

# **FIPS 140-2 Security Policy**

## **MRV LX-4000T and LX-8000S Series**

---

MRV Communications  
295 Foster St.  
Littleton, MA 01460  
USA

August 2, 2007

Revision Version .29



# FIPS 140-2 Security Policy

## LX-4000T and LX-8000S Series

### 1. Introduction

The following describes the security policy for the LX-4000T and LX-8000S Series Console Servers. The LX Series is a key component of MRV's Out-of-Band Network solution. Out-of-Band Networks provide secure remote service port access and remote power control to devices in an organization's networks and infrastructures. This nearly eliminates the need for physical presence at a device to correct problems or manage its everyday operation. MRV's Out-of-Band Network solution includes console servers, terminal servers, device servers, remote power control and management system. These capabilities combined with FIPS 140-2 security make the LX Series an ideal choice for providing secure remote access in a variety of environments.

#### 1.1. Purpose

This document covers the secure operation of the LX-4000T and LX-8000S Series including initialization, roles, and responsibilities of operating the product in a secure, FIPS 140-2 compliant manner.

#### 1.2. Versions

The module consists of two firmware images, linuxito and ppciboot, that have following firmware versions.

linuxito version : 4.1.4

ppciboot version: 4.1.4

For the LX-4000T Series there are thirty-two hardware configurations as described in Section 2.1. Therefore, there are thirty-two hardware versions in the table below.

<b>Model</b>	<b>Top Level</b>	<b>Rev</b>	<b>B/L</b>	<b>Rev</b>
LX-4008T-001ACF	600-R3265	A	400-R0029	A
LX-4008T-002ACF	600-R3266	A	400-R0029	A
LX-4008T-012DCF	600-R3267	A	400-R0030	A
LX-4008T-101ACF	600-R3268	A	400-R0029	A
LX-4008T-102ACF	600-R3269	A	400-R0029	A
LX-4008T-112DCF	600-R3270	A	400-R0030	A
LX-4016T-001ACF	600-R3271	A	400-R0031	A
LX-4016T-002ACF	600-R3272	A	400-R0031	A
LX-4016T-012DCF	600-R3273	A	400-R0032	A
LX-4016T-101ACF	600-R3274	A	400-R0031	A
LX-4016T-102ACF	600-R3275	A	400-R0031	A
LX-4016T-112DCF	600-R3276	A	400-R0032	A
LX-4032T-001ACF	600-R3277	A	400-R0033	A
LX-4032T-002ACF	600-R3278	A	400-R0033	A
LX-4032T-012DCF	600-R3279	A	400-R0034	A
LX-4032T-101ACF	600-R3280	A	400-R0033	A
LX-4032T-102ACF	600-R3281	A	400-R0033	A
LX-4032T-112DCF	600-R3282	A	400-R0034	A
LX-4048T-001ACF	600-R3283	A	400-R0027	A
LX-4048T-002ACF	600-R3284	A	400-R0027	A
LX-4048T-012DCF	600-R3285	A	400-R0028	A
LX-4048T-101ACF	600-R3286	A	400-R0027	A
LX-4048T-102ACF	600-R3287	A	400-R0027	A
LX-4048T-112DCF	600-R3288	A	400-R0028	A

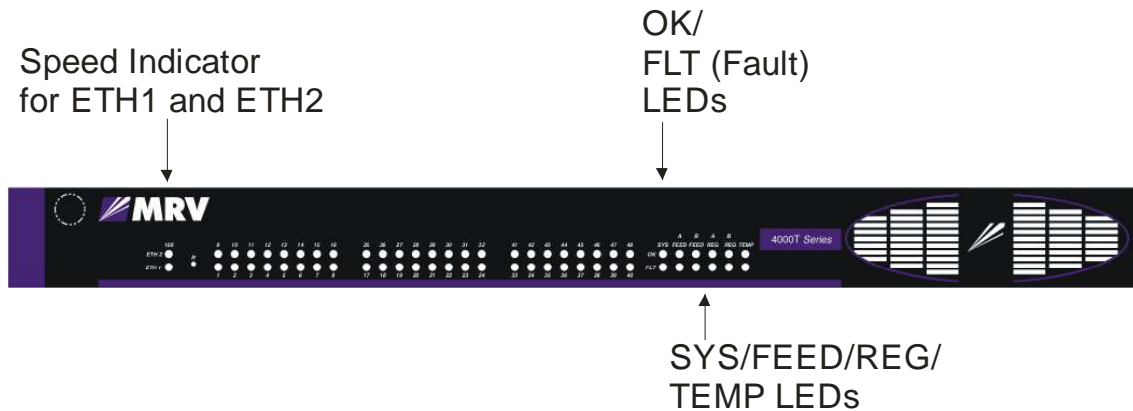
For the LX-8000S Series there are twelve hardware configurations as described in Section 2.2. Therefore, there are twelve hardware versions in the table below.

