Oracle® Communications

LSMS Configuration Guide

Release 13.5
F42041-06
January 2022

ORACLE

Oracle Communications LSMS Configuration Guide, Release 13.5

F42041-06

Contents

3 Completing Configuration and Starting Connections

A Configuring the Query Server

My Oracle Support (MOS)

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support can assist you with My Oracle Support registration.

Call the Customer Access Support main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

- For Technical issues such as creating a new Service Request (SR), select **1**.
- For Non-technical issues such as registration or assistance with My Oracle Support, select **2**.
- For Hardware, Networking and Solaris Operating System Support, select **3**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

What's New in This Guide

This section introduces the documentation updates in Oracle Communications Local Service Management System (LSMS) for Release 13.5.

Bug 33748695 - January 2022

- Added additional capacities in LSMS. See Configure/Update LSMS Quantity Keys.

1 Introduction

This manual contains information you need to configure the **LSMS**. Topics include integrating **LSMS** into your network, configuring and starting connections with **NPACs** and network elements, and configuring optional features.

Overview

This manual contains information you need to configure the **LSMS**. Topics include integrating **LSMS** into your network, configuring and starting connections with **NPACs** and network elements, and configuring optional features.

Scope and Audience

This manual is written for system administrators and persons responsible for configuring the **LSMS**. The manual provides routine operating procedures and guidance in the tasks of integrating the platform with the network and configuring and starting up **LSMS** and connections.

The manual assumes the system administrator is familiar with the Linux operating system.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1-1 Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Manual Organization

The manual contains the following chapters:

- Introduction contains general information about the organization of the manual, description of the **LSMS** document suite, and a list of acronyms and abbreviations.
- Integrating EAGLE Application B Card (E5-APP-B) into the LSMS Network provides guidance for integrating an Oracle Communications EAGLE Application B Card (E5-APP-B) **LSMS** into your internal and external local area network or wide area network.
- Completing Configuration and Starting Connections describes how to configure components, use key lists, and work with **NPAC** associations.
- Configuring the NAS explains how to configure the Oracle Communications LSMS Network Attached Storage (NAS).
- Configuring Optional Features explains how to configure the various optional features.
- Configuring the Query Server provides overview information as well as detailed, step-by-step configuration procedures to get the query server up-and-running.

My Oracle Support (MOS)

MOS (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request
2. Select 3 for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select 1
   - For Non-technical issues such as registration or assistance with MOS, Select 2

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides

immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Related Publications

For information about additional publications related to this document, refer to the Oracle Help Center site. See Locate Product Documentation on the Oracle Help Center Site for more information on related product publications.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click `Industries`.
3. Under the Oracle Communications subheading, click the `Oracle Communications documentation` link.

   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then the Release Number.

   A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the `PDF` link, select `Save target as` (or similar command based on your browser), and save to a local folder.

Using Login Sessions

Login sessions are used for the following user functions:

- To use the command line for any of the following functions:
  - To access the `lsmsmgr` text interface, which is used for configuring and maintaining the **LSMS** system.
  - To enter **LSMS** commands (generally used for managing **LSMS** applications). For more information, refer to appendices in *Alarms and Maintenance Guide*.
  - To start the optional Command Line Administration Capability feature (the `lsmsclaa` utility); for more information, see Command Line Interface Utility.

> **Note:**
>
> For procedures on logging in to sessions, see "Using Login Sessions" in the *Alarms and Maintenance Guide*.

Support of Multiple Users

The **LSMS** allows, as a standard feature, a maximum of eight simultaneous users. The Support for Additional Users optional feature enables you to have a maximum of 25 simultaneous users. A user is defined to be any of the following:

- `lsmsmgr` user (a user who logs in as the `lsmsmgr` user to start the `lsmsmgr` text interface).
- Server-side **GUI** user (a user who has logged into the command line of a server and started a **GUI** with the `start_mgui` command).
- **GUI** user (a user who has logged into the active server **GUI** over the web.
- `lsmsclaa` user (a user who is using the optional **LSMS Command Class** Management optional feature).

Establishing Login Sessions

From any network-connected terminal, you can establish a variety of sessions with the active server or with a specific server in one of the following ways:

- Display the `lsmsmgr` text interface of either the active server or of a specific server
- Display the command line of either the active server or a specific server for entering commands; see Logging In to LSMS Server Command Line.

  From the displayed command line, you can start a server-side **GUI**, as described in "Starting a Server-Side LSMS GUI Session" in *Alarms and Maintenance Guide*.

- Display the **GUI** by using a web browser; see "Starting an LSMS GUI Session" in *Alarms and Maintenance Guide*.

Logging In to LSMS Server Command Line

You can log in to the **LSMS** active server or in to a specific server from any terminal that has an **SSH** client installed.

> **Note:**
>
> If your terminal does not already have `ssh` installed, PuTTY (Oracle Communications does not make any representations or warranties about this product) is an open source `ssh` utility for Windows that you can download from the web.

You must have a user **ID** and password before you can log in to **LSMS**.

1. From a command line prompt on any X-windows-compatible terminal, enter one of the following commands (depending on the terminal operating system) to start a secure shell session with the **LSMS** server:
   - On a Windows or Linux-based terminal, enter:
     `ssh -x <username>@<server_IP_address>`

     For **<username>** and **<server_IP_address>**, specify a value shown in the following table as appropriate to the procedure you are performing:

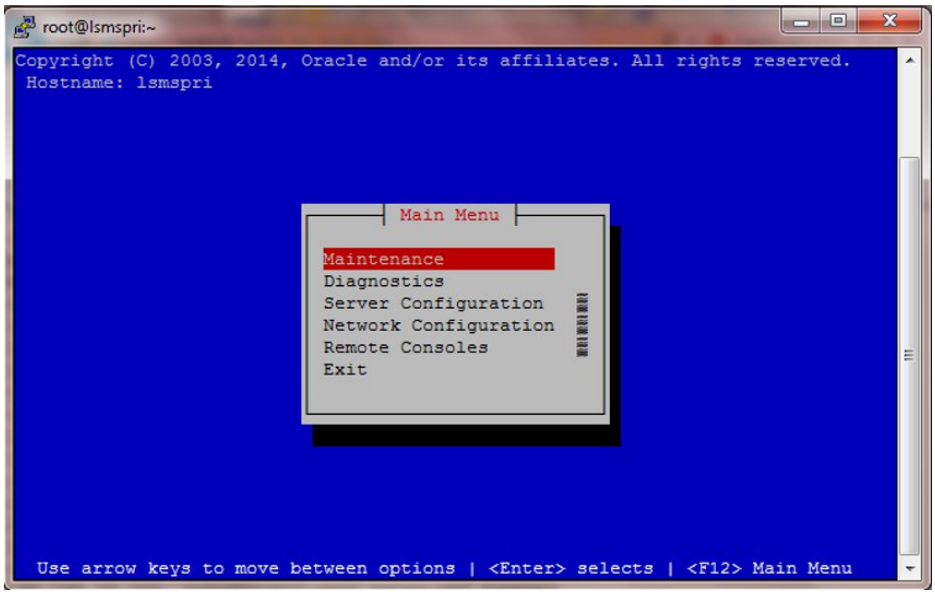
     Table 1-2 Parameters Used in Accessing Server Command Line

