the following:

Config:0>>`cluster`

Creating a Cluster Secret at the Quick Configuration Menu

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. The LX unit that pushes its configuration to the cluster is thought to be the master. When configuring the shared IP address on the master, be sure to include its own address on the list as well.

Prerequisites

None.

Procedure

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). It is recommended that your terminal also be set to Autowrap.
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                    0.0.0.0
          2 Subnet mask                        0.0.0.0
          3 Default Gateway                    0.0.0.0
          4 Domain Name Server
          5 Domain Name Suffix
          6 Cluster Secret               Not Configured
          7 Superuser Password
          8 Exit and Save
Enter your choice:
```

Figure 11 - Quick Configuration Menu

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
             8 Exit and Save
  Is this information correct?  (y/n) :
```

Figure 12 - Configuration Summary

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.

Creating a Cluster

This example shows you how to create a cluster.

Prerequisites

None.

Procedure

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.

3. To see the members of the cluster, enter:

   InReach:0>`show cluster characteristics`

```
Time:   Sun, 08 Jul 2004 22:22:47 UTC  System Name:           In-Reach
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
Timed is being shared
Fingerd is being shared
LogSize is being shared
Gateway1 is being shared
Dns1 is being shared
Dns2 is being shared
Subscriber billm is being shared
Subscriber timb is being shared
```

Figure 13 - Show Cluster Characteristics Screen

Sharing an Attribute

This example explains how to share attributes.

Prerequisites

All cluster members must have a secret configured and enabled.

Procedure

1. To share attributes; see the following examples:

   To get a list of the supported shared parameters:

   Cluster:0>> `share ?`

```
all               Share/unshare all available parameters
finger            Share/unshare finger daemon enable/disable
gateway           Share/unshare gateway address
ldap              Share/unshare ldap configuration
logging           Share/unshare logging size
ntp               Share/unshare ntp settings
outlet            Share/unshare outlet access
port              Share/unshare port async configuration
primary           Share/unshare primary dns server
radius            Share/unshare Radius configuration
secondary         Share/unshare secondary dns server
securid           Share/unshare SecurID configuration
service           Share/unshare service configuration
snmp              Share/unshare SNMP information
ssh               Share/unshare ssh daemon enable/disable
subscriber        Share/unshare subscriber configuration
tacacs+           Share/unshare TACACS+ configuration
telnet            Share/unshare telnet daemon enable/disable
tftp              Share/unshare tftp configuration
timed             Share/unshare timed daemon enable/disable
timezone          Share/unshare timezone configuration
webbanner         Share/unshare web banner configuration
web_server        Share/unshare web server configuration
```

Figure 14 - Share Attributes List

   To share subscriber bob:

   Cluster:0>> `share subscriber bob`

To share the SecurID Config as on the master machine:

Cluster:0>> `share securid`

To share all attributes:

Cluster:0>> `share all`

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 an actual change is made.

```
Time:   Sun, 08 Feb 2004 22:22:47 UTC  System Name:            In-Reach
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
Timed is being shared
Gateway1 is being shared
Dns1 is being shared
Dns2 is being shared
Subscriber billm is being shared
Subscriber timb is being shared
```

Figure 15 - Show Cluster Characteristics

Chapter 2

Setting Up LX Authentication and Accounting

This chapter provides examples of how to set up authentication, and (in the case of RADIUS and TACACS+) accounting, for the LX unit. The examples in this chapter include the following:

- RADIUS Authentication and Accounting (see below)
- SecurID Authentication (see page 54)
- TACACS+ Authentication and Accounting (see page 59)

RADIUS Authentication and Accounting

This example shows how to configure RADIUS security for the LX unit. For background information on this task, refer to "Setting Up RADIUS" in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisites for this task are the following:

- Set up the RADIUS authentication server(s), and the RADIUS accounting server(s), for the LX unit. For background information on this task, refer to "Installing and Configuring the RADIUS Server on a Network-based Host" in the *LX-Series Configuration Guide*.
- Ensure that the LX unit can ping its RADIUS authentication server(s) and RADIUS accounting server(s). For more information, refer to the `ping` command in the *LX-Series Commands Reference Guide*.

Procedure

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

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

2. Specify the RADIUS primary server address:

   AAA:0 >>`radius primary authentication server address 10.240.10.150`

3. Specify the RADIUS primary server secret:

   AAA:0 >>`radius primary authentication server secret boston`

4. Specify the RADIUS primary accounting address:

   AAA:0 >>`radius primary accounting server address 10.240.10.150`

5. Specify the UDP port that the RADIUS Primary Authentication Server will use to listen to the LX unit:

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

6. Specify the maximum number of retries that the LX unit will have for sending an Access Request to the RADIUS Primary Authentication Server:

   AAA:0 >>`radius primary authentication server retransmit 3`

7. Specify the length of time that the LX unit will wait for the RADIUS Primary Authentication Server to respond before retransmitting packets:

   AAA:0 >>`radius primary authentication server timeout 3`

8. Specify the interval at which the LX unit will update the RADIUS accounting server with the status of each RADIUS user:

   AAA:0 >>`radius period 10`

9. Exit the AAA Command Mode and access the Asynchronous Command Mode for the asynchronous ports that you want to configure for RADIUS authentication:

   AAA:0 >>`exit`
   Config:0 >>`port asynchronous 3`

10. Specify RADIUS as the method of inbound authentication for the port:

    Async 3-3:0>>`authentication inbound radius enable`

11. Specify RADIUS as the method of outbound authentication for the port:

    Async 3-3:0>>`authentication outbound radius enable`

12. Enable RADIUS accounting on the port:

    Async 3-3:0>>`radius accounting enable`

13. Verify that RADIUS is enabled on the port that you specified in step 9 and step 11:

    Async 3-3:0 >>`show port async 3 characteristics`

The highlighted fields on the following Port Characteristics Screen show that RADIUS is enabled on the port that you specified in step 10 and step 11:

```
Time:                                          Sat, 10 Jan 2004 04:01:20 UTC
 Banner:        /config/banner.default  Banner Display:               Both
 Port Number:                       3  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:                 Auto Dial:                   Disabled
 Inbound Authentication:        Radius Autohangup:                   Enabled
 Outbound Authentication:       Radius Radius Accounting:            Disabled
 Authentication FallBack:     Disabled Tacacs+ Accounting:           Disabled
 Data Buffer Size:                1024 Data Buffer Display:            Prompt
 Data Buffer Syslog:          Disabled Data Buffer Time Stamp:       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
 Connect Command:
```

Figure 16 - Port Characteristics Screen

14. Verify that the RADIUS primary server address and the RADIUS primary server secret have been configured:

    Async 3-3:0 >>`show radius characteristics`

    The highlighted fields on the following RADIUS Characteristics Screen show that the RADIUS primary server address and the RADIUS primary server secret have been configured.

```
Time:                                  Wed, 10 Apr 2002 00:44:48 UTC
Primary RADIUS Authentication Server:
IP Address: 10.240.10.150              RADIUS Auth. UDP Port: 1812
Secret:     Configured                 Timeout:                  4
Retry:      4

Secondary RADIUS Authentication Server:
IP Address: 0.0.0.0                    RADIUS Auth. UDP Port: 1812
Secret:     Not Configured             Timeout:                  4
Retry:      4

Primary RADIUS Accounting Server:
IP Address: 0.0.0.0                    RADIUS Acct. UDP Port: 1813
Secret:     Not Configured             Timeout:                  4
Retry:      4

Secondary RADIUS Accounting Server:
IP Address: 0.0.0.0                    RADIUS Acct. UDP Port: 1813
Secret:     Not Configured             Timeout:                  4
Retry:      4

Local Subscriber: Disabled
RADIUS Accounting Server Period: 1280
Inbound RADIUS Enabled Serial Ports:
Outbound RADIUS Enabled Serial Ports: 3
RADIUS Enabled Interfaces:
```

Figure 17 - RADIUS Characteristics Screen

Notes

The parameters that can be configured for the RADIUS Authentication and Accounting Servers include **IP address**, **UDP port**, **Retransmit Value**, **Server Secret**, and **Timeout**.

Refer to Chapter 4 of the *LX-Series Commands Reference Guide* for descriptions of the commands that are used to configure parameters for each type of RADIUS Server.

Each RADIUS Server command begins with a string specifies the type of RADIUS Server that it applies to; for example `radius primary authentication server`, `radius primary accounting server`, `radius secondary authentication server`, and `radius secondary accounting server`.