<b>Model</b>	<b>Top Level</b>	<b>Rev</b>	<b>B/L</b>	<b>Rev</b>
LX-8040S-112DCF	600-R3248	B	400-R0021	D
LX-8020S-001ACF	600-R3249	B	400-R0022	E
LX-8020S-002ACF	600-R3250	B	400-R0022	E
LX-8020S-012DCF	600-R3251	B	400-R0021	D
LX-8020S-101ACF	600-R3252	C	400-R0022	E
LX-8020S-102ACF	600-R3253	C	400-R0022	E
LX-8020S-112DCF	600-R3254	B	400-R0021	D
LX-8040S-001ACF	600-R3255	B	400-R0022	E
LX-8040S-002ACF	600-R3256	B	400-R0022	E
LX-8040S-012DCF	600-R3257	B	400-R0021	D
LX-8040S-101ACF	600-R3258	C	400-R0022	E
LX-8040S-102ACF	600-R3259	C	400-R0022	E

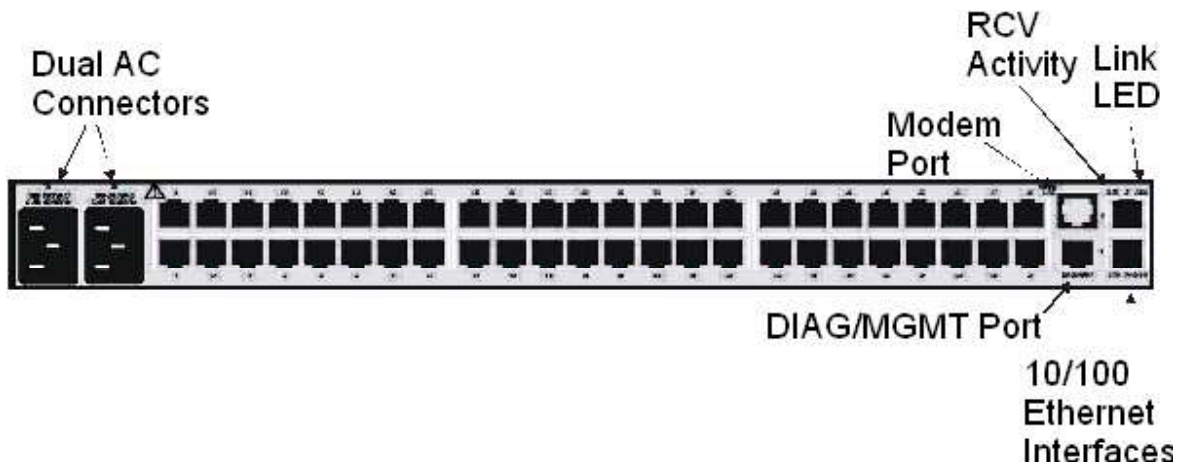
## 2. Interfaces

The LX-4000T and LX-8000S Series are considered a multi-chip standalone module, and the cryptographic boundary of the module is defined by the outer case of module.