Parameter	Value
<username>	Use one of the following: – `lsmsmgr` to access the `lsmsmgr` text interface for configuration, diagnostics, and other maintenance functions – `syscheck` to run the `syscheck` command with no options, which returns overall health checks and then exits the login session (for more information about the `syscheck` command, refer to the *Alarms and Maintenance Guide*) – Other user names, as directed by a procedure
<server_IP_address>	Use one of the following: – **VIP** (Virtual **IP** address) to access the **LSMS** Web **GUI** – **IP** address of the specific server, when directed by a procedure to access a particular server

2. When prompted, enter the password associated with the user name.
3. You can now continue with any of the following functions:

- If you entered `lsmsmgr` as the username, the `lsmsmgr` text interface displays, as shown in the following Figure.
  You can use any of the `lsmsmgr` functions, described also in the *Alarms and Maintenance Guide*.

Figure 1-1 lsmsmgr Text Interface Main Menu



> **Note:**
>
> Selections in the `lsmsmgr` text interface are made either by using the Up and Down Arrow keys on your keyboard or by typing the first letter of your menu choice to change which menu item is highlighted. When the desired menu item is highlighted, press the Enter key.
>
> In this manual, menu selections are indicated as a series; for example, select Maintenance > Start Node indicates that you should highlight the Maintenance item on the main menu, press Enter, then highlight the Start Node item on the next menu, and press Enter again.

- If you entered `syscheck` as the username, the command line window displays the System Health Check output.
  For more information about `syscheck`, refer to the *Alarms and Maintenance Guide*.
- If you entered any other username the command line prompt displays a prompt that shows the username and host name, similar to the following example (in this example, the user logged in as the `lsmsadm` user to the server whose host name is `lsmspri`):

```
[lsmsadm@lsmspri lsmsadm]$
```

> **Note:**
>
> In this manual, the prompt will be indicated simply by $.

At this prompt, you can do any of the following:

- Enter **LSMS** commands.
- Start the `lsmsclaa` utility if you have the **LSMSCommand Class** Management optional feature installed.
- If you need to start an **LSMS** graphical user interface (**GUI**), see "Starting a Server-Side LSMS GUI Session" in the *Alarms and Maintenance Guide*.

You have now completed this procedure.

Logging in from One Server to the Mate's Command Line

Sometimes it may be necessary to have access to the command line interfaces for both servers. You can log into each server separately using `ssh`, or you can use `ssh` to go back and forth between servers.

To log in from one server's command line to the mate server's command line, use the following procedure:

1. Log in as any user except `lsmsmgr` or `syscheck`, using the procedure described in "Logging In to LSMS Server Command Line" to log into a server command line.
2. Enter the following command to access the command line on the mate server:

   ```
   ssh mate
   ```

   If you have not previously logged into the mate, the following information displays:

   ```
   The authenticity of host 'mate (192.168.1.1)' can't be established.
   RSA key fingerprint is 1c:14:0e:ea:13:c8:68:07:3d:7c:4d:71:b1:0c:33:04.
   Are you sure you want to continue connecting (yes/no)?
   ```

   Type `yes`, and press Enter.
3. When prompted, enter the password for the same user name.
4. The prompt on your terminal now displays the host name of the mate server, and you can enter commands for the mate server.

   Following is an example of the sequence of commands and prompts that display during this procedure:

   ```
   [lsmsadm@lsmspri lsmsadm]$ ssh mate
   lsmsadm@mate's password:
   [lsmsadm@lsmssec lsmsadm]$
   ```

You have now completed this procedure.

Inactivity Timeout

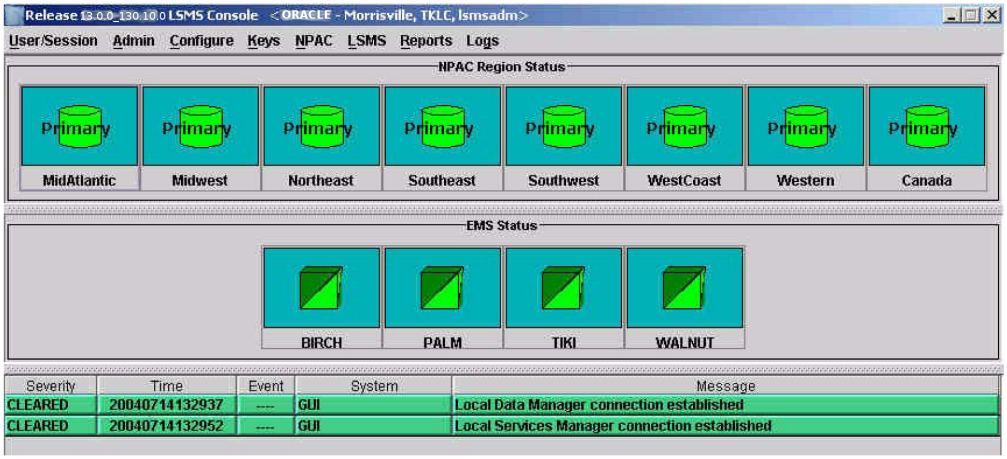
The Automatic Inactivity Logout (inactivity timeout) feature, when activated, logs out **LSMS GUI** and command line users after a preset period of inactivity occurs. For more information, refer to the topic “Inactivity Timeout Submenu”.

Modifying Title Bar in LSMS Console Window

After you successfully log in to **LSMS**, the console window appears. If the `/usr/TKLC/lsms/config/LSMSname` file exists and contains a (0–30 character) unique **LSMS** name, the name (in this example, “Oracle - Morrisville”) is displayed in the title bar along with the **SPID** and user name (see Figure 1-2).

If the `/usr/TKLC/lsms/config/LSMSname` file does not exist or is empty (null), no name is displayed and the title bar will display only the **SPID** and user name.

Figure 1-2 LSMS Console Window with Modified Title Bar



Command Line Interface Utility

To use the command line interface, use the following procedures to start and exit the command line interface utility.

