CHAPTER 4

LightStream 2020 Set-up Procedures

This chapter describes set-up procedures that you may need to perform before activating your LS2020 switch in the network. These set-up procedures include the following tasks:

- Enabling/disabling secure single-user mode
- Creating new user accounts
- Changing default SNMP community names
- Changing default trap delivery addresses
- Changing default terminal type
- Editing the */usr/etc/hosts* file

After completing the initial installation of LS2020 hardware and software, as described in the "Installing StreamView Software" chapter, you may need to perform some or all of the set-up procedures described in this chapter, depending on your particular network operating requirements. Hence, you should review these procedures to determine which ones apply to your network.

Some set-up procedures call for you to signal the master management agent (MMA) to re-read configuration data for the affected LS2020 switch. Note, however, that you can perform any or all of the procedures in this chapter without sending interim restart signals to the MMA. Thus, after completing the last of the set-up procedures you intend to perform, you need only signal the MMA once to place all the set-up procedures into effect.

Enabling/Disabling Secure Single-User Mode

The purpose of the secure single-user mode is to prevent unauthorized superuser access to the NP of your LS2020 switch.

To enable or disable this feature, perform the following steps at the LS2020 console:

Step 1 Log onto the active NP as root.

Step 2 Back up the */etc/starttab* file, using the copy command:

```
cp /etc/starttab /etc/starttab.bak
```

Step 3 Invoke the vi editor to open the */etc/starttab* file:

```
vi /etc/starttab
```

Step 4 Look for the following comment line in the */etc/starttab* file:

```
#Name of single_user shell
```

- To enable secure single-user mode, change the line following this comment line to read as follows:

  ```
  /bin/single-user_login
  ```

- To disable secure single-user mode, change the line following this comment line to read as follows:

  ```
  /bin/bash
  ```

By default, single-user mode is disabled in the LS2020 system distribution software. Thus, whenever you upgrade to a new software version using the distributed *system* diskette set, the default */etc/starttab* file is written to the LS2020 hard disk. Consequently, if you wish to activate this feature after installing new platform software, you must enable it as described above.

To restore multi-user mode operation after running in the secure single-user mode, you must log out (by entering [^**D**], for example). The NP then comes up in multi-user mode after the following sequence of events:

1. The fsck program runs a check on all file systems.
2. The following prompt appears, at which you enter "**y**".

   ```
   Mount all filesystems (y/n) [y]
   ```

3. The NP is activated and runs the LS2020 platform (chassis) software.

Creating New User Accounts

This section describes how to create a new user account. The LS2020 switch provides an *adduser* script to simplify the task of adding a new user account to your system.

To create a new user account, perform the following steps:

Step 1 Log in to the root account on your LS2020 switch to bring up the bash# prompt.

Step 2 Start the *adduser* script by entering the following at the prompt:

```
bash# adduser
```

Step 3 Enter the login name for the new user account at the following prompt:

```
Enter login name, must be <= 8 characters:
```

Step 4 Enter the full name for the new user account at the following prompt:

```
Enter user's full name:
```

The system then displays the login account information shown below:

```
Login Name:       <login>
User ID:          <UID>
Home Directory:   /usr/<login>
Password Entry:   <login>::<UID>:<GID>:<username>:/usr/
<login>:          /bin/bash
```

where:

`<login>` is the login name of the user.

`<UID>` is the user identification number.

`<GID>` is the group identification number.

`<username>` is the full name of the user.

Step 5 If the information displayed in Step 4 is correct, respond yes (**Y**) to the following prompt:

```
Add the new user to the password database (Y/N)? [Y]
```

Step 6 Enter a password for the new user at the following prompt:

```
Adding entry to the /etc/passwd database
Making /usr/<login> home directory
Changing password for <login>
Enter new password:
```

The password must be unique and at least six alphanumeric characters in length.

Step 7 Re-enter the password at the prompt for confirmation:

```
Retype new password:
```

If you entered the new password correctly, the system changes the existing password and displays the following prompt:

```
bash#
```

As a result of this procedure, a new user account is created with the attributes you specified. You can then log in to the new user account and begin using it.

Changing Default SNMP Community Names

Each LS2020 switch has a file detailing the privileges for each switch in the network that has *read* or *read/write* access to its MMA. To monitor the network, you need to have only read access privileges to the MMA; however, to make changes to MMA values or to issue control commands, you need to have read/write access privileges to the MMA.