### 2.1. LX-4000T Series



Dual AC 4048T Front Panel



Dual AC 4048T Rear Panel

- **LX-4008T-001ACF LX-4000T** with (8) RS232 RJ45 ports, & single AC power
- **LX-4008T-002ACF LX-4000T** with (8) RS232 RJ45 ports, & dual AC power
- **LX-4008T-012DCF LX-4000T** with (8) RS232 RJ45 ports, & dual DC (36-72V) power

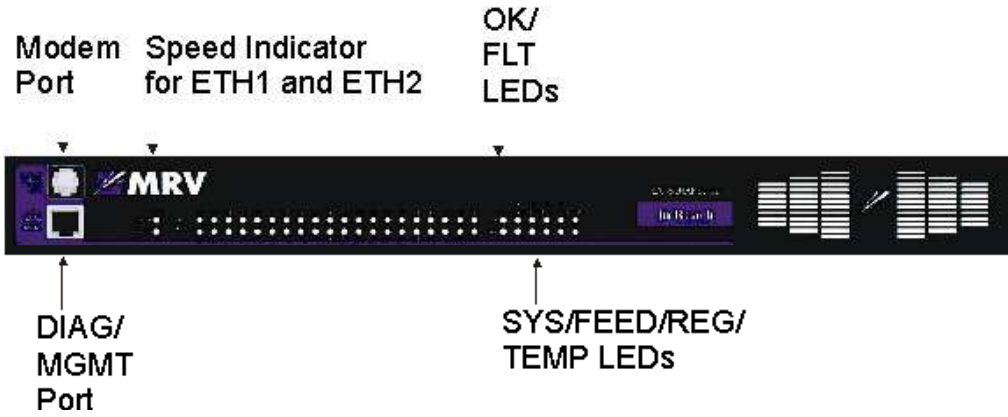
- **LX-4008T-101ACF LX-4000T** with (8) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-4008T-102ACF LX-4000T** with (8) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-4008T-112DCF LX-4000T** with (8) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40016T-001ACF LX-4000T** with (16) RS232 RJ45 ports, & single AC power
- **LX-40016T-002ACF LX-4000T** with (16) RS232 RJ45 ports, & dual AC power
- **LX-40016T-012DCF LX-4000T** with (16) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-40016T-101ACF LX-4000T** with (16) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40016T-102ACF LX-4000T** with (16) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-40016T-112DCF LX-4000T** with (16) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40032T-001ACF LX-4000T** with (32) RS232 RJ45 ports, & single AC power
- **LX-40032T-002ACF LX-4000T** with (32) RS232 RJ45 ports, & dual AC power
- **LX-40032T-012DCF LX-4000T** with (32) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-40032T-101ACF LX-4000T** with (32) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40032T-102ACF LX-4000T** with (32) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-40032T-112DCF LX-4000T** with (32) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90
- **LX-40048T-001ACF LX-4000T** with (48) RS232 RJ45 ports, & single AC power
- **LX-40048T-002ACF LX-4000T** with (48) RS232 RJ45 ports, & dual AC power
- **LX-40048T-012DCF LX-4000T** with (48) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-40048T-101ACF LX-4000T** with (48) RS232 RJ45 ports, & single AC power & internal V.90 modem
- **LX-40048T-102ACF LX-4000T** with (48) RS232 RJ45 ports, & dual AC power & internal V.90 modem
- **LX-4048T-112DCF LX-4000T** with (48) RS232 RJ45 ports, & dual DC (36-72V) power & internal modem V.90

## **2.2. LX-8000S Series**

- **LX-8020S-001ACF LX-8000S** with (20) RS232 RJ45 ports, & AC power
- **LX-8020S-101ACF LX-8000S** with (20) RS232 RJ45 ports, AC power & internal V.90 modem
- **LX-8040S-001ACF LX-8000S** with (40) RS232 RJ45 ports, & AC power
- **LX-8040S-101ACF LX-8000S** with (40) RS232 RJ45 ports, AC power & internal V.90 modem
- **LX-8020S-002ACF LX-8000S** with (20 )RS232 RJ45 ports, & dual AC power
- **LX-8020S-102ACF LX-8000S** with (20) RS232 RJ45 ports, dual AC power & internal V.90 modem
- **LX-8040S-002ACF LX-8000S** with (40) RS232 RJ45 ports, & dual AC power
- **LX-8040S-102ACF LX-8000S** with (40) RS232 RJ45 ports, dual AC power & internal V.90 modem
- **LX-8020S-012DCF LX-8000S** with (20) RS232 RJ45 ports, & dual DC (36-72V) power
- **LX-8020S-112DCF LX-8000S** with (20) RS232 RJ45 ports, dual DC (36-72V) power & internal V.90 modem
- **LX-8040S-012DCF LX-8000S** with (40) RS232 RJ45 ports, & dual DC (36-72V) power