Starting the Command Line Interface

You can use the command line interface utility, `lsmsclaa`, to manage some functions that can also be managed from the **LSMS** graphical user interface. Once the command line interface is running, you can enter as many of its allowed actions as are required to fulfill a task.

For detailed information about the using the command line interface utility, including error situations, refer to “Using lsmsclaa Commands” in Appendix A of *Alarms and Maintenance Guide*.

Use the following procedure to start the command line interface utility:

1. Use the procedure described in Logging In to LSMS Server Command Line to log in to the command line of the active server as a member of the permission group required for the function you need to perform.

   For more information about permission groups and authorized functions, and for more information about the command line interface, refer to “Using lsmsclaa Commands” in Appendix A of *Alarms and Maintenance Guide*.

2. Start the command line interface by entering the following command with parameters as defined in Table 1-3:

   ```
   $LSMS_DIR/ <SPID> <REGION> [<COMMANDFILE>]
   ```

   Table 1-3 Parameters Used by Command Line Interface

Parameter	Description	Required?	Characters
<**SPID**>	Service Provider **ID**	Yes	4
<**REGION**>	Name of **NPAC** region	Yes	6 to 11
<**COMMANDFILE**>	Full name of a text file that contains a series of commands to be run by the command line interface utility	No	1 to 256

3. The following prompt appears, at which you enter the action you desire:

   ```
   Enter command ->
   ```

You have now completed this procedure.

Exiting the Command Line Interface

Use the following procedure to exit the command line interface utility:

- Enter the following at the command line interface prompt:

  ```
  Enter Command -> EXIT
  ```

You have now completed this procedure.

GUI Function Access

Access to the various **LSMS GUI** functions is determined by the permission group assigned by the system administrator. For more information, refer to “Managing User Accounts” in *Alarms and Maintenance Guide*.

The following tables show the configuration functions each permission group can access. Inaccessible functions are deselected (grayed-out) on the actual menus.

- Table 1-4
- Table 1-5
- Table 1-6

For more about using the **GUI** menu items other than those shown in the tables listed above, refer to *Database Administrator's Guide*.

Table 1-4 Admin GUI Access by Permission Group

Admin GUI Functions	Admin GUI Access by Permission Group X = This GUI function is accessible to the indicated permission group.				
	Default Permission Groups				
	lsmsadm	lsmsuser	lsmsview	lsmsall	lsmsuext
Admin	X			X	
Users	X			X	
Modify	X			X	
View	X			X	
Permission Groups	X			X	
Create	X			X	
Modify	X			X	
View	X			X	
Delete	X			X	
Inactivity Timeout	X			X	
System Inactivity Timeout	X			X	
View	X			X	
Modify	X			X	
User Inactivity Timeout	X			X	
View	X			X	
Modify	X			X	
Password Timeout	X			X	
System Level	X			X	
View	X			X	
Modify	X			X	
User Level	X			X	
View	X			X	
Modify	X			X	
Alarm Filter	X			X	
MySQL port	X			X	
QS MySQL port	X			X	
LNP Threshold	X			X	

Table 1-5 Configure GUI Access by Permission Group

Configure GUI Functions	Configure GUI Access by Permission Group X = This GUI function is accessible to indicated permission group.				
	Default Permission Groups				
	lsmsadm	**lsmsuser**	**lsmsview**	**lsmsall**	**lsmsuext**
Configure	X	X	X	X	X
LNP System	X	X	X	X	X
NPAC	X	X	X	X	X
Modify	X			X	
View	X	X	X	X	X
LSMS	X	X	X	X	X
Modify	X			X	
View	X	X	X	X	X
EMS	X	X	X	X	X
Create	X			X	
Modify	X			X	
View	X	X	X	X	X
Delete	X			X	
Service Provider	X	X	X	X	
Create	X			X	
Modify	X			X	
View	X	X	X	X	
Delete	X			X	
TT/SSN Values	X			X	X [1]

[1] Users belonging to the **lsmsuext** permission group are authorized to access Default TT/**SSN values only for GTT groups assigned to the login SPID**.

Table 1-6 Keys GUI Access by Permission Group

Keys GUI Functions	Keys GUI Access by Permission Group X = This GUI function is accessible to the indicated permission group.				
	Default Permission Groups				
	lsmsadm	**lsmsuser**	**lsmsview**	**lsmsall**	**lsmsuext**
Keys	X			X	
NPAC	X			X	
LSMS	X			X	

The **OK**, **Apply** and **Cancel** buttons have specific GUI functions that are as follows:

- When there is a change in the data and **OK** is clicked:

  - GUI updates the value in the database
  - GUI displays a message that the update is successful
  - GUI closes the Menu/Window
- When there is no change in the existing data and **OK** is clicked:
  - GUI returns an error that there is nothing to update
  - GUI does not close the Menu/Window
- When there is no data entered and **OK** is clicked the GUI returns an error.
- When there is a change in the data and **Apply** is clicked:
  - GUI updates the value in the database
  - GUI displays a message that the update is successful
  - GUI does not close the Menu/Window
- When there is no change in the existing data and **Apply** is clicked:
  - GUI returns an error that there is nothing to update
  - GUI does not close the Menu/Window
- If **Cancel** is clicked the open Menu/Window is closed.

2

Integrating EAGLE Application B Card (E5-APP-B) into the LSMS Network

This chapter provides guidance for integrating the **LSMS** into your internal and external local area network (**LAN**) or wide area network (**WAN**).

Overview

This chapter provides guidance for integrating the **LSMS** into your internal and external local area network (**LAN**) or wide area network (**WAN**).

This chapter describes how to provide preliminary planning guidance, help you assemble the data for the **LSMS** Site Survey, and provide source material for installation and upgrade procedures.

Understanding the LSMS Network

LSMS provides a series of network connections to enable it to interact with **NPAC**s, **EMS**s, and local and remote consoles. The following sets of network connections can be made to your network:

- **E5-APP-B**

  LSMS blade server that is EAGLE Extension Shelf compatible.

- **NPAC**

  Depending on your network configuration, a Gigabit Ethernet interface typically connects to an external **WAN**. This interface provides connectivity to one or more remote **NPAC** sites. These connections are shown going to the **NPACWAN** in Figure 2-1.

- **EMS**

  Depending on your network configuration, a Gigabit Ethernet interface typically connects to your site's secure **WAN**. This interface provides connectivity to the customer's **EMS** (**EAGLE**) sites. These connections are shown going to the **EMSWAN** in Figure 2-1.

- **Application**

  Depending on your network configuration, a Gigabit Ethernet interface typically connects to your site's internal **LAN** or secure **WAN**. The internal **LAN** is also known as the customer **LAN**, and the application network operates on it. This interface provides connectivity for workstations that use the **IP** User Interface. These connections are shown going to the Application **WAN** in Figure 2-1.

