Release Notes

LX Series
Version 3.0.1
April 2003
450-0143J

Contents

Introduction

These release notes provide important information about the LX product line. They cite supported features as well as any notes and restrictions for the following software version:

- Software Image Version 3.0.1

Earlier releases are documented in the **Archives** Directory on the LX Documentation CD. It is also possible to download release notes by doing the following:

1. Point your browser to the MRV Service and Support site (http://service.mrv.com/support/).
2. Select **In-Reach (IR and LX)** from the Product Type pulldown list.
3. Select any LX product from the Product pulldown list.
4. Select the **Software Updates** option below the Products pulldown list.
5. Click the **Get Information** button. This displays the Software Updates page.
6. Select a Release Notes filename from the Software Updates page.

   NOTE: You must supply a User Name and password to download the Release Notes.

New Version of ppciboot

IMPORTANT

The LX-4048 must run on 3.0.1 or higher software and the latest ppciboot firmware. If you have an LX-4008S-xxx unit running software version V2.0.0 or above, and you are updating to Release V3.0.1, you must also update the ppciboot (V1.0.1) for the software to function properly. If you have a different model LX unit, MRV Communications recommends that you perform the same ppciboot update. Refer to "Upgrading Software and ppciboot with the Command Line Interface" for information on performing the upgrade. When you upgrade the software, use the DIAG port (port 0) as your management port.

MRV Communications recommends that you update to the latest software and ppciboot, regardless of which LX model you are upgrading. However, each model will run on a minimum required software and ppciboot version. The minimum requirements for each model are shown in the following table:

LX Model	LX Software Version	ppciboot – Minimum Revision Required to Support Hardware
LX-4008	V2.2.0	V1.0.0
LX-4016	V2.2.1	V1.0.0
LX-4032	V2.2.2	V1.0.0
LX-4048	V3.0.1	V1.0.1

New Features and Enhancements

The following new features are supported in this release of the LX software:

LX-4048S Device Support

V3.0.1 and ppciboot V1.0.1 include hardware platform support for the 48 port LX unit.

Notification Enhancements

The notification messaging feature allows you to redefine 40 predefined syslog messages. Each configurable syslog message has a default message string, facility grouping, and priority level. You can modify these settings to generate a more useful syslog message for its environment. This allows the administrator to eliminate unwanted messages and group messages deemed useful by changing them to the desirable facility and priority levels.

The "`show notification message all`" commands list the 40 predefined syslog messages. An administrator can modify these records with the following commands:

`InReach:0``>> config`

`Config:0``>>notification`

`Notification:0``>>message # string "text message"`

`Notification:0``>>message # facility [`*`authpriv |daemon |user |kern |syslog`*`]`

`Notification:0``>>message # priority [`*`emergency|alert|critcal|error|warn|notice|info`*`]`

`Notification:0``>>message # default`

To view the notification message, enter the following command:

`InReach:0``>> show notification message #`

```
Message record 1:
Message: Configuration mode has been entered by
Facility: user  Priority: notice

Message record 2:
Message: Configuration mode has been exited by
Facility: user  Priority: notice

Message record 3:
Message: The Shell has been entered by
Facility: user  Priority: notice

Message record 4:
Message: The Shell has been exited by
Facility: user  Priority: notice
```

Notification Message Display

Example

You may have one administrator interested in receiving messages for all users entering config mode, (MESSAGE #1). You may have another administrator who only wants to be notified if someone attempts to enter the shell mode (MESSAGE #3). To achieve this, set up two notification Service Profiles, one for each administrator. Configure the first administrator to receive messages at priority notice, and the second administrator to receive messages at priority warning. Change message records 1 and 3 as follows:

```
Notification:0>>message 1 priority notice

Notification:0>>message 3 priority warning

Notification:0>> serviceprofile admin1_email protocol smtp
Notification:0>> serviceprofile admin1_email server 10.179.176.21
Notification:0>> userprofile jsmith service admin1_email
Notification:0>> userprofile jsmith contact 1112223333@vtext.com
Notification:0>> userprofile jsmith facility user
Notification:0>> userprofile jsmith priority notice

Notification:0>> serviceprofile admin2_email protocol smtp
Notification:0>> serviceprofile admin2_email server 10.179.176.21
Notification:0>> userprofile djones service admin2_email
Notification:0>> userprofile djones contact 1112223334@vtext.com
Notification:0>> userprofile djones facility user
Notification:0>> userprofile djones priority warning
```