- **LX-8040S-112DCF LX-8000S** with (40) RS232 RJ45 ports, dual DC (36-72V) power & internal V.90 modem



**LX-Series Dual AC 8040S Front Panel**



**LX-Series Dual AC 8040S Rear Panel**

The logical interfaces and their module mapping are described in the following table:

Logical Interface	Physical Interface Mapping
Data Input Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 20 RS232 RJ45 Ports / 32 RS232 RJ45 Ports 40 RS232 RJ45 Ports / 48 RS232 RJ45 Ports Console Port (RS232 Modem Port)
Data Output Interface	2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 20 RS232 RJ45 Ports / 32 RS232 RJ45 Ports 40 RS232 RJ45 Ports / 48 RS232 RJ45 Ports Console Port (RS232 Modem Port)
Control Input Interface	Reset Button 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 20 RS232 RJ45 Ports / 32 RS232 RJ45 Ports 40 RS232 RJ45 Ports / 48 RS232 RJ45 Ports Console Port (RS232 Modem Port)
Status Output Interface	LEDs, 2 10/100 BASE-TX Ports 2 10/100 BASE-TX Ports 8 RS232 RJ45 Ports / 16 RS232 RJ45 Ports 20 RS232 RJ45 Ports / 32 RS232 RJ45 Ports 40 RS232 RJ45 Ports / 48 RS232 RJ45 Ports Console Port (RS232 Modem Port)
Power Interface	(Dual) AC Power Input / Dual DC Power Input



### **3. Roles, Services, and Authentication**

The LX-4000T and LX-8000S Series provides three different roles and a set of services specific to each of the roles. The LX4000T and LX-8000S Series will authenticate an operator by verifying his password and will then explicitly assign him either the Crypto-Officer or User role, depending on his security level. The module provides role-based authentication for all operators.

When operating in FIPS-mode, the LX4000T and LX-8000S Series enforce a minimum password length of six characters; this minimum length combined with the 94 possible characters and a second delay after an incorrect password ensure that role authentication meets the 140-2 strength of authentication requirements (yielding a probability of  $1/6.89 \times 10^{11}$  to guess a password and a probability of  $1/1.14 \times 10^{10}$  to guess a password within a one-minute period).

#### **3.1. Roles**

The roles of the module include a PPCIBOOT User, Crypto-Officer and a User Role.

##### ***PPCIBOOT User***

The PPCIBOOT User is responsible for configuring the boot loader.

The following services are provided:

- Configure boot parameters
- Unconfigure boot parameters
- Enable FIPS 140-2 mode
- Disable FIPS 140-2 mode

##### ***Crypto-Officer Role***

The Crypto-Officer is the administrator of the LX and does the configuration.

The following services are provided:

- Configure system parameters
- Unconfigure system parameters
- Get system status
- Save configuration
- Exec system commands
- Exit from system

### **User Role**

The User Role performs a limited set of services to retrieve information or status. This role cannot perform services to configure the box.

The module allows concurrent users.

All roles can use role-based authentication locally or remotely via RADIUS, TACACS+, or RSA SecurID.

### **3.2. Algorithms**

The LX supports the following cryptographic algorithms.

#### **Approved cryptographic algorithms**

##### **Symmetric Key Algorithms**

Algorithm	Modes	Key Size
AES	ECB, CBC, CFB, CTR	128, 192, 256
Triple-DES	ECB, CBC	112, 168

##### **Hashing Algorithms**

SHA-1
-------

##### **Message Authentication Algorithms**

HMAC SHA-1
------------

##### **Public Key Algorithms**

Algorithm	Key Size
RSA (PKCS 1.5)	1024
DSA	1024

#### **Non-FIPS Approved Algorithm**

##### **Symmetric Key Algorithms**

Algorithm	Modes	Key Size
DES	ECB, CBC	64

##### **Public Key Algorithms**

Algorithm	Key Size
RSA encrypt / decrypt (key wrapping)	1024 (min), 2048 (max)

### Hashing Algorithms

MD5
-----

### Key Exchange Algorithm

Algorithm	Key Size
Diffie-Hellman (key agreement)	1024 (min), 6144 (max)

## **Key Generation**

The module implements the ANSI X9.31 A.2.4 based PRNG. All key generation functions use the approved PRNG implementation.