LS2020 software maps the SNMP community name and IP address of each LS2020 switch to a set of privileges. Each switch has a default file named */usr/app/base/config/mma.communities* that contains details about the SNMP communities and access privileges defined for the switch. Figure 4-1 is an example of such a file. The lines in this example file preceded by the number sign (#) are informational comments; the last three lines of this file show the names of the defined SNMP communities (*public*, *trap*, and *write*).

Figure 4-1 Sample mma.communities File

```
bash# more mma.communities
# This is the session configuration file that determines who may
# access the gateway. Each line consists of three items:
# 1st, the session name.
# 2nd, the IP address of the remote site. If address is 0.0.0.0, any
# address may communicate on that session name.
# 3rd, the privileges given that session name. These currently
# consist of READ for read only, WRITE for read/write, or NONE to
# lock out a session name.
# The format is
# session_name IP_address_in_dot_notation privileges
public 0.0.0.0 read
trap 127.0.0.1 write
write 0.0.0.0 write
bash#
```

H3693

The line *public 0.0.0.0 read* indicates that a user issuing commands from any IP address (that is, IP address 0.0.0.0) who has set the SNMP community name to *public* has read access privileges to the MMA for this switch.

The line *trap 127.0.0.1 write* indicates that a user issuing commands from this local switch (that is, IP address `127.0.0.1`) who has set the SNMP community name to *trap* has read/write access privileges to the MMA for this switch.

The line *write 0.0.0.0 write* indicates that a user issuing commands from any IP address (that is, IP address `0.0.0.0`) who has set the SNMP community name to *write* has read/write access privileges to the MMA for this switch.

Note that SNMP community names can be used to provide a level of security for each LS2020 switch in the network. For this reason, it is advisable to change the names of the *trap* and *write* SNMP communities to names of your choosing. By so doing, you can restrict access to your LS2020 switch to only those users who know your SNMP community name(s).

As a convention, most SNMP devices have a *public* community name with read-only access privileges. You should not change this name, but you can change its associated privileges, if necessary.

Note The SNMP community name is set to *public* whenever you invoke the CLI. You can change this setting by issuing the `set snmp community <community_name>` command at the CLI prompt.

Note The procedure for upgrading a chassis to a new software release has a mechanism for preserving local changes to files, such as *mma.communities*, during the upgrade process. Therefore, the procedure below for changing the default SNMP community name(s) in the *mma.communities* file must be performed **exactly** as described to ensure that changes to this locally-modified file are copied forward into the new software release. The upgrade mechanism copies "regular files" forward into the new release, but not "symbolic links." Thus, the upgrade procedure ensures that the locally-modified *mma.communities* file will be changed from a "symbolic link" into a "regular file" for purposes of the software upgrade.

To change the default SNMP community name or the MMA read/write access privileges for your LS2020 switch, edit the file *mma.communities* according to the following procedure:

Step 1 Log in to the root account on your LS2020 switch.

Step 2 Change to the directory containing the files you want to edit by entering the following command:

```
bash# cd /usr/app/base/config
```

Step 3 Move the *mma.communities* file to a file renamed *mma.communities.orig* to maintain the symbolic link between the two files, as shown below:

```
bash# mv mma.communities mma.communities.orig
```

The *mma.communities.orig* file now points to the */usr/app/dist/base-x.x.x/config/mma.communities* file

where:

base-x.x.x is the current version of LS2020 software.

Step 4 Copy the contents of the linked *mma.communities.orig* file to a new file named *mma.communities* by entering the following command:

```
bash# cp mma.communities.orig mma.communities
```

As a consequence of Steps 3 and 4, you now have two *mma.communities* files, each containing identical information. Note, however, that the copy operation does not carry the symbolic link forward into the new, renamed *mma.communities* file. Thus, the resulting *mma.communities* file is not linked to any other files, while the *mma.communities.orig* file remains linked to the current */usr/app/dist/base-x.x.x/config/mma.communities* file.

The rationale for creating a new *mma.communities* file for the LS2020 switch in the manner described above is twofold:

- To preserve your current LS2020 operational settings for use in the next LS2020 software upgrade. For example, if you have defined a customized *mma.communities* file (containing desired SNMP communities, IP addresses, and so forth) and you do not want this file to be overwritten at the next upgrade, you can break the symbolic link, as described above. Breaking the link causes these current settings to be carried forward into the upgraded LS2020 configuration.
- To provide a backup file in the event that the original *mma.communities* file becomes corrupted for some reason and must be replaced.