- **OOBM** (Only on Tekserver)

  Depending on your network configuration, a Gigabit Ethernet interface typically connects to your site's internal **LAN** or secure **WAN**. This interface provides connectivity to the T1100 **AS** console port via the **OOBM** card.

- **Internal Networks**

Depending on your network configuration, a Gigabit Ethernet interface typically connects to your site's internal **LAN** or secure **WAN**. These interfaces cross connect the two servers for use with heartbeats and database replication.

Understanding the Primary Protocols

The following primary protocols are used in **LSMS** network connections:

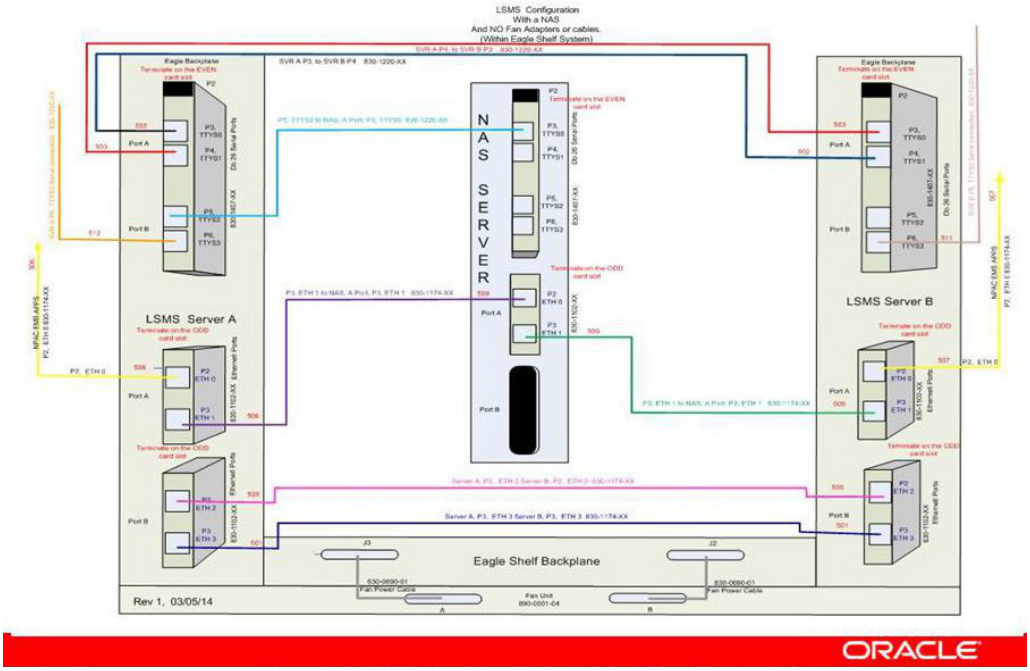
- The Q.3 protocol employs standard **TCP/IP** at **OSI** layers 1 through 3, and the **OSI** protocol at levels 4 through 7. **LSMS** uses a TMN tool kit and Marben protocol stack to implement the **OSI** protocols for these interfaces. This protocol stack does not use the **TSEL** parameter in the **LSMS** configuration. This protocol is used for connections with **NPAC**s.

> **Note:**
>
> The copying of both the runtime NETECH license at path `/usr/local/netech/etc/license` and the Marben OSI license at path `/usr/TKLC/osi/conf/license` is required.

- The standard **TCP/IP** stack is used for:
  - Application network
  - Connections with **ELAP**s

Figure 2-1 shows the **LSMS** network Single Subnet backplane connections.

Figure 2-1 LSMS Configuration: Single Subnet Backplane Connections



Understanding the Multiple Network Interfaces

Each external interface is connected to each LSMS server. Each interface has a redundant interface that can be used if there is a system failure. These multiple interfaces:

- Provide network security by establishing a clear boundary between the various external networks
- Provide dedicated bandwidth for each interface, reducing the risk of congestion while allowing growth
- Aid in troubleshooting and isolating errors

Understanding the Physical Port Assignments

The number of active Ethernet connections for a server depends on which network configuration is used to implement the redundant connectivity between the servers and with external entities.

- Single subnet: each server requires four Ethernet connections and five **IP** addresses (one for the **VIP** address and two for the cloud)

  The following figures and tables show E5-APP-B configuration. Figure 2-2 shows how to connect cables to the server in a single subnet configuration and Table 2-1 defines the physical port assignments.

> **Note:**
>
> A single subnet network configuration is recommended due to the ease of configuration and maintenance.