## 4. Setting FIPS 140-2 Mode

The module images are pre-installed in the flash and new versions of software are shipped on CDs. All shipping occurs via a reputable courier service. The administrator should also inspect to make sure the boxes have not been tampered with or damaged upon receiving the modules, which could indicate a security compromise.

### 4.1. Prerequisites

The following requirements must be met to use the product in a FIPS 140-2 compliant configuration:

- You must use the FIPS 140-2 validated versions of the LX linuxito and ppciboot software. *Only specific versions of the LX software are tested by an accredited cryptographic module test lab.*
- You must be running the software on the FIPS 140-2 tested LX-Series platform.
- FIPS 140-2 mode must be enabled on the LX-Series FIPS 140-2 validated unit(s).
- If you intend to use SNMP with FIPS 140-2, you must use the SNMP V3 version.
- You must place the provided tamper-evident labels in the proper locations.

### 4.2. Notes and Restrictions

- The default subscriber InReach password must be changed.
- The default ppciboot password must be changed.
- The default system password must be changed.
- All configured passwords must be greater than or equal to 6 characters in length.
- If using an SNMP NMS or SNMP MIB browser, the application must support SNMPV3 and must support AES encryption. By default SNMP is disabled for security reasons. SNMP V3 must be enabled and configured fully on the LX in order to function with the NMS.
- SSH Clients must support sshV2, AES or 3DES ciphers, and HMAC-SHA1 or HMAC-SHA1-96 message authentication codes.

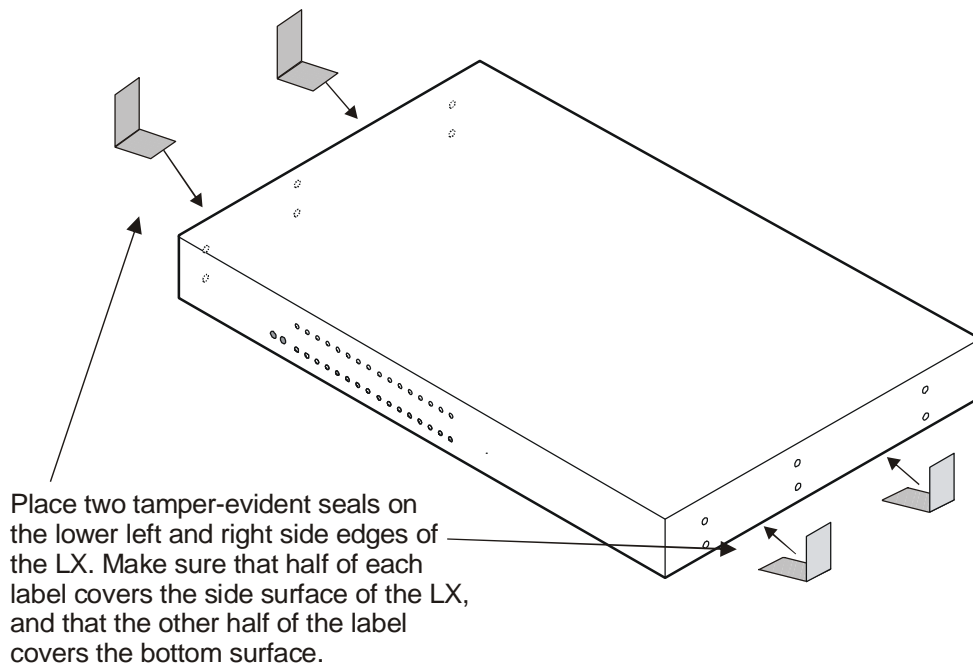
### 4.3. Applying Tamper Evident Labels

NOTE: To be FIPS 140-2 compliant, you must apply the tamper-evident labels before you power on and configure the LX unit.