SecurID Security (Version 5 Example)

This example shows how to configure Version 5 of SecurID for the LX unit. For background information on this task, refer to "Setting Up SecurID" in the *LX-Series Configuration Guide*.

NOTE: This example shows how to configure Version 5 of SecurID. If you want to configure a legacy version of SecurID, refer to "SecurID Security (Legacy Example)" on page 57.

Prerequisites

The prerequisites for this task are the following:

- Set up the SecurID server(s) for the LX unit. For background information on this task, refer to "Installing and Configuring the SecurID Server on a Network-based Host" in the *LX-Series Configuration Guide*.

  NOTE: In addition to the SecurID authentication server, replica SecurID servers can be configured for Version 5 of SecurID. For more information on SecurID replica servers, go to http://www.rsasecurity.com/products/securid/index.html.

- The SecurID application must be running on the SecurID Server.

- Ensure that the LX unit can ping the SecurID server(s). For more information, refer to the `ping` command in the *LX-Series Commands Reference Guide*.

Procedure

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

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

2. Specify the SecurID primary server address:

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

3. Specify the SecurID encryption method for the LX unit:

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

4. Specify the SecurID authentication version for the LX unit:

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

5. Specify the socket the SecurID server is listening to:

```
AAA:0 >>securid authentication port 1812
```

6. Specify the maximum number of retries that the LX unit will have for sending an Access Request to the SecurID Authentication Server:

```
AAA:0 >>securid authentication retransmit 7
```

7. Specify the length of time that the LX unit will wait for the SecurID Authentication Server to respond before retransmitting packets:

```
AAA:0 >>securid authentication timeout 3
```

8. Exit the AAA Command Mode and access the Asynchronous Command Mode for the asynchronous ports that you want to configure for SecurID authentication:

   AAA:0 >>`exit`
   Config:0 >>`port asynchronous 3`

9. Access the Asynchronous Command Mode for the asynchronous ports that you want to configure for SecurID authentication:

   AAA:0 >>`port asynchronous 3`

10. Specify SecurID as the method of inbound authentication for the port:

    Async 3-3:0>>`authentication inbound securid enable`

11. Specify SecurID as the method of outbound authentication for the port:

    Async 3-3:0>>`authentication outbound securid enable`

12. Verify the LX SecurID configuration:

    Async 3-3:0>>`show securid characteristics`

```
Time:                                          Mon, 17 Mar 2003 18:09:34 UTC
SecurID Configuration Settings
 Authentication Version:     Version_5     Authentication Encryption:     DES
 Authentication Timeout:             3     Authentication Retransmit:       7
 Authentication Port:             1812
 V5 Primary Server:       149.19.87.89      Primary Name:
 Legacy Master Server:         0.0.0.0      Master Name:
 Legacy Slave Server:          0.0.0.0      Slave Name:
 Local Subscriber: Disabled
 Inbound SecurID Enabled Serial Ports: 3
 Outbound SecurID Enabled Serial Ports: 3
 SecurID Enabled Interfaces:
```

Figure 18 - SecurID Characteristics Screen

SecurID Security (Legacy Example)

This example shows how to configure the Legacy Version of SecurID for the LX unit. For background information on this task, refer to "Setting Up SecurID" in the *LX-Series Configuration Guide*.

NOTE: This example shows how to configure the Legacy Version of SecurID. If you want to configure Version 5 of SecurID, refer to "SecurID Security (Version 5 Example)" on page 54.

Prerequisites

The prerequisites for this task are the following:

- Set up the SecurID server(s) for the LX unit. For background information on this task, refer to "Installing and Configuring the SecurID Server on a Network-based Host" in the *LX-Series Configuration Guide*.

  NOTE: In addition to the SecurID authentication master server, slave servers can be configured for Legacy Versions of SecurID. For more information on configuring slave servers for SecurID, go to http://www.rsasecurity.com/products/securid/index.html.

- Ensure that the LX unit can ping the SecurID server(s). For more information, refer to the `ping` command in the *LX-Series Commands Reference Guide*.

- The SecurID application must be running on the SecurID Server.

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. Specify the SecurID master server address:

   AAA:0 >>`securid master authentication server address 192.16.65.38`

3. Specify the SecurID slave server address:

   AAA:0 >>`securid slave authentication server address 192.19.72.112`

4. Specify the SecurID encryption method for the LX unit:

   AAA:0 >>`securid authentication encryption des`

5. Specify the SecurID authentication version for the LX unit:

   AAA:0 >>`securid authentication version legacy`

6. Specify the socket the SecurID server is listening to:

   AAA:0 >>`securid authentication port 1812`

7. Specify the maximum number of retries that the LX unit will have for sending an Access Request to the SecurID Master Authentication Server:

   AAA:0 >>`securid authentication retransmit 7`

8. Specify the length of time that the LX unit will wait for the SecurID Master Authentication Server to respond before retransmitting packets:

   AAA:0 >>`securid authentication timeout 3`

9. Exit the AAA Command Mode and access the Asynchronous Command Mode for the asynchronous ports that you want to configure for SecurID authentication:

   AAA:0 >>`exit`
   Config:0 >>`port asynchronous 3`

10. Specify SecurID as the method of inbound authentication for the port:

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

11. Specify SecurID as the method of outbound authentication for the port:

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

12. Verify the LX SecurID configuration:

    InReach:0 >>`show securid characteristics`

```
Time:                                          Mon, 17 Mar 2003 18:09:34 UTC
SecurID Configuration Settings
 Authentication Version:        Legacy     Authentication Encryption:     DES
 Authentication Timeout:             3     Authentication Retransmit:       7
 Authentication Port:             1812
 V5 Primary Server:             0.0.0.0     Primary Name:
 Legacy Master Server:    192.16.65.38     Master Name:
 Legacy Slave Server:    192.19.72.112     Slave Name:
 Local Subscriber: Disabled
 Inbound SecurID Enabled Serial Ports: 5
 Outbound SecurID Enabled Serial Ports: 5
 SecurID Enabled Interfaces:
```

Figure 19 - SecurID Characteristics Screen

TACACS+ Security

This example shows how to configure TACACS+ security for the LX unit. For background information on this task, refer to "Setting Up TACACS+" in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisites for this task are the following:

- Set up the TACACS+ authentication server(s), and the TACACS+ accounting server(s), for the LX unit. For background information on this task, refer to "Installing and Configuring the TACACS+ Server on a Network-based Host" in the *LX-Series Configuration Guide*.
- Configure the TACACS+ Server Client database.

- Ensure that the LX unit can ping its TACACS+ authentication server(s) and TACACS+ accounting server(s). For more information, refer to the `ping` command in the *LX-Series Commands Reference Guide*.

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. Specify the TACACS+ primary authentication server address:

```
AAA:0 >>tacacs+ primary authentication server address
10.242.131.13
```

3. Specify the TACACS+ primary authentication server secret:

```
AAA:0 >>tacacs+ primary authentication server secret
jets
```

4. Specify the TACACS+ primary accounting server address:

```
AAA:0 >>tacacs+ primary accounting server address
10.242.131.13
```

5. Specify the UDP port that the TACACS+ Primary Authentication Server will use to listen to the LX unit:

```
AAA:0 >>tacacs+ primary authentication server port 1645
```

6. Specify the maximum number of retries that the LX unit will have for sending an Access Request to the TACACS+ Primary Authentication Server:

```
AAA:0 >>tacacs+ primary authentication server
retransmit 3
```

7. Specify the length of time that the LX unit will wait for the TACACS+ Primary Authentication Server to respond before retransmitting packets:

   AAA:0 >>`tacacs+ primary authentication server timeout 3`

8. Specify the interval at which the LX unit will update the TACACS+ accounting server with the status of each TACACS+ user:

   AAA:0 >>`tacacs+ period 10`

9. Specify the Superuser password that resides on the TACACS+ authentication server that will be used to enter the Superuser Command Mode:

   AAA:0 >>`tacacs+ superuser password request enable`

10. Exit the AAA Command Mode and access the Asynchronous Command Mode for the asynchronous ports that you want to configure for TACACS+ authentication:

    AAA:0 >>`exit`
    Config:0 >>`port asynchronous 6`

11. Specify TACACS+ as the method of inbound authentication for the port:

    Async 6-6:0>>`authentication inbound tacacs+ enable`

12. Specify TACACS+ as the method of outbound authentication for the port:

    Async 6-6:0>>`authentication outbound tacacs+ enable`

13. Enable TACACS+ accounting on the port:

    Async 6-6:0>>`tacacs+ accounting enable`

14. Verify that the TACACS+ primary server address and the TACACS+ primary server secret have been configured:

    Async 6-6:0>>`show tacacs+ characteristics`

    The highlighted fields on the following TACACS+ Characteristics Screen show that the TACACS+ primary server address and the TACACS+ primary server secret have been configured.

```
Time:                                  Wed, 10 Apr 2002 00:44:48 UTC
Primary TACACS+ Authentication Server:
IP Address: 10.242.131.13              TACACS+ Auth. TCP Port:  1812
Secret:     Configured                 Timeout:                    3
Retry:      3

Secondary TACACS+ Authentication Server:
IP Address:                            TACACS+ Auth. TCP Port:  1812
Secret:     Configured                 Timeout:                    3
Retry:      3

Primary TACACS+ Accounting Server:
IP Address: 10.242.131.13              TACACS+ Acct. TCP Port:  1813
Secret:     Configured                 Timeout:                    3
Retry:      3

Secondary TACACS+ Accounting Server:
IP Address: 10.242.131.11              TACACS+ Acct. TCP Port:  1813
Secret:     Configured                 Timeout:                    3
Retry:      3

Local Subscriber: Disabled
TACACS+ Superuser Request:  Enabled    TACACS+ Accounting Server Period: 5
Inbound TACACS+ Enabled Serial Ports:
Outbound TACACS+ Enabled Serial Ports:
TACACS+ Enabled Interfaces:
```

Figure 20 - TACACS+ Characteristics Screen

15. Verify that TACACS+ is enabled on the port that you specified in step 11 and step 12:

    InReach:0 >>`show port async 6 characteristics`

The highlighted fields on the following Port Characteristics Screen show that TACACS+ is enabled on the port that you specified in step 11 and step 12:

```
Time:                                        Sat, 10 Jan 2004 04:01:20 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:               Auto Dial:                   Disabled
Inbound Authentication:    Tacacs+  Autohangup:                   Enabled
Outbound Authentication:   Tacacs+  Radius Accounting:           Disabled
Authentication FallBack:   Disabled  Tacacs+ Accounting:          Enabled
Data Buffer Size:            1024  Data Buffer Display:           Prompt
Data Buffer Syslog:        Disabled  Data Buffer Time Stamp:       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
Connect Command:
```

Figure 21 - Port Characteristics Screen

Notes

The parameters that can be configured for the TACACS+ Authentication and Accounting Servers include **IP address**, **UDP port**, **Retransmit Value**, **Server Secret**, **Timeout**, **Superuser Request**, and **Local Subscriber**.

Refer to Chapter 4 of the *LX-Series Commands Reference Guide* for descriptions of the commands that are used to configure parameters for each type of TACACS+ Server.

Each TACACS+ Server command begins with a string specifies the type of TACACS+ Server that it applies to; for example `tacacs+ primary authentication server`, `tacacs+ primary accounting server`, `tacacs+ secondary authentication server`, and `tacacs+ secondary accounting server`.

Chapter 3

Configuring Asynchronous Ports

This chapter provides examples of how to configure Asynchronous ports on the LX unit. The examples in this chapter include the following:

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 from a device that sends data to a port on the LX unit. (**Note:** The port that receives the data will be the port that you configure for data buffering in step 4 of the following procedure.)

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 port that you want to configure for data buffering:

```
Config:0 >>port asynchronous 3
```

3. Disable Autohangup before setting the access to databuffer:

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

NOTE: Autohangup is required for ports with modems attached.

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/`.

8. Specify the data buffer display option:

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

   NOTE: In the above example, the data buffer display option of `enable` specifies that the contents of the data buffer will be displayed as soon as the user logs into the port.

9. Go to the Superuser Command Mode:

   Config:0 >>`end`

10. Verify that the port has been configured or 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:                                    Sat, 10 Jan 2004 04:01:20 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:                  Auto Dial:                   Disabled
Inbound Authentication:       Tacacs+  Autohangup:                   Enabled
Outbound Authentication:      Tacacs+  Radius Accounting:           Disabled
Authentication FallBack:     Disabled  Tacacs+ Accounting:           Enabled
Data Buffer Size:                1024  Data Buffer Display:          Enabled
Data Buffer Syslog:          Disabled  Data Buffer Time Stamp:       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
Connect Command:
```

Figure 22 - Port Characteristics Screen

11. Access the Linux shell:

    Config:0 >>`shell`

12. In the Linux shell, execute the following commands to view the databuffer message:

```
InReach:/# cd /var/log
InReach:/var/log# tail databuffer
```

NOTE: The databuffer contents are lost during a reboot of the LX.

Configuring Asynchronous Ports for Pattern Matching

This example shows how to configure an asynchronous port on the LX unit for Pattern Matching. When data that matches a pattern string is received at a port that has Pattern Matching, the data is put into a notification message. In this example, the notification message is sent to all notification clients that have a facility of `user` and a priority of `notice`.

For background information on this task, refer to the `pattern match enable` command, and the `pattern string` command, in the *LX-Series Commands Reference Guide*.

Prerequisites

The prerequisites for this task are the following:

- The port that will be used for pattern matching must be configured for databuffer access. Refer to "Configuring Asynchronous Ports for Data Buffering" on page 67 for an example of how to configure a port for databuffer access.
- Configure notification clients that have a facility of `user` and a priority of `notice` in their User Profiles. For more information, refer to Chapter 4, "Setting Up the Notification Feature" in the *LX-Series Configuration Guide*.

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 port(s) that you want to configure for pattern matching:

   Config:0 >>`port asynchronous 3`

   NOTE: The port must be configured for databuffer access as described in the Prerequisites for this procedure (see above).

3. Create a match pattern for the port(s):

   Async 3-3:0>>`pattern string 5 1234B`

4. Enable the Pattern Matching Feature on the port(s):

   Async 3-3:0>>`pattern match enable`

5. Display the match patterns, and the status of the Pattern Match Feature, for the specified port(s):

   Async 3-3:0>>`show port asynchronous 3 pattern match characteristics`

   The highlighted fields on the following screen indicate that match pattern 5 is `1234B`, and Pattern Matching is enabled, on port 3:

```
Time:                                          Mon, 23 Jun 2003 07:05:52
Banner:                                           /config/banner.default
Port Number:                    3
Pattern Match:              Enabled

Pattern 1: SuperUser
Pattern 2: tes.t
Pattern 3: Unix Reboot
Pattern 5: 1234B
```

Figure 23 - Pattern Match Characteristics Screen

Configuring Ports for Remote Console Management

This example shows how to configure an asynchronous port on the LX unit for remote console management. When a port is configured for remote console management, you can connect a network element to it. You can configure subscribers to access the port and manage the network element that is connected to it. (Refer to "Configuring Subscribers for Remote Console Management" on page 116 for more information.)

For background information on this task, refer to "Configuring Ports for Remote Console Management" in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisites for this task are the following:

- Connect the asynchronous port to the network element that is to be managed (see "Connecting the Console Port to the Network Element" in the *LX-Series Configuration Guide*).
- If you are using a server-based authentication method (i.e., RADIUS, TACACS+, or SecurID), set up the authentication server that you will be using to authenticate connections to the port. For more information, refer to the following sections in the *LX-Series Configuration Guide*:
  - "Installing and Configuring the RADIUS Server on a Network-based Host"
  - "Installing and Configuring the TACACS+ Server on a Network-based Host"
  - "Installing and Configuring the SecurID Server on a Network-based Host"

Procedure (Non-modem Port Example)

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 port(s) that you want to configure for remote console management:

   Config:0 >>`port asynchronous 6`

3. Set the access for the asynchronous port(s) to Remote:

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

4. Enable the Autohangup feature on the asynchronous port(s):

   Async 6-6:0 >>`autohangup enable`

5. Specify the following asynchronous port settings to match the corresponding settings on the attached network element:

   - Data Bits:
     Command Example: **Async 6-6:0 >>**`bits 6`
   - Flow Control:
     Command Example: **Async 6-6:0 >>**`flowcontrol xon`
   - Parity:
     Command Example: **Async 6-6:0 >>**`parity even`
   - Speed:
     Command Example: **Async 6-6:0 >>**`speed 19200`
   - Stop Bits:
     Command Example: **Async 6-6:0 >>**`stop bits 2`

6. Enable an authentication method on the asynchronous port(s):

   Async 6-6:0 >>`authentication outbound radius enable`

Procedure (Modem Port Example)

1. Access the Asynchronous Command Mode for the asynchronous port that you want to set up for remote console management.

   ```
   Login: InReach
   Password: access
   InReach:0>enable
   Password>> system
   InReach:0 >>config
   Config:0 >>async port 5
   ```

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. Enable autohangup to ensure the port resets when the modem drops DSR:

   Async 5-5:0 >>`autohangup enable`

7. Execute the `modem` command to access the Modem Command Mode for the port under configuration; for example:

   Async 5-5:0 >>`modem`

8. In the Modem Command Mode, execute the `type` command to set the Modem Type to DIALOUT; for example:

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

9. 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`

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

    Modem 5-5:0 >>`initstring AT S7=45 S0=1 L1 V1 X4 &C1 &1 Q0 &S1 &B1`

    NOTE: The initialization string may vary between modem types.

11. 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`

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

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

Setting Up Authentication for Remote Console Ports

This example shows how to configure LOCAL Authentication, RADIUS Authentication, SecurID Authentication, and TACACS+ Authentication for remote console ports.

Prerequisites

If you are using a server-based security method (i.e., RADIUS, TACACS+, or SecurID), set up the authentication server that you will be using to authenticate connections to the port. For more information, refer to the following sections in the *LX-Series Configuration Guide*:

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

Procedure (Non-modem Port Example)

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 a Remote Console port:

```
Config:0 >>port asynchronous 6
```

3. Specify LOCAL as the authentication method for the port:

```
Async 6-6:0 >>authentication outbound local enable
```

4. Return to the Configuration Command Mode:

```
Async 6-6:0 >>exit
```

5. Access the Asynchronous Command Mode for another Remote Console port:

   Config:0 >>`port asynchronous 7`

6. Specify RADIUS as the authentication method for the port:

   Async 6-6:0 >>`authentication outbound local radius`

7. Return to the Configuration Command Mode:

   Async 6-6:0 >>`exit`

8. Access the Asynchronous Command Mode for another Remote Console port:

   Config:0 >>`port asynchronous 8`

9. Specify SecurID as the authentication method for the port:

   Async 6-6:0 >>`authentication outbound local securid`

10. Return to the Configuration Command Mode:

    Async 6-6:0 >>`exit`

11. Access the Asynchronous Command Mode for another Remote Console port:

    Config:0 >>`port asynchronous 9`

12. Specify TACACS+ as the authentication method for the port:

    Async 9-9:0 >>`authentication outbound tacacs+`

Configuring Asynchronous Ports for Power Management

You can use the asynchronous ports on an LX unit as Power Masters for IR-5100 and IR-5150 series units. This enables network and systems administrators to remotely power cycle locked up equipment and/or bring redundant systems online.

To keep power management simple the outlets can be assigned to a group and turned on/off or rebooted by the group number. The power outlets can also be turned on/off or rebooted individually. You can set a minimum amount of time for the outlet to remain off. Currently, the outlet stays off for the time the port APD timeout setting is set to. The software provides the ability to name each power outlet as well as a group.

This example shows how to manage the IR-5150 from the LX CLI. For background information on this task, refer to "Configuring Power Control Units" in the *LX-Series Configuration Guide*, and to *Getting Started with the MRV Communications 5150 Power Control Series*.

Prerequisites

The prerequisites for this task are the following:

- A serial crossover cable must be connected between an LX port and the RS-232 port on the IR-5100/5150.
- The IR-5100/5150 must be turned on.

Procedure

To manage the IR-5150 from the LX CLI:

1. Login to the LX as a superuser:

```
Welcome to MRV Communications, In-Reach Product Division.
Login: InReach
Password: ******
InReach:0 >enable
Password: ******
```

2. Configure port 6 for a power device:

```
InReach:0 >>configuration
Config:0 >>port async 6
Async 6-6:0 >>access power model ir5150
```

3. Give names to all the outlets managed by port 6:

Example:

Async 6-6:0 >>outlet 1 name Sun1

Async 6-6:0 >>outlet 2 name Aircond2

Async 6-6:0 >>exit

The above commands assign a name to a power outlet. A name can be up to 15 characters long.

4. In this example, we create two groups: **Group 1** includes all of the odd-number outlets, while **Group 2** includes all of the even-numbered outlets. Assign Group 2 a group name of **Labservers**:

   Example:

   Config:0 >>outlet group 1 6:1 6:3 6:5 6:7

   Config:0 >>outlet group name LabServers 6:2 6:4 6:6 6:8

   This command allows you to group outlets by group number so an administrator can manage several outlets at once. The group number cannot be higher than 16. The list is separated by spaces. Commas are not allowed.

5. Set the outlet off time period:

   Config:0 >>outlet group LabServers off time 3

   This command defines the amount of time the outlet should remain off before turning back on. The default value is 15 and the valid range is 0 to 255 seconds. The group name must match exactly the group name used in the previous step.

   The above setup creates group 1, which group odd number outlets from two different async ports. A second group is created by name with even number outlets.

   Config:0 >>exit

6. Display the outlet groups:

```
InReach:0 >>show outlet group 1 status
```

```
Time:   Sun, 18 March 18 18:06:51 UTC  Group Number:              1
Group Name:                            Group Off Time:            3
Port  Outlet    State
  6     1       On
  6     3       On
  6     5       On
  6     7       On
```

Figure 24 - Outlet Group Status Screen

NOTE: If the group has no name, the LX gives it a group number.

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

```
Time:   Sun, 18 March 18:07:17 UTC  Group Number:                      2
 Group Name:                LabServers  Group Off Time:                3
 Port  Outlet    State
   6      2       On
   6      4       On
   6      6       On
   6      8       On
```

Figure 25 - Outlet Group Status Screen

NOTE: The system assigns group numbers based on the order in which they are created.

7. Display the status of port 6:

```
InReach:0 >>show device 6 status
InReach:0>> show port async 6 status
```

8. To display which ports are configured for device, enter:

   InReach:0 >>`show device sum`

```
Device Number    Device Type       Model Name
        6          IR5150          IR-5150-2108V
```

Figure 26 - Device Summary Screen

9. Turn the outlets off by groups:

   InReach:0 >>`outlet group 1 off`

   InReach:0>>`outlet group LabServers off`

10. Turn the outlets on by groups:

    InReach:0 >>`outlet group 1 on`

    InReach:0>>`outlet group LabServers on`

11. Reboot the outlets by groups:

    InReach:0 >>`outlet group 1 reboot`

    InReach:0>>`outlet group LabServers reboot`

12. Turn the individual outlets off one at a time:

    InReach:0>>`outlet 6:1 off`

    You are now configured to manage the IR-5150 via the LX CLI.

    NOTE: All configured outlet names and power management groups are stored on the LX, not on the IR-5100 and IR-5150 devices.

Configuring Asynchronous Ports for Sensor Management

This example shows how to configure LX sensor management. For background information on this task, refer to "Configuring Ports for Temperature/Humidity Sensors" in the *LX-Series Configuration Guide*.

Prerequisites

The prerequisite for this task is the following:

- Connect a Temperature/Humidity Sensor to the port that you will configure as a SENSOR port in step 3 in the following procedure.

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 port that you want to configure as a SENSOR port:

```
Config:0 >>port asynchronous 5
```

3. Specify SENSOR as the Access method for the port:

```
Async 5-5:0 >>access sensor
```

4. Display the current Temperature and Humidity readings on the SENSOR port:

```
Async 5-5:0 >>show device 5 status
```

```
Time:   Tue, 01 Jul 2003 21:14:29 UTC
Port Name:                  Port_5   Device Number:                    5
Device Type:                                                      Sensor
Humidity Level(%):                                                 65.00
Temperature (Celsius):                                             25.00
Temperature (Fahrenheit):                                          77.00
```

Figure 27 - Device Screen for A SENSOR Port

Chapter 4

Configuring the Notification Feature

This chapter provides examples of how to configure the Notification feature for the LX unit. The examples are organized according to Service Profile types. The following sections contain configuration examples for each Service Profile type:

- "ASYNC Example" (see page 84)
- "LOCALSYSLOG Example" (see page 86)
- "REMOTESYSLOG Example" (see page 88)
- "SMTP Example" (see page 90)
- "SNMP Example" (see page 92)
- "SNPP Example" (see page 93)
- "TAP Example" (see page 95)
- "WEB Example" (see page 99)

This chapter also contains an example of how to change the text field, facility, and priority of a configurable syslogd message (see "syslogd Message Configuration Example" on page 84).

For background information on the Notification feature, refer to "Setting Up the Notification Feature" in the *LX-Series Configuration Guide*.

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
```

ASYNC Example

This example shows how to configure the Notification feature to send event messages to asynchronous ports. In order to configure the Notification feature for this purpose, you must create a Service Profile of the ASYNC type. You can then create User Profiles that are linked to a Service Profile of the ASYNC type.