For more information on the Notification enhancement commands, refer to the *LX-Series Commands Reference Guide.*

Viewing All Notification Messages, Facilities, and Priorities

Use this command to show all notification message/facility/priority information.

```
InReach:0 >> show notification messages all/number [1-40]
```

```
Message record number: 1
Message:  Configuration mode has been entered by
Facility:   user        Priority:   notice

Message record number: 2
Message:  Exiting Config mode by
Facility:   user  Priority:  notice
~
```

Notification Message/Facility/Priority All Display

Viewing Specific Notification Messages, Facilities, and Priorities

Use the following command to show the notification message/facility/priority for a specific record.

```
InReach:0 >> show notification message 3
```

```
Message record number: 3
Message:  The Shell Level Mode has been entered by
Facility:   user        Priority:   notice
```

Specific Notification Message/Facility/Priority Display

Reporting State Transitions of DCD/DSR and CTS to syslogd

The `sigsnotice` priority can now be specified for a Notification User Profile. When the `sigsnotice` priority is in effect, state transitions of serial input signals DCD/DSR and CTS are reported through syslogd to the configured user profile through the linked service profile.

Before you can configure a priority of sigsnotice for a User Profile, you must configure the asynchronous port in question to generate a syslog message for a state transition of the serial input signals CTS and DCD/DSR. Use the following command:

```
Async 4-4:0>>signals syslog enable
```

In order for the state transitions of DCD/DSR and CTS to be reported to a user, the applicable User Profile must have a priority of `sigsnotice` and a facility of `kern`. Use the `userprofile facility` command to specify the facility setting of a User Profile. Use the `userprofile priority` command to specify the priority setting of a User Profile.

NOTES: If the port has CTS flow control, DCD/DSR transition will be logged, but the CTS State transition is not.

You can enable signals syslogd enable SIGsNotice on a per port basis with this command.

Refer to the *LX-Series Commands Reference Guide* for more information on the commands.

Global Feature Control

Global Feature Control allows administrators to disable several features and remote access protocols for security and access control. When a protocol is disabled, that protocol cannot establish a connection to the LX console or the virtual ports. Global Feature Control is configured in the Configuration Command mode. Features that you can enable or disable are SNMP, Telnet, GUI/Web, SSH, NTP, timed, and fingerd. SSH versions 1 and 2 are mutually exclusive; you can configure only one version at a time.

For more information on the Global Feature Control commands, refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide.*

Pattern Matching

The Pattern Matching feature is now supported on ports that are configured for databuffer access. Up to 8 pattern strings can be specified for a port. When data that matches a pattern string is received at the port, the data is put into a notification message. The notification message is in the following format:

```
Pattern match found:<data>:Msg39
```

where`<data>` is the incoming data that matches the specified pattern.

For example, the following notification messages could be generated for incoming data that matched the pattern Sun.root>:

```
Pattern match found:Sun root> Panic Dump:Msg39
```

NOTE: The text `Pattern match found` is the default content of Message 39. This text can be changed. If it is changed, the text that precedes the colon (:) will be different from Pattern match found.

The messages will be forwarded to Notification clients that have a facility of `user` and a priority of `notice` configured in their User Profiles.

You can create pattern strings with the `pattern string` command, which is executed in the Asynchronous Command Mode.

In order for the Pattern Matching feature to take effect on an asynchronous port, you must execute the `pattern match enable` command *after* you have created pattern strings with the `pattern string` command.

To display information on the Pattern Matching feature, execute the `show port async number/all pattern match characteristics` command.

Refer to the *LX-Series Commands Reference Guide* for more information on the commands.

SSH Public Key/Trusted Keys

You can create a Trusted Key for a subscriber in the Subscriber command mode. This improves ease of use and helps prevent spoofing issues. You 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. MRV supports both RSA and DSA keys. Refer to the *LX-Series Commands Reference Guide* and the *LX-Series Configuration Guide* for further details.