Once the LX has been configured in FIPS 140-2 mode, the cover cannot be removed without signs of tampering. Applying tamper-evident labels to the LX unit will prevent anyone from opening the unit without your knowledge.

To seal the cover of the LX, apply a tamper-evident label as follows:

1. Clean the LX surface of any grease or dirt before you apply the tamper-evident labels.
2. Apply two labels each to the bottom left and right sides of the unit, as shown in Figure 1.



**Figure 1 – Location of the Tamper Evident Labels**

3. Record the serial numbers of the labels you attached to the LX unit.
4. Allow 24 hours for the adhesive in the tamper-evident labels to cure.

NOTE: You should periodically check the labels to ensure that no one has tampered with the unit.

### 4.4. Making Sure Your Software is FIPS 140-2 Validated

Do the following to determine if the software you are running has been FIPS 140-2 validated:

1. Log into the CLI.

2. Enter the `show version` command at the `InReach:0 >` prompt; for example:

```
InReach:0 > show version
```

The Show Version screen appears, with the relevant fields highlighted:

Linux Kernel Version:	x.x.x.x
Linux In-Reach Version:	x
Software Version (Runtime):	x.x.x.x (FIPS 140-2)
Software Version (Flash):	x.x.x.x (FIPS 140-2)
Ppciboot Version:	x.x.x.x (FIPS 140-2)

**Figure 2 – Show Version Screen**

If the software you are running has been FIPS 140-2 validated, the word (FIPS 140-2) appears to the right of the Software Version number and the Ppciboot Version number. If (FIPS 140-2) does not appear, your software has not been validated.

#### 4.5. Enabling FIPS 140-2 Mode of Operation

##### **IMPORTANT!**

If you want to configure your unit to run FIPS 140-2 Mode of Operation, you must do so **before** you attempt to configure the unit over and above the default settings. The act of enabling FIPS 140-2 mode will default the unit's configuration.

When FIPS 140-2 is enabled, the configuration file is returned to defaults. Therefore, if you fully configured your unit and then turned on FIPS 140-2, your configuration will return to factory defaults. FIPS 140-2 mandates this to ensure that any passwords with fewer than six characters are purged, and that all unsupported applications are disabled.

**NOTE:** If you enable FIPS 140-2 Security, option [1] Boot from Network is set to Flash Only automatically. You can only update from the CLI or GUI while FIPS 140-2 is enabled. Option [4] Update ppciboot Firmware is disabled when FIPS 140-2 is enabled.

The following passwords must be at least six characters long:

- Subscriber
- Config
- ppciboot
- Radius Secret
- TACACS+ Secret
- PAP/CHAP Outgoing Secret

- SSH Public Key must be at least 1024 bits.

The FIPS 140-2 Security option lets you enable or disable FIPS 140-2 mode of operation.

```

Main Menu

[1] Boot from:                               Flash only
    Image currently in flash:                 4.1.4 (FIPS 140-2)
[2] Time Out, in seconds (0=disabled): 8
[3] IP Configuration Menu
[4] Update Ppciboot Firmware
[5] Ethernet Network Link:                   auto
[6] Change PPCiBoot password
[7] FIPS 140-2 Security:                 yes
[9] ppciboot image name:                    ppciboot.img
[0] software image name:                    linuxito.img

[*] Reset to System Defaults
[D] Downgrade Ppciboot Firmware
[S] Save Configuration
[B] Boot System

Make a choice:

```

To enable or disable FIPS 140-2 security:

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

```

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

```

2. If you select *y* (this defaults the flash immediately), a Resetting Linux Configuration message appears, and the Main Menu reappears after a few seconds. If you select *n*, the Main Menu reappears immediately.
3. If FIPS 140-2 is already enabled and you want to disable it, press 7 (FIPS 140-2 Security) from the Main Menu.
4. Press *B* to Boot the system. Do this only after you have configured the ppciboot options and saved the configuration.

#### 4.6. **Changing the Default ppciboot Password**

After enabling FIPS 140-2, you must enter a new ppciboot password of greater than six characters.