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. Create a Service Profile called `OnBoardPort` and access the Service Profile Command Mode:

   Notification:0>>`profile service OnBoardPort`

3. Specify ASYNC as the type of the Service Profile, and access the ASYNC Protocol Command Mode:

   Noti_Serv_Protocol:0 >>`async`

4. Specify the outbound asynchronous ports to which the event messages will be sent:

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

5. Return to the Notification Command Mode:

   Noti_Serv_Async:0 >>`exit`

6. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user AsyncUser1`

7. Specify the Service Profile `OnBoardPort` as the Service Profile for the current User Profile:

   Noti_User_Service:0 >>`service OnBoardPort`

   When you execute the `service` command, the CLI enters the User Information command mode.

8. Use the `priority` command to specify a priority characteristic for the User Profile `AsyncUser1`:

   Noti_User_Info:0 >>`priority warning`

9. Use the `facility` command to specify a facility characteristic for the User Profile `AsyncUser1`:

   Noti_User_Info:0 >>`facility user`

LOCALSYSLOG Example

This example shows how to configure the Notification feature to send event messages to a file in the `/var/log` directory on the LX unit. In order to configure the Notification feature for this purpose, you must create a Service Profile of the LOCALSYSLOG type. You can create User Profiles that are linked to a Service Profile of the LOCALSYSLOG type.

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. Create a Service Profile called `OnBoardLog1` and access the Service Profile Command Mode:

   Notification:0>>`profile service OnBoardLog1`

3. Specify LOCALSYSLOG as the type of the Service Profile, and access the LOCALSYSLOG Protocol Command Mode:

   Noti_Serv_Protocol:0 >>`localsyslog`

4. Specify the local file to which event messages will be sent:

   Noti_Serv_LSyslog:0 >>`file box3`

5. Return to the Notification Command Mode:

   Noti_Serv_LSyslog:0 >>`exit`

6. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user Locallog`

7. Specify the Service Profile `OnBoardLog1` as the Service Profile for the current User Profile:

   Noti_User_Service:0 >>`service OnBoardLog1`

   When you execute the `service` command, the CLI enters the User Information command mode.

8. Use the `facility` command to specify a facility characteristic for the User Profile `AsyncUser1`:

   Noti_User_Info:0 >>`facility all`

9. Use the `priority` command to specify a priority characteristic for the User Profile `Locallog`:

   Noti_User_Info:0 >>`priority warning`

REMOTESYSLOG Example

This example shows how to configure the Notification feature to send event messages to a remote host. In order to configure the Notification feature for this purpose, you must create a Service Profile of the REMOTESYSLOG type. You then create User Profiles that are linked to a Service Profile of the REMOTESYSLOG type.

Prerequisites

Do the following on the remote Unix host to which event messages will be sent:

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

   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 take effect.

   # ps –ef|grep syslog
   # kill –HUP 683

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. Create a Service Profile called `OffShore1` and access the Service Profile Command Mode:

   Notification:0>>`profile service OffShore1`

3. Specify REMOTESYSLOG as the type of the Service Profile, and access the REMOTESYSLOG Protocol Command Mode:

   Noti_Serv_Protocol:0 >>`remotesyslog`

4. Specify the remote UNIX host to which event messages will be sent:

   Noti_Serv_RSyslog:0 >>`host 10.179.170.253`

5. Return to the Notification Command Mode:

   Noti_Serv_RSyslog:0 >>`exit`

6. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user OffShoreUser1`

7. Specify the Service Profile `OffShore1` as the Service Profile for the current User Profile:

   Noti_User_Service:0 >>`service OffShore1`

   When you execute the `service` command, the CLI enters the User Information command mode.

8. Use the `priority` command to specify a priority characteristic for the User Profile `OffShore1`:

   Noti_User_Info:0 >>`priority warning`

9. Use the `facility` command to specify a facility characteristic for the User Profile `OffShore1`:

   Noti_User_Info:0 >>`facility user`

SMTP Example

This example shows how to configure the Notification feature to send event messages to a text phone and email address. In order to configure the Notification feature for this purpose, you must create a Service Profile of the SMTP type. You must also create User Profiles to specify the text phones, or email addresses, to which the event messages will be sent.

Prerequisites

The prerequisites for this task are the following:

- Configure DNS on the LX unit. (This is necessary to resolve the Email provider's address.) For more information, refer to the `primary dns` command in the *LX-Series Commands Reference Guide*.
- Specify a fully qualified domain name suffix for the LX unit. For more information, refer to the `domain name` command in the *LX-Series Commands Reference Guide*.

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. Create a Service Profile called `MailServerLun` and access the Service Profile Command Mode:

```
Notification:0>>profile service MailServerLun
```

3. Specify SMTP as the type of the Service Profile, and access the SMTP Protocol Command Mode:

   Noti_Serv_Protocol:0 >>`smtp`

4. Specify the IP Address of an email server:

   Noti_Serv_SMTP:0 >>`server 10.179.176.21`

5. Give the email a specific sender name known by your email server:

   Noti_Serv_SMTP:0 >>`bobLX`

6. Specify a unique email subject:

   Noti_Serv_SMTP:0 >>`subject LX rack 3 unit 4 reporting`

7. Return to the Notification Command Mode:

   Noti_Serv_SMTP:0 >>`exit`

8. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user JAllen`

9. Specify the Service Profile `MailServerLun` as the Service Profile for the User Profile `JAllen`:

   Noti_User_Service:0 >>`service MailServerLun`

   When you execute the `service` command, the CLI enters the User Information command mode.

10. Specify the email address to which messages will be sent:

    Noti_User_Info:0 >>`contact jallen@yourco.com`

11. Use the `priority` command to specify a priority characteristic for the User Profile `JAllen`:

    Noti_User_Info:0 >>`priority warning`

12. Use the `facility` command to specify a facility characteristic for the User Profile `JAllen`:

    Noti_User_Info:0 >>`facility user`

SNMP Example

This example shows how to configure the Notification feature to send event messages to certain SNMP trap clients of the LX unit. In order to configure the Notification feature for this purpose, you must create a Service Profile of the SNMP type. You then create a User Profile that is based on a Service Profile of the SNMP type.

Prerequisites

The prerequisites for this task are the following:

- Create one or more Version 1, 2, or 3 SNMP trap clients with a community setting of `public`; for example:

  SNMP:0>> `trap client 1 version 2`

  SNMP:0>> `trap client 1 192.168.32.4`

  SNMP:0>> `trap client 1 community public`

- After you have created one or more SNMP trap clients with a community setting of `public`, you must enable the SNMP Feature by executing the `snmp enable` command in the Configuration Command Mode; for example:

  Config:0 >>`snmp enable`

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. Create a Service Profile called `AdminClients` and access the Service Profile Command Mode:

   Notification:0>>`profile service AdminClients`

3. Specify SNMP as the type of the Service Profile, and return to the Notification Command Mode:

   Noti_Serv_Protocol:0 >>`snmp`

   Executing the `snmp` command returns you to the Notification Command Mode.

4. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user NetworkMgr1`

5. Specify the Service Profile `AdminClients` as the Service Profile for the User Profile `NetworkMgr1`:

   Noti_User_Service:0 >>`service AdminClients`

   When you execute the `service` command, the CLI enters the User Information command mode.

6. Use the `priority` command to specify a priority characteristic for the User Profile `NetworkMgr1`:

   Noti_User_Info:0 >>`priority warning`

7. Use the `facility` command to specify a facility characteristic for the User Profile `NetworkMgr1`:

   Noti_User_Info:0 >>`facility user`

SNPP Example

This example shows how to configure the Notification feature to send event messages to a pager. In order to configure the Notification feature for this purpose, you must create a Service Profile of the SNPP type. You must also create User Profiles to specify the pagers to which the event messages will be sent.

Prerequisites

The prerequisite for this task is the following:

- Configure DNS on the LX unit. (This is necessary to resolve the paging provider's address.) For more information, refer to the `primary dns` command in the *LX-Series Commands Reference Guide*.