Specifying a Unique SSH Key for the Subscriber

To specify a unique SSH key for the subscriber, execute the `ssh key` command; for example:

```
Subs_jack >>ssh key
```

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

```
Please enter your key:
```

Paste the unique SSH key for the subscriber at the above prompt. (The unique SSH key must be generated on the host from which the subscriber will make SSH connections to the LX unit. Refer to your Linux documentation for more information on generating an SSH key.) When a subscriber has a unique SSH key, he can log on to the LX unit via SSH, without entering a password. (The only requirement is that the user must log on from the host on which his SSH key was generated.)

SecurID Authentication

This release of the LX software supports SecurID authentication. RSA SecurID® is a two-tier authentication method. A two-tier method is based on something you *know* (PIN), and something you *have* (token card). SecurID sessions are authenticated by a username and passcode. The passcode is a 4 digit PIN followed by 8 digits generated by the token card. SecurID supports both DES and SDI encryption. The primary SecurID server may have multiple identical servers on the network. These are referred to as replicas. One primary server may have as many as five replicas. You can authenticate from any one of these replicas.

1. Access the Configuration Command Mode on the LX.
2. Use the SecurID primary authentication server address command to specify the IP address of the SecurID primary authentication server:

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

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

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

   ```
   Config:0 >>securid authentication encryption sdi
   ```

4. Use the `securid authentication version` command to specify the SecurID authentication version for the LX unit. You can specify the authentication version as Version 5, or pre-Version 5 (legacy):

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

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

NOTE: When configured for legacy, use the master authentication server address in place of the primary authentication server address attribute.

5. Use the `securid authentication port` command to specify the socket your SecurID server is listening to:

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

6. Enable SecurID on the desired ports.

   ```
   Config:0 >>port async 2
   Async 2-2:0 >>access local
   Async 2-2:0 >>authentication inbound securid enable
   Async 2-2:0 >>authentication fallback enable
   Async 2-2:0 >>exit

   Config:0 >>port async 3
   Async 3-3:0 >>access remote
   Async 3-3:0 >>authentication outbound securid enable
   Async 3-3:0 >>authentication fallback enable
   Async 3-3:0 >>end
   ```

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

   ```
   InReach:0 >>show securid characteristics
   ```

```
SecurID Configuration Settings
 Authentication Version:  Version_5     Authentication Encryption:        DES
 Authentication Timeout:          5     Authentication Retransmit:          3
 Authentication Port:          5500
 V5 Primary Server:         0.0.0.0     Primary Name:            149.19.87.89
 Legacy Master Server:      0.0.0.0     Master Name:
 Legacy Slave Server:       0.0.0.0     Slave Name:
 Inbound SecurID Enabled Serial Ports: 2
 Outbound SecurID Enabled Serial Ports: 3
 SecurID Enabled Interfaces:
```

SecurID Characteristics Display

For more information on the LX implementation of SecurID authentication, refer to the following sections in the *LX-Series Configuration Guide*:

- "Setting Up RADIUS, SecurID, and TACACS+ for the LX Unit"
- "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface"
- "Setting Up Security for a Console Port"

For more information on the commands (as well as other commands), refer to the *LX-Series Commands Reference Guide.*

The iptables Commands

The iptables commands are used to create IP filters for the LX unit. IP filters are used to allow certain IP packets to pass, or not pass, through an LX unit. The iptables can be applied to IP packets that originate on the network side, or the serial side, of the LX unit.

You must navigate to the Linux shell and use the iptables commands that are available in the Kernel.

Use iptables to set up, maintain, and inspect the tables of IP packet filter rules in the Linux Kernel. iptables help manage IP traffic by creating filters known as chains. Each chain is a list of rules that can match a set of packets. Each rule specifies what to do with a packet that matches. The options are ACCEPT, DENY, or DROP. The INPUT chain filters packets coming from the LAN to the LX-Series and the OUTPUT chain filters packets leaving the LX-Series destined for the LAN.