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

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

**Enter your current ppciboot password:**



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

**Enter your NEW password: :**

2. Enter the new ppciboot password at the above prompt. The password must be greater than six characters long.

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

**Re-enter your NEW password:**

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

#### **4.7. Changing the Default Subscriber Password**

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

##### *Changing the Default Password for the InReach User*

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

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

```
Config:0 >> subscriber InReach
```

3. Enter the `password` command at the **Subs\_InReach >>** prompt; for example:

```
Subs_InReach:0 >> password
```

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

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

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

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

## Changing the Default Configuration Password

It is also widely known that the default Superuser password is **system**. To reduce the risk of an unauthorized user gaining access to the Superuser Command Mode, you must change this password to something other than **system**. The password must be at least six characters long.

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

1. Access the Configuration Command Mode.
2. Enter the password command at the **Config:0 >>** prompt; for example:  
**Config:0 >>**password
3. Enter a new Superuser password at the **Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:  
**Enter your NEW password:\*\*\*\*\***
4. Re-enter the new Superuser password at the **Re-Enter your NEW password:** prompt. The password will be displayed as asterisks, as in the following example:

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

## 4.8. FIPS 140-2 Mode Console Access

When the LX is in FIPS 140-2 mode telnet is not allowed. Therefore, you must ssh to the unit in Version 2 mode.

```
ssh -l InReach 10.10.10.10
```

If non-FIPS 140-2 approved algorithms are being used, please see and edit the `/etc/ssh/ssh_config` file on your host system.

## 4.9. Applications Unsupported in FIPS 140-2 Mode of Operation

Listed below are all the unsupported FIPS 140-2 protocols and features, which are disabled when FIPS 140-2 mode of operation is enabled on the LX software.

Unsupported FIPS Protocols and Features

Feature	Impact	Reason
Telnet client/server	Disabled	Passwords are passed in plaintext
rlogin client	Disabled	Passwords are passed in plaintext
Web GUI	Disabled	Only AES encryption mode will be

unencrypted		supported, customer is required to run FIPS 140-2 approved JRE on host machine
SNMP v1 & v2	Disabled	Community strings are passed in plaintext
SSH V1 Client / Server	Disabled	Security flaws / known vulnerabilities
Passwords/ Secrets less than 6 characters	Disabled	Due to FIPS 140-2 max authentication fail attempts
Linux shell access	Restricted	Disabled access to secret and private keys
Boot or load software image from network	Disabled	FIPS 140-2 requires DSA signatures on images, units must boot from FLASH
Updating ppciboot.img from ppciboot menu	Disabled	FIPS 140-2 requires ppciboot to be updated from runtime software via CLI or GUI
LDAP	Disabled	Passwords passed in plaintext
Login mode shell	Disabled	Unfettered access
Broadcast Groups	Limited	No support for groups that have a master/slave of TCP
Fingerd	Disabled	Allows anyone to see who is logged in
Boot config from network (tftp)	Disabled	Configuration sent in plaintext
Save config to network (tftp)	Disabled	Configuration sent in plaintext
No authentication	Disabled	Insecure
Dedicated Services	Disabled	Passwords are passed in plaintext
Port Async Connect	Disabled	Insecure
TCP Pipe	Disabled	In plain text

#### **4.10. Upgrading Software**

The `ppciboot.img.sign` and `linuxito.img.sign` digital signature files are used to authenticate load images during loading. Place these

files on the TFTP server. The LX unit will download them automatically.

Refer to “How to Upgrade the Software” in the *LX-Series Configuration Guide* for more information on upgrading the software.

#### 4.11. FIPS 140-2 JCE Module Commands

NOTE: These commands apply only if you want to use the GUI in FIPS 140-2 mode.

NOTE: You can purchase FIPS 140-2 compliant JCE modules from two vendors. The vendors are listed below, along with the specific JCE Module name.

- IBM – IBMJCEFIPS
- RSA – JSafeJCE

NOTE: These commands are available only when the LX is running in FIPS 140-2 Mode.

A new FIPS 140-2 JCE Module command allows you to name the web server FIPS 140-2 JCE Module. You can access it in the Configuration Command Mode.