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. Create a Service Profile called `FieldPagers` and access the Service Profile Command Mode:

```
Notification:0>>profile service FieldPagers
```

3. Specify SNPP as the type of the Service Profile, and access the SNPP Protocol Command Mode:

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

4. Specify the IP Address of an SNPP server:

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

```
Noti_Serv_SNPP:0 >>snpp skytel.com
```

5. Specify the LX TCP port that will be used to send messages to the SNPP server:

```
Noti_Serv_SNPP:0 >>port 7777
```

6. Return to the Notification Command Mode:

   Noti_Serv_SNPP:0 >>`exit`

7. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user RSmythe`

8. Specify the Service Profile `FieldPagers` as the Service Profile for the User Profile `RSmythe`:

   Noti_User_Service:0 >>`service FieldPagers`

   When you execute the `service` command, the CLI enters the User Information command mode.

9. Specify the Pager Pin Number for the User Profile `RSmythe`:

   Noti_User_Info:0 >>`contact 8875551212`

10. Use the `priority` command to specify a priority characteristic for the User Profile `RSmythe`:

    Noti_User_Info:0 >>`priority warning`

11. Use the `facility` command to specify a facility characteristic for the User Profile `RSmythe`:

    Noti_User_Info:0 >>`facility user`

TAP Example

This example shows how to configure the Notification feature to send event messages as text to a telephone. In order to configure the Notification feature for this purpose, you must create a Service Profile of the TAP type. You must also create User Profiles to specify the telephones to which the event messages will be sent.

Prerequisites

The prerequisites for this task are the following:

- A modem must be connected to each LX asynchronous port that is used to send messages to the Short Message Service Center (SMSC). (The port that is used to send messages to the SMSC is specified in step 8 of the following procedure.)
- The modem must be connected to a working telephone for dialout services.

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. Create a Service Profile called `TextPagers` and access the Service Profile Command Mode:

```
Notification:0>>profile service TextPagers
```

3. Specify TAP as the type of the Service Profile, and access the TAP Protocol Command Mode:

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

4. Specify the provider SMSC that will be used to send the event messages to the pager:

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

5. Specify the bit parity setting for the Service Profile:

   Noti_Serv_TAP:0 >>`parity even`

6. Specify the bits-per-byte setting for the Service Profile:

   Noti_Serv_TAP:0 >>`bits 7`

7. Specify the stop bits setting for the Service Profile:

   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.

8. Specify the modem port(s) that syslog can dial out to send a message with this Service Profile:

   Noti_Serv_TAP:0 >>`modem port 2`

9. Go to the Configuration Command Mode by executing the `exit` command twice:

   Noti_Serv_TAP:0 >>`exit`
   Notification:0>>exit

10. Access the Asynchronous Command Mode for the modem port that you specified in step 8:

    Config:0 >>`port asynchronous 2`

11. Access the Modem Command Mode:

    Async 2-2:0 >>`modem`

12. Enable the Modem Feature on the modem port that you specified in step 8:

    Modem 2-2:0 >>`modem enable`

13. Disable Autohangup on the modem port that you specified in step 8:

    Modem 2-2:0 >>`no autohangup`

14. Specify remote access on the modem port that you specified in step 8:

    Modem 2-2:0 >>`access remote`

15. Return to the Configuration Command Mode:

    Modem 2-2:0 >>`exit`
    Async 2-2:0 >>exit

16. Access the Notification Command Mode:

    Config:0 >>`notification`

17. Create a User Profile and access the User Service Command Mode:

    Notification:0>>`profile user WJones`

18. Specify the Service Profile `TextPagers` as the Service Profile for the User Profile `WJones`:

    Noti_User_Service:0 >>`service TextPagers`

    When you execute the `service` command, the CLI enters the User Information command mode.

19. Specify the Pager Number to which messages will be sent:

    Noti_User_Info:0 >>`contact 8552222`

20. Use the `priority` command to specify a priority characteristic for the User Profile `WJones`:

    Noti_User_Info:0 >>`priority warning`

21. Use the `facility` command to specify a facility characteristic for the User Profile `WJones`:

    Noti_User_Info:0 >>`facility user`

WEB Example

This example shows how to configure the Notification feature to send event messages to pagers or wireless telephones. In order to configure the Notification feature for this purpose, you must create a Service Profile of the WEB type. You must also create User Profiles to specify the pagers or wireless telephones to which the event messages will be sent.

Prerequisites

The prerequisite for this task is the following:

- The correct timezone must be configured for the LX unit. To set the timezone for the LX unit, refer to the `timezone` command in the *LX-Series Commands Reference Guide*.
- The date and time for the LX unit must be current. (**Note:** Some wireless providers will reject event messages that originate on an LX unit that does not have the current date and time.)

  To set the date and time for the LX unit, refer to the `date` and `clock` commands in the *LX-Series Commands Reference Guide*.

  NOTE: You can also configure the LX unit to get the time and date from a Network Time Server. To configure the LX unit to get the time and date from a Network Time Server, refer to the `ntp enable` command in the *LX-Series Commands Reference Guide*. To specify a Network Time Server for the LX unit, refer to the `ntp server address` command in the *LX-Series Commands Reference Guide*.

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. Create a Service Profile called `NetClients` and access the Service Profile Command Mode:

   Notification:0>>`profile service NetClients`

3. Specify WEB as the type of the Service Profile, and access the WEB Protocol Command Mode:

   Noti_Serv_Protocol:0 >>`web`

4. Specify the Web Driver that will be used to send event messages to the pager or cell phone:

   Noti_Serv_WEB:0 >>`driver ATT_WEB`

5. Return to the Notification Command Mode:

   Noti_Serv_WEB:0 >>`exit`

6. Create a User Profile and access the User Service Command Mode:

   Notification:0>>`profile user RJenks`

7. Specify the Service Profile `NetClients` as the Service Profile for the User Profile `RJenks`:

   Noti_User_Service:0 >>`service NetClients`

   When you execute the `service` command, the CLI enters the User Information command mode.

8. Specify the telephone number to which messages will be sent:

   Noti_User_Info:0 >>`contact 19785551212`

9. Use the `priority` command to specify a priority characteristic for the User Profile `RJenks`:

   Noti_User_Info:0 >>`priority warning`

10. Use the `facility` command to specify a facility characteristic for the User Profile `RJenks`:

    Noti_User_Info:0 >>`facility user`

Chapter 5

Configuring the Menu Feature

This chapter provides an example of how to create a multi-level subscriber login menu and how to associate that menu with a subscriber.

Menu Creation Example

This example shows how to create a multi-level subscriber menu, and the entries, for the multi-level menu. After you have created a menu, you can associate it with a subscriber (see "Associating a Subscriber With a Menu" on page 109).

NOTE: Software release V3.3.0 and higher include a two-page menu file named `demo_menu`. You can use `demo_menu` to test menus for a subscriber, as well as a reference menu for form and structure.

Prerequisites

The prerequisites for this task are the following:

- Configure the Primary Domain Name Server for the LX unit. For more information, refer to the `primary dns` command in the *LX-Series Commands Reference Guide*.
- Specify a fully qualified domain name suffix for the LX unit. For more information, refer to the `domain name` command in the *LX-Series Commands Reference Guide*.
- Specify a gateway for the LX unit. For more information, refer to the `gateway name` command in the *LX-Series Commands Reference Guide*.

Procedure

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

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

2. Create, or access, a menu file:

```
Menu :0 >>open marks
```

NOTE: Executing the `open` command puts the CLI into the Menu Editing Command Mode. The Menu Editing Command prompt (e.g., **marks-1:0 >>**) is displayed.

3. Create a header for the menu `marks`:

```
marks-1:0 >>header This is a sample menu for the user Mark
```

4. Create entry 1 of the menu, along with its entry label:

```
marks-1:0 >>entry 1 command telnet 10.82.240.10
marks-1:0 >>entry 1 label Telnet to host Venus
```

5. Create entry 2 of the menu, along with its entry label:

```
marks-1:0 >>entry 2 command ping –c4 10.10.10.12
marks-1:0 >>entry 2 label Ping the Local device on the LAN
```

6. Create entry 3 of the menu, along with its entry label:

```
marks-1:0 >>entry 3 command telnet 10.10.10.10 2500
marks-1:0 >>entry 3 label Telnet to remote access port 5
```

7. Create entry 4 of the menu, along with its entry label:

```
marks-1:0 >>entry 4 command ssh 10.10.10.10 –p 2522
marks-1:0 >>entry 4 label SSH to a remote serial port 5
```

8. Create entry 5 of the menu, along with its entry label:

```
marks-1:0 >>entry 5 command %menu 2
marks-1:0 >>entry 5 label Jump ahead to menu level 2
```

9. Create entry 6 of the menu, along with its entry label:

```
marks-1:0 >>entry 6 command telnet #
marks-1:0 >>entry 6 label Telnet to a user supplied IP
address
```

NOTE: When the pound symbol (#) is used in a command entry, it means that the user must complete the command by entering input at the command line.