Figure 2-2 Physical Port Assignments - E5-APP-B Single Subnet Configuration

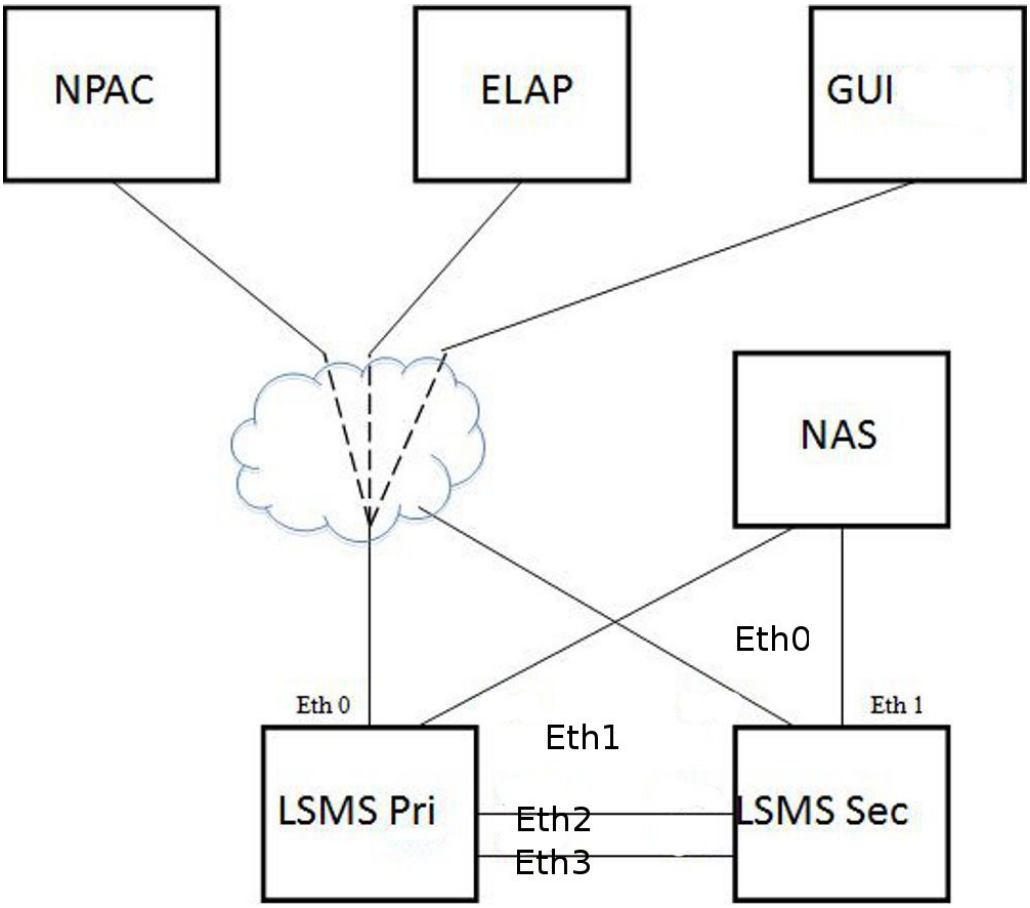


Table 2-1 Physical Port Assignments - E5-APP-B Single Subnet Configuration

LAN Interface	Connections	Speed
Eth0	NPAC, ELAP, GUI, EMS, SSH	Gigabit Ethernet
Eth1	Direct connect to NAS	Gigabit Ethernet
Eth2	Direct connect to Mate for Heartbeat and MySQL replication	Gigabit Ethernet
Eth3	Direct connect to Mate for Heartbeat and MySQL replication	Gigabit Ethernet

The NAS is directly connected with the LSMS in the single subnet configuration. The NAS is configured using `dhcp`.

Eth0 is used to configure the NPAC, ELAP and APP (GUI/SSH).

- Segmented network: each server requires eight Ethernet connections and nine IP addresses (one for the VIP address and six for the clouds)

> **Note:**
>
> There are more switch/router ports required to enable the segmented configuration, which the customer is required to provide. The local switch needs one port for each LSMS Primary, Secondary and NAS. For E5-APP-B, Eth1 is no longer physically connected to the NAS. Eth1 must connect to a local switch for proper NAS performance. The dedicated switch ports must be set to 1Gbps.

Figure 2-3 shows how to connect cables to the server in a segmented configuration and Table 2-2 defines the physical port assignments.

Figure 2-3 Physical Port Assignments - E5-APP-B Segmented Configuration

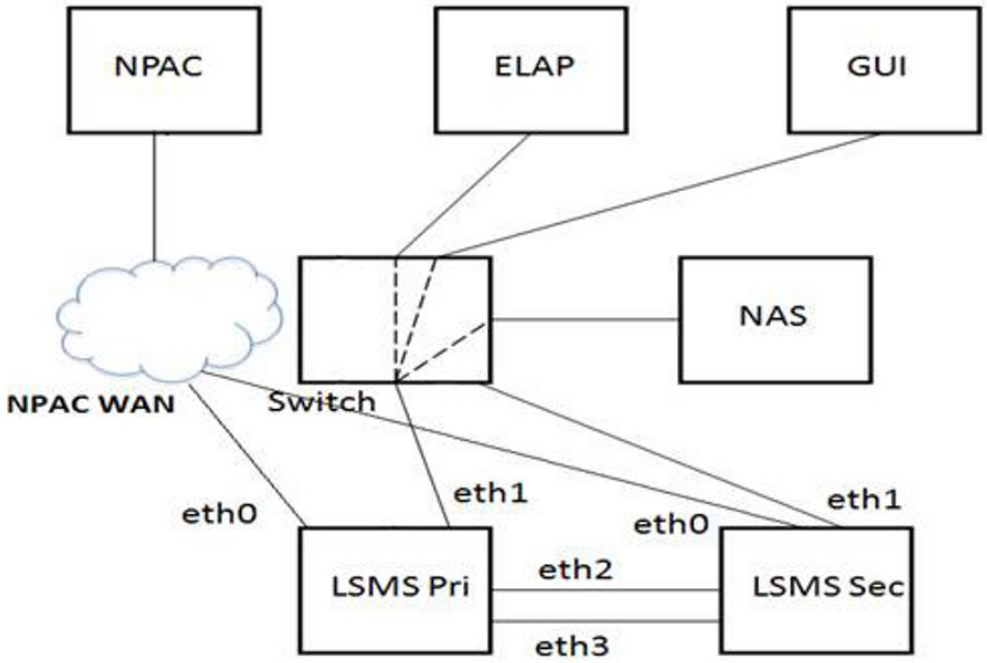
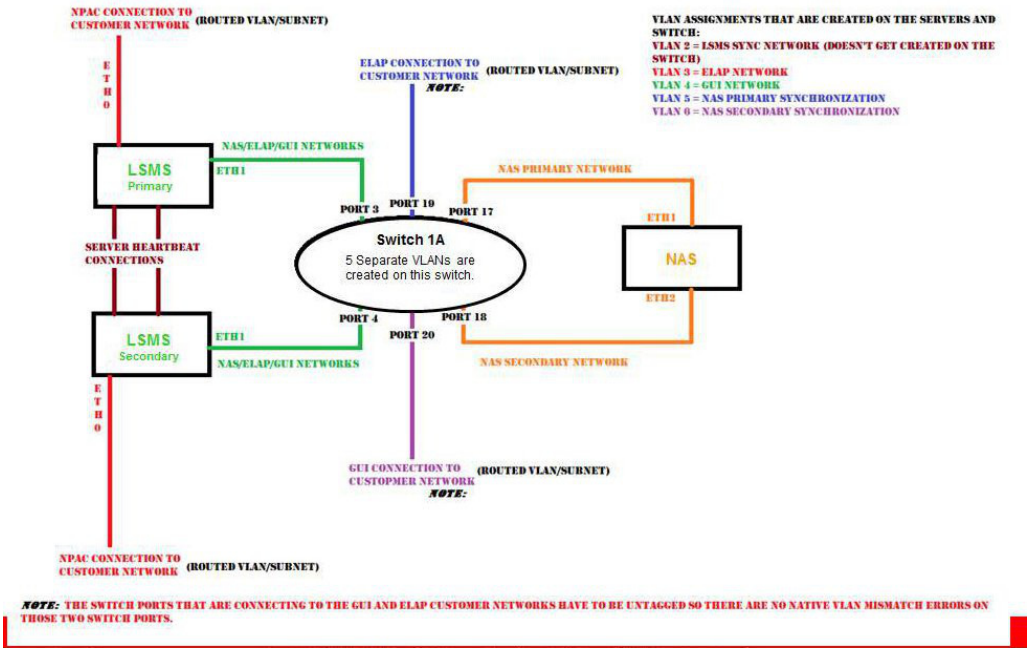


Table 2-2 Physical Port Assignments - E5-APP-B Segmented Configuration

LAN Interface	Connections	Speed
Eth0	NPAC	Gigabit Ethernet
Eth1	NAS, ELAP, GUI, EMS, SSH, Query Server, SNMP	Gigabit Ethernet
Eth2	Direct connect to Mate for Heartbeat and MySQL replication	Gigabit Ethernet
Eth3	Direct connect to Mate for Heartbeat and MySQL replication	Gigabit Ethernet

Figure 2-4 LSMS Configuration: Segmented Configuration



The NAS is connected to Eth1 via switch. The NAS is configured using `dhcp`.