##### *Configuring a Web Server FIPS 140-2 JCE Module Name*

Use the following command to configure a Web Server FIPS 140-2 JCE Module name. The module name is set by the module vendor. For example, if you are using RSA’s JSafe cryptographic module, the module name would be JSafeJCE. Enter `no web_server fips jcemodule` to reset to the default, which is “null”. The module name can be up to 16 characters long.

```
Config:0>> web_server fips jcemodule <module_name>
```

##### **Examples**

```
Config:0>> web_server fips jcemodule JSafeJCE
```

```
Config:0>> no web_server fips jcemodule
```

#### 4.12. Viewing the Web Server FIPS 140-2 JCE Module Name

Use the `show web characteristics` command to display the Web Characteristics Screen. An example of this screen follows, with the new Web JCEModule field highlighted:

Time:		Fri, 28 Jan 2005 13:52:48 US/EASTERN	
Web Server:	Enabled	Web Server Port:	80
Web Server Timeout:	20	Web Encrypt:	Disabled
Web Banner:	Enabled	<b>Web JceModule:</b>	<b>JsafeJCEFIPS</b>

## 5. Definition of SRDIs Modes of Access

This section specifies the LX's Security Relevant Data Items.

### 5.1. Cryptographic Keys, CSPs, and SRDIs

While operating in a level 2 FIPS compliant manner, the LX-4000T and LX-8000S Series contains the following security relevant data items:

Security Relevant Data Item	SRDI Description
SSH RSA host 1024-bit private authentication key	Used for SSH authentication. Stored in flash.
SSH DSA host 1024-bit private authentication key	Used for SSH authentication. Stored in flash.
Web Server RSA 1024-bit private key	Used for Web server authentication and key transport. Stored in flash.
SSH Session key (AES, TDES)	Used to encrypt SSH sessions. Not stored across power cycles, stored in RAM.
Cluster Secret	Shared secret used to authenticate cluster members. Stored in configuration file in flash.
User passwords	User passwords. Stored in configuration file in flash.
Crypto Officer password	Password used to authenticate Crypto Officer. Stored in configuration file in flash.
Iboot User password	Password used to authenticate Iboot User. Stored in flash.
SNMP v3 AES key	Key used for SNMP v3 encryption. Stored in flash.
Outgoing PAP Secret	Used in PPP authentication. Stored in configuration file in flash.
Outgoing CHAP Secret	Used in PPP authentication. Stored in configuration file in flash.
RADIUS secret	Shared secret used with authentication server. Stored in configuration file in flash.
TACACS+ secret	Shared secret used with authentication server. Stored in configuration file in flash.
Cluster Diffie-Hellman private key	Diffie-Hellman private key used in Clustering. Stored in RAM.
SSH Diffie-Hellman private key	Diffie-Hellman private key used in SSH. Stored in RAM.

Web Server Session key	Web server session encryption key. Stored in RAM.
Cluster Session key	Cluster session encryption key. Stored in RAM.
RSA SecurID Secret	Shared secret of RSA SecurID. Stored in Flash.
DSA public key for firmware load	DSA public key used in signature verification when loading firmware. Stored in flash.
Approved PRNG initial seed and seed key	Used to initialize approved PRNG. Stored in flash.
Runtime approved PRNG seed and seed key	The runtime seed and seed key values stored in RAM

The following matrix defines the set of services to the CSP of the module, providing information on reading, writing, and deleting.

The matrix uses the following convention:

- R: Read
- W: Write
- D: Delete

SRDI/Role/Service Access Policy	Security Relevant Data Item																				
Role/Service																					
User role																					
Connect to an outside unit via console ports																					
Get system status							R		R	R		R	R	R	R	R	R				
Clear screen																					
Use ping utility																					
Exit from system																					
Crypto-Officer Role																					
Configure system parameters							W		W	W	W	W	W	W	W	W	W				
Unconfigure system parameters							D		D	D	D	D	D	D	D	D	D				
Get system status							R		R	R		R	R	R	R	R					
Save Configuration																					
Exec system commands																					
Exit from system																					
Iboot User Role																					
Configure boot parameters																					
Unconfigure boot parameters																					
Enable FIPS 140-2 mode		D	D	D	D	D	D	D	D	D	D	D	D	D	D	D					
Disable FIPS 140-2 mode																					

## **6. Mitigation of Other Attacks**

This section is not applicable.