Step 5 Invoke the vi editor to revise the *mma.communities* file by entering the following command:

```
bash# vi mma.communities
```

Change the *mma.communities* file to reflect your desires for SNMP community names.

If you are not familiar with the vi editor, refer to the *LightStream 2020 NP O/S Reference Manual* for additional information.

Step 6 Save the changes to the edited *mma.communities* file and exit the vi editor by entering the following:

```
ZZ
```

Step 7 Use either of the following methods to cause the MMA to re-read the *mma.communities* file:

- From the bash# prompt, determine the process ID (PID) number of the MMA by entering the following:

  ```
  bash# ps -ax
  ```

  This command lists all the processes running on your LS2020 switch.

  After determining the PID number for the MMA, enter the following to cause the MMA to re-read the *mma.communities* file:

  ```
  bash# kill -hup <mma pid #>
  ```

  where:

  `<mma pid #>` is the PID number determined above for the MMA process in this LS2020 switch.

- From the CLI prompt, determine the PID number of the MMA by entering the following command:

  ```
  cli> walk pidName
  ```

  Change to the protected mode of the CLI prompt by entering the following:

  ```
  cli> protected
  ```

  Enter the protected mode password at the prompt:

  ```
  Enter password:
  ```

  The CLI protected mode prompt then appears (signified by `*cli>`), at which you enter the following command to cause the MMA to re-read the *mma.communities* file:

  ```
  *cli> shell “kill -hup <mma pid #>”
  ```

Step 8 If you wish to verify your changes to the *mma.communities* file, enter the following at the protected mode CLI prompt:

```
*cli> shell "more /usr/app/base/config/mma.communities"
```

This command displays the *mma.communities* file for inspection.

If you wish to exit the protected mode CLI at this juncture, issue the following command:

```
*cli> quit
```

Step 9 Repeat Steps 2 through 8 for each LS2020 switch in the network whose default SNMP community name or read/write access privileges you wish to change.

At the conclusion of this procedure, you have defined one or more new SNMP community names for one or more LS2020 switches to reflect your particular network operating requirements.

Changing Trap Delivery Addresses

When you start the CLI, the LS2020 switch finds the addresses for trap delivery in the */usr/app/base/config/mma.trap_communities* file. By default, LS2020 switches send traps only to their local network processor (NP) card. However, by editing the *mma.trap_communities* file, you can cause traps to be sent to as many as 25 different destinations. Similarly, by editing this file, you can also cause traps for all LS2020 switches in the network to be sent to the same device.

For additional information about trap-handling mechanisms, refer to the *LightStream 2020 Traps Reference Manual.*

This section tells you how to edit the *mma.trap_communities* file. Before proceeding, however, note that each line in the *mma.trap_communities* file consists of three elements:

- The community name
- The IP address for trap delivery
- The user datagram protocol (UDP) port on which traps are to be sent. Normally, the SNMP protocol uses UDP port 162 for trap delivery.

Figure 4-2 shows a sample *mma.trap_communities* file. Note that the first entry in each line is the community name (*trap*); the second entry is an IP address (the default IP address, the NP IP address, the NMS IP address, or the IP address of a destination device); the third entry (162) identifies the UDP port number for delivering traps.

Figure 4-2 Sample mma.trap_communities File

```
trap 127.0.0.1 162           (Default entry)
trap <NP IP address> 162     (Entry sending traps to a different NP)
trap <NMS IP address> 162    (Entry sending traps to an NMS)
trap <device IP address> 162 (Entry sending traps to a destination device)
```

H3694

Note The procedure for upgrading a chassis to a new software release has a mechanism for preserving local changes to files, such as *mma.trap_communities*, during the upgrade process. Therefore, the procedure below for changing trap delivery addresses in the *mma.trap_communities* file must be performed **exactly** as described to ensure that changes to this locally-modified file are copied forward into the new software release. The upgrade mechanism copies "regular files" forward into the new release, but not "symbolic links." Thus, the upgrade procedure ensures that the locally-modified *mma.trap_communities* file will be changed from a "symbolic link" into a "regular file" for purposes of the platform software upgrade.

To change the trap delivery IP address(es) for an LS2020 switch, edit the file *mma.trap_communities* according to the following procedure:

Step 1 Determine the IP addresses where you want traps to be sent (any one or more of up to 25 different IP address, including another NP, an NMS, or a designated destination device).

Step 2 Log in to the root account on your LS2020 switch.