10. Display the current menu level as it would appear to the subscriber:

```
marks-1:0 >>display
```

```
                  Menu 1 This is a sample menu for user Mark
1 Telnet to host Venus
2 Ping the Local device on the LAN
3 Telnet to a remote access port 5
4 SSH to a remote serial port 5
5 Jump ahead to Menu Lever 2
6 Telnet to a user supplied IP address
Up One Level: U Top of Menu: T Refresh: R Logout: Q Enter Number of
Selection or Use Arrow Keys:
Press <RETURN> to continue...
```

Figure 28 - Menu Level 1

11. Open Level 2 of the current menu file:

```
marks-1:0 >>menu 2
```

12. Create a header for Level 2 of the current menu file:

    marks-2:0 >>`header This is the Second Level Menu`

    NOTE: The menu level is indicated by the numeral that appears between the hyphen (**-**) and the colon (**:**) in the Menu Editing Command prompt. For example, the prompt **marks-2:0 >>** indicates that the Menu Level is 2.

13. Create entry 1 of Menu Level 2, along with its entry label:

    marks-2:0 >>`entry 1 %menu 1`
    marks-2:0 >>`entry 1 label Go back to menu level 1`

14. Save the menu file:

    marks-2:0 >>`save`

15. Display the current menu level as it would appear to the subscriber:

    marks-2:0 >>`display`

```
                  Menu 1 This is the Second Level Menu.
1 Go back to menu level 1









Up One Level: U Top of Menu: T Refresh: R Logout: Q Enter Number of
Selection or Use Arrow Keys:
Press <RETURN> to continue...
```

Figure 29 - Menu Level 2

16. Verify the headers and submenu levels in the menu file:

    marks-2:0 >>`list`

```
List Menu:
Menu 1 This is a sample menu for user Mark
* Menu 2 This is the Second Level Menu.
```

Figure 30 - Headers and Submenu Levels

17. Save the file:

    marks-2:0 >>`save`

18. Exit to the Menu Command Mode:

    marks-2:0 >>`exit`

19. List the available menu files:

    Menu :0 >>`list`

Chapter 6

Configuring Subscriber Features

This chapter provides examples of how to configure subscriber features on the LX unit. The examples in this chapter include the following:

Associating a Subscriber With a Menu

This example shows how to associate a subscriber with a menu.

Prerequisites

The prerequisite for this task is the following:

- Create a subscriber menu as shown in "Menu Creation Example" on page 103.

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. Create a subscriber account, or access an existing subscriber account:

   Config:0 >>`subscriber mark`

3. Associate an existing menu (e.g., `marks`) with the subscriber account, and enable the Menu Feature on the subscriber account:

   Subs_Mark >>`menu marks enable`

4. Verify the subscriber configuration:

   Subs_Mark >>`show subscriber Mark characteristics`

```
Subscriber Name:                  Mark   Rlogin Ded. Service:
 Preferred Service:                      Dedicated Service:
 Security:                                          User Read Outlet Shell
 Login Mode  :                      CLI  User Password:                Enabled
 Maximum Connections:                50  Maximum Sessions:                   4
 Command Logging:              Disabled  Audit Logging  :              Disabled
 Idle Timeout:                        0  User Prompt:                   InReach
 Menu Name:                                                        /config/Menu2
 Web Menu Name:                                                    /config/Menu2
 Web Login Mode:                Config  Screen Pause:                  Enabled
 Forward Switch:                    ^F  Local Switch:                      ^L
 Backward Switch:                   ^B  Rlogin Transparent:           Disabled
 Dialback Feature:             Disabled
 Dialback Number:
 Port Access   list:                                                     0-33
 Remote Access list:                          Telnet Ssh Web_Server Console
 Outlet Access list:
 Outlet Group Access list:
```

Figure 31 - Subscriber Characteristics Screen

5. When you have verified the subscriber configuration, exit to the Superuser Command Mode and save the system configuration:

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

Notes

Keep the following in mind when you specify a menu for a subscriber:

- The subscriber must have a security level of `superuser` to select a command entry that executes any Superuser command other than a `monitor/show` command (for which a security level of `read` is adequate) or an outlet command (for which a security level of `outlet` is adequate).
- The subscriber must have a security level of `read` or `superuser` to select a command entry that executes a `monitor` or `show` command.
- The subscriber must have a security level of `outlet` or `superuser` to select a command entry that executes an `outlet` command.

For example, a subscriber would need a security level of `outlet` or `superuser` to select item 1 in the menu shown in Figure 32, "A Sample Menu," on page 111; a subscriber would need a security level of `read` or `superuser` to select item 2 in the same menu; he or she would need a security level of `superuser` to select item 3 in the same menu.

```
                  Menu 1 This is a sample menu for user Sam
1 Turn on Outlet 3:5
2 Show Subscriber Summaries
3 Reboot the LX with the reload command
4 SSH to a remote serial port
5 Jump ahead to Menu Lever 2
6 Telnet to a user supplied IP address
Up One Level: U Top of Menu: T Refresh: R Logout: Q Enter Number of
Selection or Use Arrow Keys:
Press <RETURN> to continue...
```

Figure 32 - A Sample Menu

For more information on Security Levels, refer to the `security level` command in the *LX-Series Commands Reference Guide*.

Configuring the Dialback Feature for a Subscriber

The Dialback Feature allows the LX to receive a call, hang up, and then call back the person who just called it. It is configured on the subscriber level, allowing the administrator to specify exactly who gets a call back from the LX unit. This feature is useful for centralized telephone billing. It can also be used as a security feature because the subscriber needs to be at the telephone that is called back.

This section provides an example of how to configure the Dialback Feature for a subscriber.

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 a subscriber account:

```
Config:0 >>subscriber Mark
```

3. Specify the dialback number for the subscriber account:

```
Subs_Mark >>dialback number 12345678901
```

4. Enable the Dialback Feature for the subscriber account:

   Subs_Mark >>`dialback enable`

5. Verify the Dialback configuration for the subscriber account:

   Subs_Mark >>`show subscriber mark characteristics`

```
Subscriber Name:                 Mark
Preferred Service:                     Dedicated Service:
Security:                                                    SuperUser
Login Mode  :                      CLI  User Password:             Enabled
Maximum Connections:                 5  Maximum Sessions:                4
Command Logging:               Disabled  Audit Logging  :          Disabled
Idle Timeout:                        0  User Prompt:                InReach
Menu Name:               /config/Menu2  Screen Pause:               Enabled
Forward Switch:                     ^F  Local Switch:                    ^L
Backward Switch:                    ^B  Dialback Feature:           Enabled
Dialback Timeout:                   45  Dialback Number:        12345678901
Port Access   list:                                                    0-8
Remote Access list:                             Telnet Ssh Web_Server Console
Outlet Access list:
Outlet Group Access list:
```

Figure 33 - Subscriber Characteristics Screen

Assigning a Trusted Key to a Subscriber

With a Trusted 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 Trusted Key to a Subscriber.

Prerequisites

There are no prerequisites for this configuration example.

Procedure

1. Connect to the SSH client that will be used to initiate the SSH connections to the LX unit:

   ```
   telnet 10.242.131.11
   ```

   NOTE: In this example, the SSH client is an LX unit.

2. Log in to the LX unit with the user name and password of the user account for which you want to create the Trusted Key:

   ```
   login: gina
   password: *********
   ```

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.