The two aliases of Eth1 are Eth1:0 and Eth1:1, respectively.

Eth1:0 is used to configure APP (GUI/SSH via switch).

Eth1:1 is used to configure ELAP via switch.

Assigning the IP Addresses

For installation of the LSMS, you must provide a minimum of three IP addresses to configure the LSMS to single subnet configuration:

- In a single subnet configuration, a minimum of 3 **IP** addresses (see Table 2-5.
- In a segmented configuration, a minimum of 9 **IP** addresses (see Table 2-6.

The servers share the **VIP** address. During a switchover, the **LSMS HA** switches the **VIP** address to the newly active server.

Handling the VIP Address during a Switchover

The Virtual **IP** (**VIP**) address is constantly associated with whichever server is active. The **VIP** is used for the active server on the Application network only.

> **Note:**
>
> All query servers must use the Application Network so that they can continue to replicate from the active server when switchover occurs.

For more information about switchover, refer to *Alarms and Maintenance Guide*.

Table 2-3 compares how **IP** and **MAC** addresses are used in **LSMS** 9.0 or later and how they were used in previous releases of **LSMS**.

Table 2-3 Comparing LSMS 7.0 and 9.0 or later Addresses

Address	LSMS 7.0		LSMS 9.0 or later	
	Configuration required	**How treated during switchover**	**Configuration required**	**How treated during switchover**
Server **MAC** addresses	Changed ha.env file to configure FirstWatch with server **MAC** addresses	When switchover occurred, both the **MAC** addresses and the **IP** addresses were swapped between the primary server and the secondary server	(Not used for switchover)	
IP address for primary server	Changed ha.env file to configure FirstWatch with primary server **IP** address	When switchover occurred, both the **MAC** addresses and the **IP** addresses were swapped between the primary server and the secondary server	Use `lsmsmgr` to specify **IP** address of server A	Assignment not changed (only the **VIP** address is switched over automatically to the new active server)
IP address for secondary server	Needed to configure FirstWatch with secondary server **IP** address	When switchover occurred, both the **MAC** addresses and the **IP** addresses were swapped between the primary server and the secondary server	Use `lsmsmgr` to specify **IP** address of server B	Assignment not changed (only the **VIP** address is switched over automatically to the new active server)
VIP (Virtual **IP**) address	N/A	N/A	Use `lsmsmgr` to specify **VIP** address	During switchover, **VIP** address is assigned to whichever server is active

NOTE: The server in the upper position in the frame is called server A and, by default, is assigned the hostname lsmspri; the other server is called server B and is assigned the hostname lsmssec. These hostnames can be changed. In LSMS 9.0 or later, lsmspri and lsmssec are merely hostnames; they do not indicate a primary/secondary relationship. In LSMS 9.0 or later, the servers are peers.

Assigning IP Addresses in LSMS 9.0 or later

The **VIP** address is another address, in addition to the **IP** addresses for each specific server. If customers desire to use the same **IP** addresses that they used for previous releases of **LSMS**, it is recommended that they configure the **LSMS** to use the **IP** address that was previously assigned to the primary server as the new **VIP** address, and assign the new **IP** address to one of the servers, as shown in Table 2-4.

Using the **IP** address that was previously used for the primary server as the **VIP** address prevents customers from having to reconfigure various applications that were configured to use that **IP** address.

Table 2-4 Reusing Existing Server IP Addresses

IP Address	In LSMS 7.0, was assigned to:	In LSMS 9.0 or later, assign to:
IP Address 1	lsmspri server	**VIP**
IP Address 2	lsmssec server	Either server
IP Address 3	N/A	Either server

Simplified Configuration Procedures

Most configuration procedures are performed by Oracle Communications employees. Details of the configuration tasks they perform are described later in this chapter. After initial configuration has been performed, customers may choose to use the `lsmsmgr` text interface to change some configuration details, such as changing **NTP** (Network Time Protocol) servers.

Query Server Configuration

Because the **LSMS** now uses database replication instead of shared storage systems, a variety of changes have been made to ensure that query servers always connect to the active server and that any database replication is performed properly. Some query server configuration procedures have changed.

For detailed information about how to configure the query server, refer to Configuring the Query Server.

Netmask and Broadcast

The **LSMS** netmask defaults to a mask matching the address class assigned to each interface. In the event of a class “C” interface, the default broadcast address is the interface address **ORed** with a mask of x000000FF. For example, an **IP** address of 192.168.89.40 would have a broadcast address of 192.168.89.255.

IP Address Provisioning

Table 2-5 and Table 2-6 details the addresses required for **LSMS** and their assignment to interfaces. In the following tables, interfaces marked with a dagger (†) are generally visible outside the immediate **LSMS** area (the customer-provided network), that is, typically they pass through routers and firewalls.

Table 2-5 IP Address Provisioning (Single Subnet Configuration)

IP Address	Protocol	Speed	Assigned to
Active **NPAC**, **EMS**, and Application Network †	Q.3 or **TCP/IP**	Gigabit Ethernet	Active **LSMS** Server `eth0` port

Table 2-5 (Cont.) IP Address Provisioning (Single Subnet Configuration)

IP Address	Protocol	Speed	Assigned to
Inactive **NPAC**, **EMS**, and Application Network	**TCP/IP**	Gigabit Ethernet	Inactive **LSMS** Server `eth0` port (port for status monitoring purposes only)

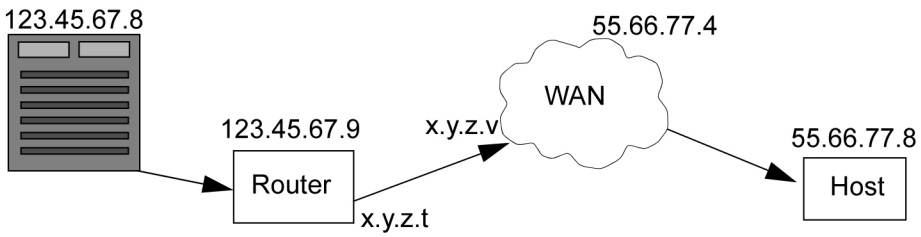
Table 2-6 IP Address Provisioning (Segmented Configuration)