After making any changes, you should always run the command " **iptables-save -f /config/iptables.conf**" to save the changes. To make the change permanent through reboots, you must save the configuration change by running the command "**save configuration** " from the superuser command mode.

Configuring INPUT and OUTPUT Chains

1. Enter the shell by typing:

   InReach:0>>shell

   #

2. Display the current iptables chains by typing:

   # iptables –L

3. Add or modify the INPUT or OUTPUT chain.

The following INPUT rule drops any packets coming to the LX from source address 10.240.10.240.

```
# iptables –A INPUT –s 10.240.10.240 –j DROP
```

The following OUTPUT rule drops packets originating from the LX destined for IP address 10.128.1.13.

```
#iptables –A OUTPUT –d 10.128.1.13 –j DROP
```

Saving iptables Changes

The configuration is kept in the **"/config/iptables.conf**" file. This file is generated by the **iptables-save** utility when reading the filter tables located in the Kernel.

The configuration is dynamically applied when a command is entered. The iptables-save command creates the new configuration file in /config/iptables.conf.

To make this configuration persistent through the reboot, save the configuration to the flash or the network from the super user command line as follows:

1. Verify the iptables configuration by typing:

   `# iptables –L`

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.128.1.11          anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  anywhere             10.128.1.10

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
```

IPTables Configuration Display

2. Save the iptables changes to the `/config/iptables.conf` file by typing:

   `# iptables-save –f /config/iptables.conf`

3. Save the `modify iptables.conf` file to flash or network by typing:

   `InReach>>` `save config [flash|network]`

Now your changes will be maintained through a reload of the LX unit.

TACACS+ Authentication and Accounting

This release of the LX software supports TACACS+ authentication and accounting.

TACACS+ is used to provide access control to devices such as network access server (NAS) or routers via a centralized server. It uses the Transport Control Protocol (TCP) on port 49 to ensure reliable transfer. The entire body of the packet is encrypted using a series of 16-byte MD5 hashes. The protocol is split up into 3 distinct categories; Authentication, Authorization, and Accounting.

Authentication is the process of determining who the user is. Usually, a user is required to enter in a user name and password to be granted access. Authorization is the process of determining what the user is able to do. The profile in the TACACS+ server should have a service of exec and a priv-lvl of 15 in order to access Superuser privileges, otherwise the user will only be allowed in user mode. The Accounting feature records what the user has done and generally occurs after authentication and authorization. There are three different types of accounting records: a start record for when a user logs on, an intermediate record, which is set with a constant interval, and a stop record when the user logs out.

The TACACS+ superuser request attribute is independent from the TACACS login.

The "**TACACS+ superuser request**" attribute is used to indicate which database to authenticate the superuser password against after a user is logged in. When you type the "enable" command, the enable password will be authenticated against the TACACS server database when the "**TACACS+ superuser request**" is enabled. Otherwise, it is checked against the LX database "system".

Sample TACACS+ Configuration

```
Login: InReach
Password: ******
InReach:0 >enable
Password: ******
InReach:0 >>configuration
Config:0 >>tacacs+ primary authentication server add 10.242.131.13
Config:0 >>tacacs+ primary authentication server secret jets
Config:0 >>tacacs+ primary account server add 10.242.131.13
Config:0 >>tacacs+ primary account server secret jets
Config:0 >>tacacs+ superuser password request enable
Config:0 >>tacacs+ secondary authentication server add 10.242.131.11
Config:0 >>tacacs+ secondary authentication server secret jets
Config:0 >>tacacs+ secondary account server add 10.242.131.11
Config:0 >>tacacs+ secondary account server secret jets
Config:0 >>tacacs+ superuser request enable

Config:0 >>port async 2
Async 2-2:0 >>access local
Async 2-2:0 >>authentication inbound tacacs+ enable
Async 2-2:0 >>tacacs+ account enable
Async 2-2:0 >>authentication fallback enable
Async 2-2:0 >>exit