Step 3 Change to the directory containing the *mma.trap_communities* file you want to edit by entering the following command:

```
bash# cd /usr/app/base/config
```

Step 4 Move the *mma.trap_communities* file to a file renamed *mma.trap_communities.orig* to maintain the symbolic link between the two files, as shown below:

```
bash# mv mma.trap_communities mma.trap_communities.orig
```

The *mma.trap_communities.orig* file now points to the */usr/app/dist/base-x.x.x/config/mma.trap_cummunities*

where:

base-x.x.x is the current version of LS2020 software.

Step 5 Copy the contents of the now linked *mma.trap_communities.orig* file to a new file named *mma.trap_communities* by entering the following command:

```
bash# cp mma.trap_communities.orig mma.trap_communities
```

As a consequence of Steps 4 and 5, you now have two *mma.trap_communities* files, each containing identical information. Note, however, that the copy operation does not carry the symbolic link forward into the new, renamed *mma.trap_communities* file. Thus, the resulting *mma.trap_communities* file is not linked to any other files, while the *mma.trap_communities.orig* file remains linked to the current operational */usr/app/dist/base-x.x.x/config/mma.trap_communities* file for your LS2020 switch.

The rationale for creating a new *mma.trap_communities* file in the manner described above is twofold:

- To preserve your current LS2020 trap settings for use in the next LS2020 software upgrade. For example, if you have defined a customized *mma.trap_communities* file (with desired trap IP addresses) and you do not want that file to be overwritten at the next upgrade, you can break the symbolic link, as described above, causing the current trap settings to be carried forward into the upgraded LS2020 configuration.
- To provide a backup file in the event that the original *mma.trap_communities* file becomes corrupted for some reason and must be replaced.

Step 6 Invoke the vi editor to edit the *mma.trap_communities* file by entering the following command:

```
bash# vi mma.trap_communities
```

Change the *mma.trap_communities* file to reflect your desires for LS2020 trap delivery. Do this by defining the community name (*trap*), the IP address for trap delivery (to another NP, an NMS, or a destination device), and the UDP port number through which the SNMP protocol will send traps from your LS2020 switch.

If you are not familiar with the vi editor, refer to the *LightStream 2020 NP O/S Reference Manual* for additional information.

Step 7 Save the changes to the mma.trap_communities file and exit the vi editor by entering the following:

```
ZZ
```

Step 8 Use either of the following methods to cause the MMA to re-read the *mma.trap_communities* file:

- From the bash# prompt, determine the process ID (PID) number of the MMA by entering the following:

  ```
  bash# ps -ax
  ```

  This command lists all the processes running on the LS2020 switch.

After determining the PID number for the MMA, enter the following to cause the MMA to re-read the *mma.trap_communities* file:

```
bash# kill -hup <mma pid #>
```

where:

`<mma pid #>` is the PID number determined above for the MMA process in the LS2020 switch.

- From the CLI prompt, determine the PID number of the MMA by entering the following command:

  ```
  cli> walk pidName
  ```

  Change to the protected mode of the CLI prompt by entering the following:

  ```
  cli> protected
  ```

  Enter the protected mode password at the prompt:

  ```
  Enter password:
  ```

  The CLI protected mode prompt then appears (signified by `*cli>`), at which you enter the following command to cause the MMA to re-read the *mma.trap_communities* file:

  ```
  *cli> shell “kill -hup <mma pid #>”
  ```

Step 9 If you wish to verify your changes to the *mma.trap_communities* file, enter the following at the protected mode CLI prompt to examine the contents of the file:

```
*cli> shell ”more /usr/app/base/config/mma.trap_communities"
```

If you wish to exit the protected mode CLI at this point, issue the following command:

```
*cli> quit
```

Step 10 Repeat Steps 3 through 9 for each LS2020 switch in the network whose trap delivery IP address(es) you wish to change.

At the conclusion of the above procedure, traps will be sent to the IP address(es) specified in the revised *mma.trap_communities* file.

Changing Default Terminal Type

Whenever you log in to the CLI, the default terminal type of each user account (oper, npadmin, fldsup, and root) is set to *vt100*. If you do not use a VT100 terminal, you may change the default terminal type in your *.profile* file to preclude having to change the *vt100* setting at each log in. The procedures described in this section enable you to change the default terminal type in the *.profile* file for each LS2020 user account. You can change the default terminal type from either the bash# prompt or the CLI prompt, as described in the following sections.

Changing Default Terminal Type from Bash# Prompt

To change the default terminal type from the bash# prompt, perform the following steps:

Step 1 Verify that the terminal type you want to use is defined in the */etc/termcap* file.