IP Address	Protocol	Speed	Assigned to
Active **NPAC** network †	Q.3	Gigabit Ethernet	Active LSMS server `eth0` port
Active NAS, **EMS** network † and Application Network	Q.3 or **TCP/IP**	Gigabit Ethernet	Active LSMS server `eth1` port
Direct connect to Mate for Heartbeat and MySQL replication	**TCP/IP**	Gigabit Ethernet	Active LSMS server `eth2` or `eth3` port
Inactive **NPAC** network †	**TCP/IP**	Gigabit Ethernet	Active LSMS server `eth0` port
Inactive **EMS** † and Application Network	**TCP/IP**	Gigabit Ethernet	Active LSMS server `eth1` port
Inactive Application Network	**TCP/IP**	Gigabit Ethernet	Active LSMS server `eth2` or `eth3` port

Adding Additional Routes

If you use a multiport router or an Ethernet switch in your network, it is your responsibility to ensure that the network connection receiving packets for the destination end (typically the **NPAC** or **EMS** networks) has an address on the same subnet as each interface. Figure 2-5 illustrates the routing methodology.

Figure 2-5 LSMS Interface Routing in a Segmented Configuration



Note: Addresses shown in this figure are for illustration purposes only.

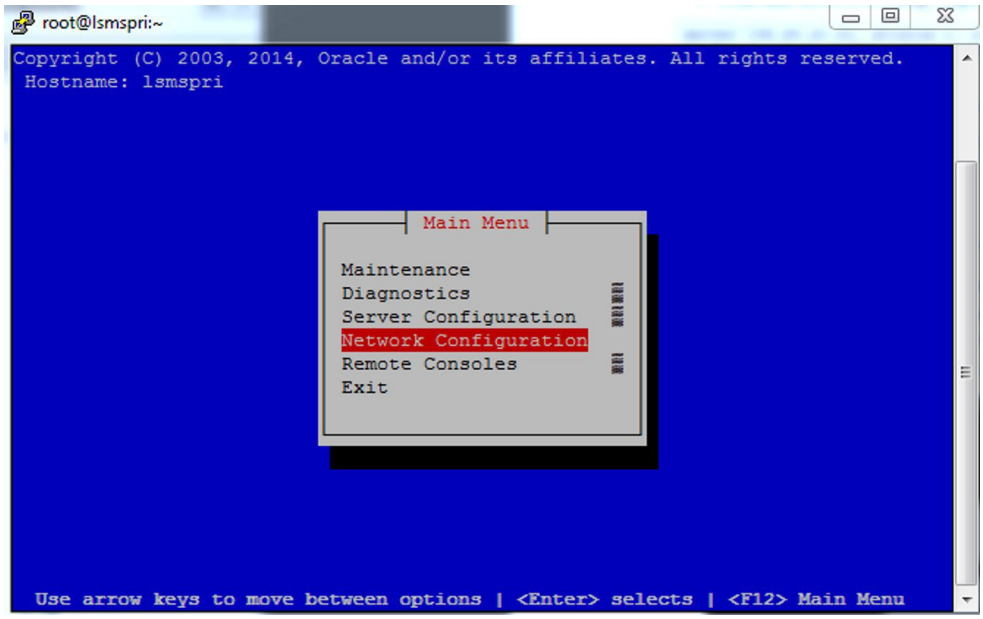
For more routes for your network, use this procedure to define additional routes.

1. Log in to the active server with username **lsmsmgr**.

   (For more information about logging into a server, refer to Using Login Sessions.)

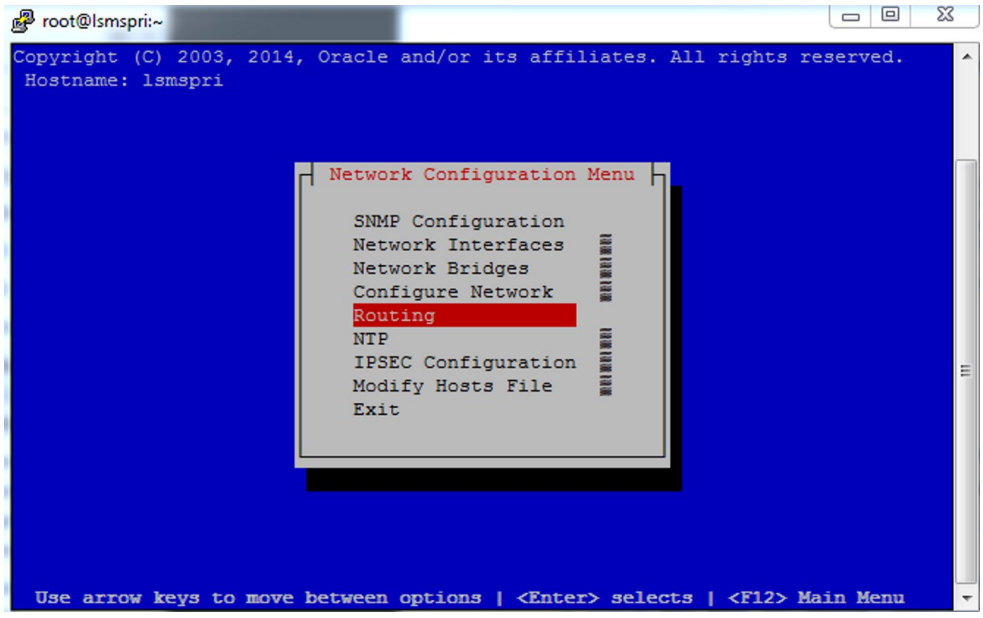
2. From the **Main Menu**, select **Network Configuration** and press **Enter**.