Config:0 >>port async 3
Async 3-3:0 >>access remote
Async 3-3:0 >>authentication outbound tacacs+ enable
Async 3-3:0 >>tacacs+ account enable
Async 3-3:0 >>authentication fallback enable
Async 3-3:0 >>end
```

Viewing TACACS+ Characteristics

Use the following command to display the TACACS+ characteristics.

InReach:0>> show tacacs+ characteristics

```
Primary TACACS+ Authentication Server:
IP Address:              10.242.131.13  TACACS+ Auth. TCP Port:           49
Secret:                     Configured  Timeout:                           5
Retry:                               3
Secondary TACACS+ Authentication Server:
IP Address:              10.242.131.11  TACACS+ Auth. TCP Port:           49
Secret:                     Configured  Timeout:                           5
Retry:                               3
Primary TACACS+ Accounting Server:
IP Address:              10.242.131.13  TACACS+ Acct. TCP Port:           49
Secret:                     Configured  Timeout:                           5
Retry:                               3
Secondary TACACS+ Accounting Server:
IP Address:              10.242.131.11  TACACS+ Acct. TCP Port:           49
Secret:                     Configured  Timeout:                           5
Retry:                               3
TACACS+ Superuser Request:    Disabled
TACACS+ Accounting Server Period:    5
Inbound TACACS+ Enabled Serial Ports: 2
Outbound TACACS+ Enabled Serial Ports: 3
TACACS+ Enabled Interfaces:
```

TACACS+ Characteristics Display

Viewing TACACS+ Status

Use the following command to display the TACACS+ status.

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

```
Total TACACS+ Authentication Message Exchange:      Primary     Secondary
   Successful attempts:                                  0             0
   Failed attempts:                                      0             0

Total TACACS+ Accounting Message Exchange:          Primary     Secondary

   Successful attempts:                                  0             0
   Failed attempts:                                      0             0

TACACS+ Authentication Counter Summary:             Primary     Secondary

   Successful Logins:                                    0             0
   Authentication Failures:                              0             0

TACACS+ Accounting Counter Summary:                 Primary     Secondary

   Successful Acct Entries:                              0             0
   Failed Acct Entries:                                  0             0

TACACS+ Superuser Enable Summary:                   Primary     Secondary

   Successful Enable Requests:                           0             0
   Failed Enable Requests:                               0             0

TACACS+ Fallback Counter Summary:
    Total Fallback Logins:                            0
```

TACACS+ Status Display

For more information on the LX implementation of TACACS+ authentication and accounting, refer to the following sections in the *LX-Series Configuration Guide*:

- "Setting Up RADIUS, SecurID, and TACACS+ for the LX Unit"
- "Configuring RADIUS, TACACS+, or SecurID Authentication on an IP Interface"
- "Setting Up Security for a Console Port"

For more information on the commands, refer to the *LX-Series Commands Reference Guide.*

Telnet Performance

Telnet performance has been improved by fine-tuning the buffering to maximize the throughput and lower the latency.

Telnet Break String

This LX feature is used when telnet clients cannot send a telnet break to a remote device. The LX administrator can configure an LX console port with a unique "telnet break string" up to four characters long. During a telnet session, when the remote telnet partner includes the LX port's telnet break string within the data stream, the LX recognizes the character sequence and sends a break signal out of the configured LX console port to the attached device.

The telnet break string is configured in the Asynchronous mode. The command is in the following format:

```
Port Async 1:0>> telnet break string "string"
```

where "string" can be up to four characters long.

Ethernet Port Enhancement

Use this feature to configure the speed and duplex mode for the Ethernet Port. This enhancement is configured in the Ethernet Command mode or in the ppciboot Main menu. Set the Ethernet port to auto if you want the port to automatically adjust to network speed and duplex. You can also set the speed and duplex manually to 10mb with full or half duplex, or to 100mb with full or half duplex.

If the LX boots from flash memory, you can auto negotiate or fix the Ethernet port speed and duplex for normal functionality. Refer to the *LX-Series Commands Reference Guide* for more information on using the following commands in the Ethernet Command mode:

- `port ethernet 1`
- `speed auto`
- `speed 10mb duplex full`
- `speed 10mb duplex half`
- `speed 100mb duplex full`
- `speed 100mb duplex half`

Refer to the "Ethernet Commands" chapter of the *LX-Series Commands Reference Guide* for more information on using the speed command to set the speed and duplex mode of the Ethernet port.

If the LX boots from the network, use the following commands to set the Ethernet port speed and duplex. Refer to the *LX-Series Commands Reference Guide* for more information on the commands:

- `ppciboot ethernet link auto`
- `ppciboot ethernet link 10half`

- `ppciboot ethernet link 10full`
- `ppciboot ethernet link 100half`
- `ppciboot ethernet link 100full`

Refer to the "Configuration Commands" chapter of the *LX-Series Commands Reference Guide* for information on using the `ppciboot ethernet network link` command to set the port speed and duplex mode of the ppciboot Ethernet link.

Broadcast Group Enhancement

Broadcast Groups now supports up to 16 TCP sockets as slave ports. Previously, the limit was two.

Authentication Fallback Enable Command

The port command `radius fallback enable` has been changed to `authentication fallback enable`. Refer to the *LX-Series Commands Reference Guide* for more information.

MIB-Related RFCs

This release of the LX software supports the following MIB-related RFCs:

- **RFC 1213** – Defines the second version of the Management Information Base (MIB-II).
- **RFC 1471** – Defines Managed Objects for the Link Control Protocol of PPP.
- **RFC 1472** – Defines managed objects for PPP Security protocols.
- **RFC 1473** – Defines Managed Objects for the IP Network Control Protocol of the Point-to-Point Protocol.
- **RFC 1658** – Defines objects for the management of character stream devices.
- **RFC 1659** – Defines objects for the management of RS-232-like devices.
- **RFC 1696** – Describes managed objects used for managing dial-up modems and similar dial-up devices.
- **RFC 1907** – Defines managed objects for SNMP V2.
- **RFC 2574** – Defines the user-based security model for SNMP V3.
- **RFC 2575** – Defines the view-based Access Control Model for SNMP V3.

Upgrading Software and ppciboot with the Command Line Interface

You can upgrade the software and ppciboot using the update command in the superuser command mode. Make sure you have a TFTP server up and running, containing the software image and the ppciboot image.

NOTE: You must enter the TFTP server address each time you update software or ppciboot, unless you have already manually entered it in ppciboot.

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

1. Type the following and press <Enter>:

   `In-Reach:0>>update ppciboot` *`tftp_server_ip_address/name`*

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

2. Type the following and press <Enter>:

   `In-Reach:0>>update software` *`tftp_server_ip_address/name`*

   Updating software can take up to five minutes. You are copying from the TFTP server to the flash.

3. Type the following and press <Enter>:

   `In-Reach:0>>save config flash`

   This stores the parameters.

4. Type the following and press <Enter>:

   `In-Reach:0>>reload`

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

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

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

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

LX Series Notes and Restrictions

SSH Public Key

You cannot paste the SSH Public Key into the LX GUI window. Use the CLI to import the SSH Public Key.

CPU Usage Field

The `CPU Usage` field in the System Status screen is inaccurate.

Global Feature Control

When you use global features control via the GUI, the results are unreliable. To avoid this, disable the LX global features through the CLI.

Rebooting Outlet Groups

If an outlet in a group is not present or reachable when you reboot the outlet group, the reboot fails and the command is not applied. To avoid this, remove the missing outlet from the group name.

GUI Outlet Wake-Up State for IR-5150

The Wake-Up State does not exist on the GUI. Use the native CLI on the IR-5150 Power Control Series unit to control the outlet Wake-Up State.

`no outlet 1 name` Command

You must add a space after the word "`name`" in the async command `no outlet 1 name` for the command to work.

Menu Item Label