Step 2 Log in to the fldsup account or the root account for the LS2020 switch whose default terminal type you wish to change.

Step 3 Edit the terminal type for the oper account by entering the following:

```
bash# vi /usr/oper/.profile
```

The vi editor opens, enabling you to edit the *.profile* file.

Step 4 Change the default terminal type for the oper account by editing the line that reads:

```
TERM=vt100
```

You should change this line to reflect the terminal type that you intend to use. (The terminal type you enter must be defined in the */etc/termcap* file.)

If the line TERM=vt100 does not appear in the *.profile* file, add this line to the file in the following format:

```
TERM=<your default terminal type>
```

Step 5 Save your changes to the *.profile* file and exit from the vi editor by entering the following:

```
ZZ
```

Step 6 Repeat Steps 3 through 5 for each remaining LS2020 login account (npadmin, fldsup, and root) by editing the following files, as appropriate:

```
/usr/npadmin/.profile
/usr/fldsup/.profile
/usr/root/.profile
```

Step 7 Repeat this procedure for any other user accounts that you may have created, in addition to the four user accounts referenced above (oper, npadmin, fldsup, and root).

Note that the new terminal type does not take effect until you log in again.

Changing Default Terminal Type from CLI Prompt

To change the default terminal type from the CLI prompt, perform the following steps:

Step 1 Verify that the terminal type you want to use is defined in the */etc/termcap* file.

Step 2 Enter the following at the `CLI` prompt:

```
cli> protected
```

This action yields the “protected” mode of the CLI (signified by `*cli>`), at which you enter the protected mode password:

```
*cli> <password>
```

Step 3 Open the *oper* account by entering the following:

```
*cli> shell ”vi /usr/oper/.profile”
```

The vi editor opens, enabling you to edit the *.profile* file.

Step 4 Change the default terminal type for the oper account by editing the line that reads:

```
TERM=vt100
```

You should change the line to reflect the terminal type you intend to use. (The terminal type you enter must be defined in the */etc/termcap* file.)

If the line `TERM=vt100` does not appear in the *.profile* file, add this line to the file in the following format:

```
TERM=<your default terminal type>
```

Step 5 Save your changes to the *.profile* file and exit from the vi editor by entering the following:

```
ZZ
```

Step 6 Repeat Steps 3 through 5 for each remaining LS2020 login account (npadmin, fldsup, and root) by editing the following files, as appropriate:

```
/usr/npadmin/.profile
/usr/fldsup/.profile
/usr/root/.profile
```

Step 7 Repeat this procedure for any other user accounts that you may have created, in addition to the four user accounts referenced above (oper, npadmin, fldsup, and root).

The new terminal type for the LS2020 switch does not take effect until you log out and log in again.

Editing the Hosts File

As the network administrator, you must maintain the */usr/etc/hosts* file for each network processor (NP) in your network. This file, which serves as a repository for the names and IP addresses of all network processors in the network, is created at installation time, but you must ensure that an entry exists in this file for each network processor in, or being added to, your network. Figure 4-3 shows typical content in a */usr/etc/hosts* file.

Figure 4-3 Sample /usr/etc/hosts File

```
127.1.22.41  Light1
127.1.22.42  Light2
127.1.22.43  Light3
127.1.22.46  Light6
127.0.0.1    localhost
```

H3695

To edit the */usr/etc/hosts* file, perform the following steps:

Step 1 Log in to the LS2020 switch as root.

Step 2 At the `bash#` prompt, change to the */usr/etc* directory by entering the following command:

```
bash# cd /usr/etc
```

Step 3 Enter the following command to open the *hosts* file for editing with the vi editor:

```
bash# vi hosts
```

If you are unfamiliar with the vi editor, refer to the *LightStream 2020 NP O/S Reference Manual* for additional information.

Step 4 Append to the end of the *hosts* file the names and IP addresses of the network processors being added to your network. Use the format shown in Figure 4-3 in making these entries.

Step 5 Save your changes to the `hosts` file and exit the vi editor by entering the following:

zz

This action returns you to the `bash#` prompt.

Editing of the */usr/etc/hosts* file is now complete.

Caution The */usr/etc/hosts* file on each LS2020 network processor contains chassis-specific information that is entered automatically and modified each time the LS2020 switch is booted. Therefore, do not copy the */usr/etc/hosts* file from one LS2020 switch or network processor to another such device in your network.