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:

   ```
   telnet 116.24.154.23
   ```

8. Log in to the LX unit:

   ```
   Login: InReach
   Password: ******
   ```

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

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

10. Access the subscriber account for which you are creating the Trusted Key:

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

11. Execute the ssh key command:

```
Subs_gina >>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.)

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

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

The first time you will get prompt to generate a password for Subscriber gina if you have not already done so. The second SSH connection will not prompt you for a password but will use the Public key and connect you directly in.

Configuring Subscribers for Remote Console Management

This example shows how to configure a subscriber for remote console management.

Prerequisites

The prerequisite for this configuration example is the following:

- Configure ports for Remote Console Management. (For more information, refer to "Configuring Ports for Remote Console Management" on page 72.)

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. Create a subscriber account, or access an existing subscriber account:

```
Config:0 >>subscriber Mark
```

3. Specify Telnet as an access method for the subscriber:

```
Subs_Mark >>access telnet enable
```

4. Specify a Telnet Mode for the subscriber:

```
Subs_Mark >>telnet mode character
```

5. Specify SSH as an access method for the subscriber:

```
Subs_Mark >>access ssh enable
```

6. Specify the SSH encryption type for the subscriber:

```
Subs_Mark >>ssh cipher triple-des
```

7. Specify the Web as an access method for the subscriber:

   Subs_Mark >>`access web enable`

8. Specify that the subscriber will have console access to the LX unit:

   Subs_Mark >>`access console enable`

9. Specify the console ports that the subscriber can access::

   Subs_Mark >>`access port 2 3 5 6`

   NOTE: The ports in the access ports command must be configured for console access as described in "Configuring Ports for Remote Console Management" on page 72.

10. Create a login password the subscriber:

    Subs_mark >>`password`

    The following prompts are displayed:

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

11. 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.)

Chapter 7

Configuring IP Interfaces and Broadcast Groups

This chapter provides an example of how to create an IP Interface and an example of how to create a Broadcast Group.

IP Interface Creation Example

This example shows how to create an IP Interface in the LX CLI. For more information on IP Interfaces, refer to "Configuring IP Interfaces" in the *LX-Series Configuration Guide*. An IP Interface can be configured as an IP Rotary. Refer to "Configuring an IP Rotary on the LX Platform" on page 125 for more information.

After you have created an IP Interface, you can configure Broadcast Groups for it. Refer to "Broadcast Group Creation Example" on page 122 for an example of creating a Broadcast Group.

Prerequisites

The prerequisites for this task are the following:

- Configure an authentication method (LOCAL, RADIUS, TACACS+, or SecurID) for the IP interface.
- If you are using a server-based authentication method (i.e., RADIUS, TACACS+, or SecurID), set up the authentication server that you will be using to authenticate connections to the port. For more information, refer to the following sections in the *LX-Series Configuration Guide*:
  - "Installing and Configuring the RADIUS Server on a Network-based Host"

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

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 Interface Command Mode for the IP Interface that you want to configure:

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

3. Specify an IP Address, and Subnet Mask, for the interface:

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

4. Specify the Broadcast Address for the IP interface:

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

5. Specify the SSH Keepalive Count for the IP Interface:

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

6. Specify the SSH Keepalive Interval for the IP Interface:

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

7. Specify the Maximum Transmission Units (MTU) for the IP Interface:

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

8. Specify the Virtual Port Socket Number for making an SSH connection to the IP interface:

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

9. Specify the Virtual Port Socket Number for making a Telnet connection to the IP interface:

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

10. Configure an authentication method for the IP Interface:

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

    NOTE: You can configure LOCAL, RADIUS, SecurID, or TACACS+ as the authentication method for an IP Interface. For more information, refer to "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface" in the *LX-Series Configuration Guide*.

11. Configure an accounting method for the IP Interface

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

    NOTE: If you specified RADIUS as the authentication method in step 10, the only accounting method that you can specify is RADIUS. If you specified TACACS+ as the authentication method in step 10, the only accounting method that you can specify is TACACS+. You cannot configure an accounting method for SecurID or LOCAL authentication.

12. Configure Fallback authentication for the IP Interface:

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

13. Verify the configuration of the IP Interface:

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

Figure 34 shows the Interface Characteristics Screen for Interface 1.

```
Time:                                          Mon, 22 Dec 1969 16:14:27
Interface Name:          Interface_1  Bound to :                     eth0
IP MTU Size:                  1200
IP Address   :          119.20.112.3  Learned IP Address  :  102.19.169.191
IP Mask      :             255.0.0.0  Learned IP Mask     :   255.255.255.0
IP Broadcast :       119.255.255.255  Learned IP Broadcast:  102.19.169.255
Interface Status:            In Use  Learned IP Gateway  :    102.19.169.1
Rotary Feature:            Disabled  Learned IP DNS      :         0.0.0.0
Authentication:              Radius  Radius Accounting:           Enabled
Authentication FallBack:     Enabled  Tacacs+ Accounting:          Disabled
SSH    port:                    988  Telnet port:                   1743
SSH Keepalive Interval:          30  SSH Keepalive Count:              8
```

Figure 34 - Interface Characteristics Screen

Broadcast Group Creation Example

This example shows how to create a Broadcast Group on an IP Interface. For more information on Broadcast Groups, refer to "Configuring IP Interfaces" in the *LX-Series Configuration Guide*. An IP Interface can be configured as an IP Rotary. Refer to "Configuring an IP Rotary on the LX Platform" on page 125 for more information.

Prerequisites

The prerequisites for this task are the following:

- Configure an IP Interface. For more information, refer to "Setting Up IP Interfaces" in the *LX-Series Configuration Guide* or "IP Interface Creation Example" on page 119.

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 Interface Command Mode for an IP Interface:

   Config:0 >>`interface 1`

3. Create a Broadcast Group on the current IP Interface:

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

   This enters the Broadcast Group Command Mode. The Broadcast Group Command prompt (**BrGroups 4:0 >>**) is displayed.

4. Specify the Master Ports for the Broadcast Group:

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

5. Specify the Slave Ports for the Broadcast Group:

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

6. Specify that a timestamp will be appended to each line of data that is broadcast from the asynchronous Master Port 5:

   BrGroups 4:0 >>`master port async 5 timestamp`

7. Specify that the asynchronous Slave Port 6 will discard data without forwarding it to the Master Port(s):

   BrGroups 4:0 >>`slave port async 6 discard`

8. Specify that the asynchronous Slave Port 7 will echo any data that comes into it from the serial line:

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

9. Specify the Telnet mode for the Broadcast Group:

   BrGroups 4:0 >>`mode line`

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

    BrGroups 4:0 >>`exit`

11. Enable the Broadcast Group that you just created; for example:

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

12. Verify the configuration of the Broadcast Group that you just created:

    Intf 1-1:0 >>`show interface broadcast group 4 characteristics`

Figure 35 shows an example of the Broadcast Group Characteristics Screen for Broadcast Group 4.

```
Time: 08 Nov 2002 16:29:26 US/EASTERN
Broadcast Group Number:            4  Mode:             Line Mode
State:                         Enabled
Async Master port(s) with Timestamp:
 5
Async Master port(s) without Timestamp:

TCP Master port(s) with Timestamp:

TCP Master port(s) without Timestamp:
 1500
Async Slave port(s) with Discard:
 6
Async Slave port(s) without Discard:
 4,7
Async Slave port(s) with Local Echo:
 7
Async Slave port(s) without Local Echo:
 4,6
TCP Slave port(s) with Discard:

TCP Slave port(s) without Discard:
 2500
TCP Slave port(s) with Local Echo:

TCP Slave port(s) without Local Echo:
 2500
```

Figure 35 - Broadcast Group Characteristics Screen

Configuring an IP Rotary on the LX Platform

This example shows how to configure an IP Rotary on the LX. For background information on this task, refer to "Configuring Rotaries" in the *LX-Series Configuration Guide*.

NOTE: If you want to use SSH only, set the telnet address to 0.

Prerequisites

The IP Interface on which you create the rotary must have an IP address specified for it. You specify an IP address for an Interface with the `address` command in the Interface Command Mode; for example:

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

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 Interface Command Mode for the IP interface that you want to configure as a Rotary:

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

3. Create a Rotary, and assign LX asynchronous ports to the Rotary:

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

4. Use the `rotary type` command to specify the type (search method) for the Rotary:

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

5. Assign a TCP socket number to the Rotary:

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

NOTE: If you do not want to specify a telnet port number, set the TCP rotary to 23 for each port of the rotary.

6. Assign an SSH socket number to the Rotary:

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

7. Enable the Rotary:

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

8. Verify the Rotary:

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

```
Rotary IP Address    TCP    SSH       Rotary Type   Rotary State  Serial Ports
   10.240.10.100    3000   3022       Round Robin        Enabled         1 2 3
```

Figure 36 - Rotary Characteristics Screen

Notes

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

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

Appendix A - Advanced Features

This Appendix explains some advanced LX 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 13 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 13 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
```

INDEX