In the Menu Item Label, you cannot enter a standalone letter "t" or the word "to".

Menu Control Key

The Menu Control Key fails if the control letter is a lower case `t`, `r`, `e`, `l`, `s`, or `u`.

Changing Notification Message Priority

When you change a notification message's priority, sigsnotice is not a valid argument.

Async Port Pattern Matching

When you configure an async port pattern matching string, the alpha string "help" is not supported. "Help" is a reserved text string.

IP Interfaces

Previously, the LX allowed 15 IP interfaces. IP interfaces are now limited to four.

PCMCIA Port

The PCMCIA port on the front panel of the LX-4048 is inactive in this release.

Outlet Groups

You can configure a maximum of 16 outlet groups. However, when you attempt to create an outlet group via the CLI, there is not enough room to enter all 16, especially if you use long names or multiple digits. This occurs because the maximum number of characters on a CLI line is limited to 80. However, you can enter all 16 outlet groups via the GUI.

At the GUI window, do the following:

1. Select **Ports: Async**. The Async window opens.
2. Click on the **Group** button at the bottom of the window. The Group window opens.
3. Select the **New Group** tab. Configure the groups you want.

Known External Limitations

Java Cache Issue

The Java Cache in JRE 1.4 is set ON by default. There is an anomaly within Java Cache 1.4 regarding cache functionality, which requires you to disable the cache. At **Settings: Control Panel**, open the **Java Plug-in 1.4.0** icon, and click the **Cache** tab. At the Cache window, click the **Clear Cache** button and uncheck the **Enable Caching** checkbox. Click **OK**.

Windows 2000 Server

The Windows 2000 server does not support dialback.

Java Runtime Environment

The JRE used in the LX GUI does not support Macintosh operating systems.

Notification Web Driver Nextel, Skytel, and Sprint

The Web Drivers Nextel, Skytel, and Sprint are not supported because their sites use SSL.

Issues Fixed in 3.0.1

Configuring the IP Address

In Release 3.0, defining the IP address through the Quick Configuration menu did not work. You had to configure the IP address via the CLI. Upgrading to Release 3.0.1 resolves this issue.

Issues Fixed in 3.0.0

ppciboot Updates

In a previous release, when you ran the ppciboot update (Main Menu entry #6) over a routed network, the update failed. This feature now works properly.

Menu File Names

Previously, the command line parser had issues with underscores. You can now use underscores in menu file names.

Mail Commands in Multiple Packets

In a previous release, the LX sent the first character of a word in a packet by itself, then a second packet containing the rest of the word. SMTP mail commands are now sent intact in a single tcp packet.

Default Modem Command

In a previous release, you had to default the port and the modem if you wanted to default the modem. Now you can default the modem settings without defaulting the port.

Show Interface Port Mapping Screen

The Show interface X port mapping screen no longer includes port 0, because port 0 cannot be reached via telnet or ssh.

Modem Init String

Previously, if you set S registers (S0=1), the modem initstring did not accept the equal symbol (=). The equal symbol is now accepted.

Notification Service Profiles and User Profiles

Previously, if you created a notification serviceprofile or userprofile with a underscore in the name, you could not view the serviceprofile or userprofile by its name, even though it appeared in the all list. This no longer occurs.

3DES

Previously, the `3DES` command returned an error. Under subscriber/ssh/cipher, you can no longer enter `3DES`, but must enter `triple-DES` instead. The correct value of 3DES is displayed throughout all SHOW screens.

Config IP Network Number

Previously, if a unit's IP address was defined from the ppciboot Main menu, you could not change the network address to interface 1 when the unit was booted. You can now change the address.

LX Broadcast Address

In the previous release, when the unit was loaded and you changed the network address to the interface, the broadcast address was not adjusted properly. This no longer occurs.

SNMP Contact and Location

Previously, you could enter up to 256 characters for Contact and Location, but only the last 26 characters were displayed on the screen. The character limit is now 26.

V3 Client View Mask

Previously, when you tried to set the v3 client view mask by typing the `snmp:0>>v3 client 3 view mask 1.2.3.4` command, the following incorrect error message was displayed:

```
Non printable character a Call 7004.
```

Now the correct error message (`syntax error`) is displayed.

V3 View Mask Error Message

Previously, no error message was displayed when the `snmp>>v3 client 3 view mask jj22` command was executed with a value other than hex. Now, an error message is displayed.

10/100 Ethernet Port

Previously, you could not configure the 10/100 Ethernet port speed and duplex, but you can in this release.

TFTP Issue

Previously, TFTP caused a software update to fail if any timeouts were encountered. This no longer occurs.