Figure 2-6 Selecting the Network Configuration



3. From the **Network Configuration Menu**, select **Routing** and press **Enter** to display the existing routes.

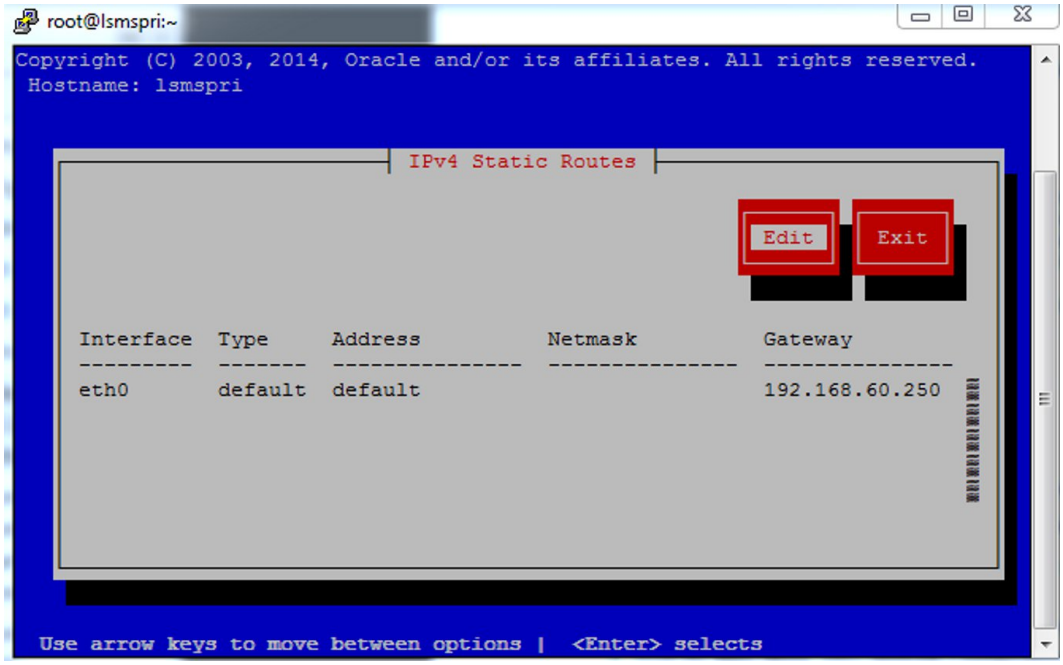
Figure 2-7 Selecting the Routing Menu



4. Examine the current routes on the system.

Consider any additional routes you may wish to add, and click the **Edit** button to start adding other routes.

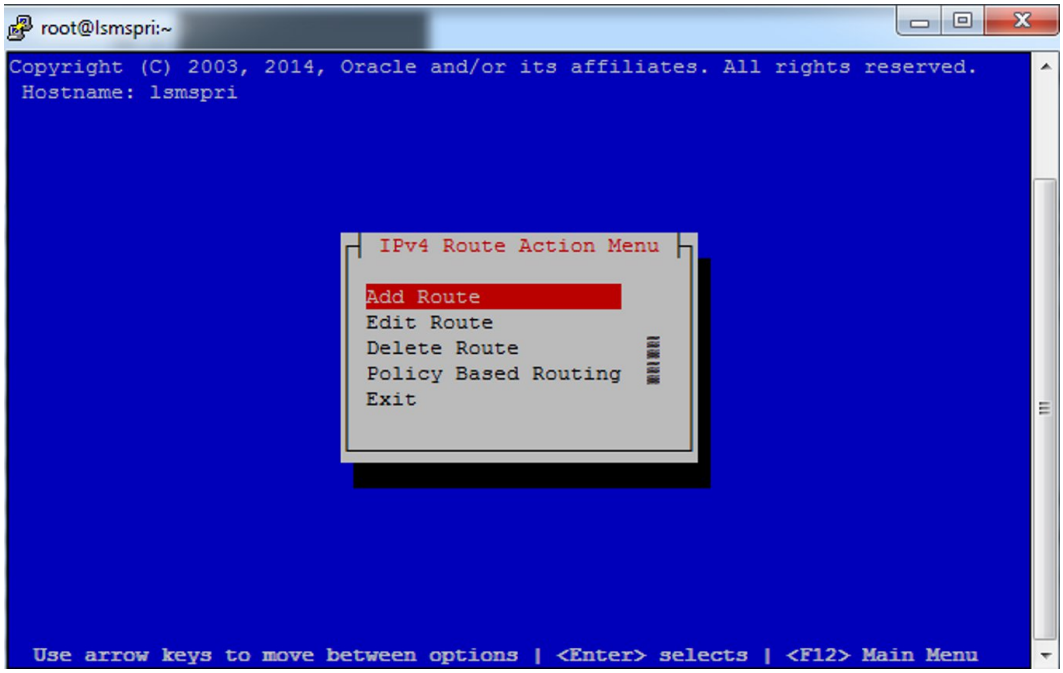
Figure 2-8 Displaying Current System Routes



5. When you want to add another route, press the **Edit** button and see the **Route Action Menu**.

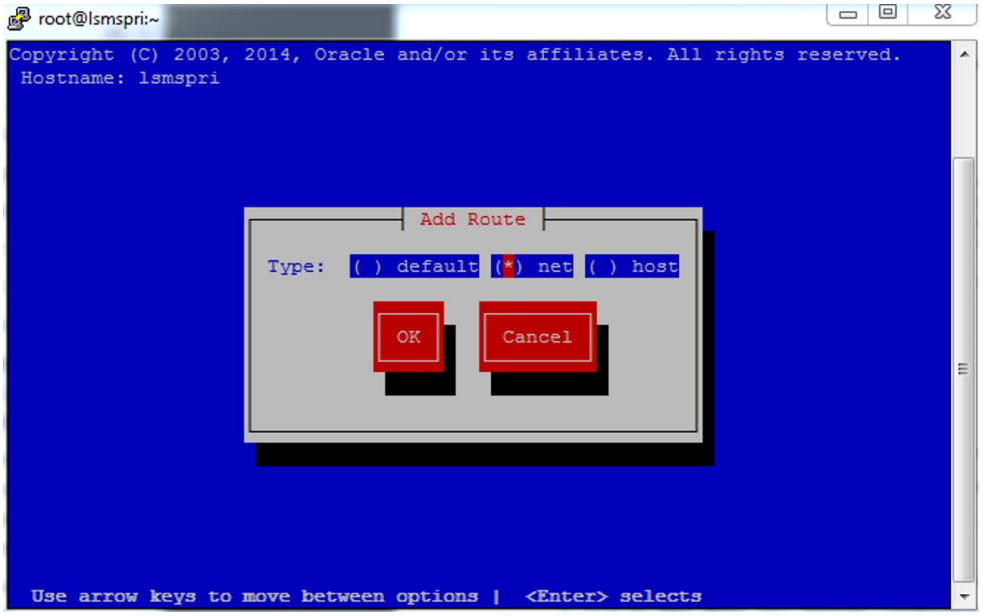
   Select the **Add Route** button and press **Enter**.

Figure 2-9 Choosing to Add a New System Route



6. In the **Add Route** screen, you can select the **( )net** or **( )host** entry by pressing the **space bar**, and press the **OK** button to bring up the screen to add a new route.

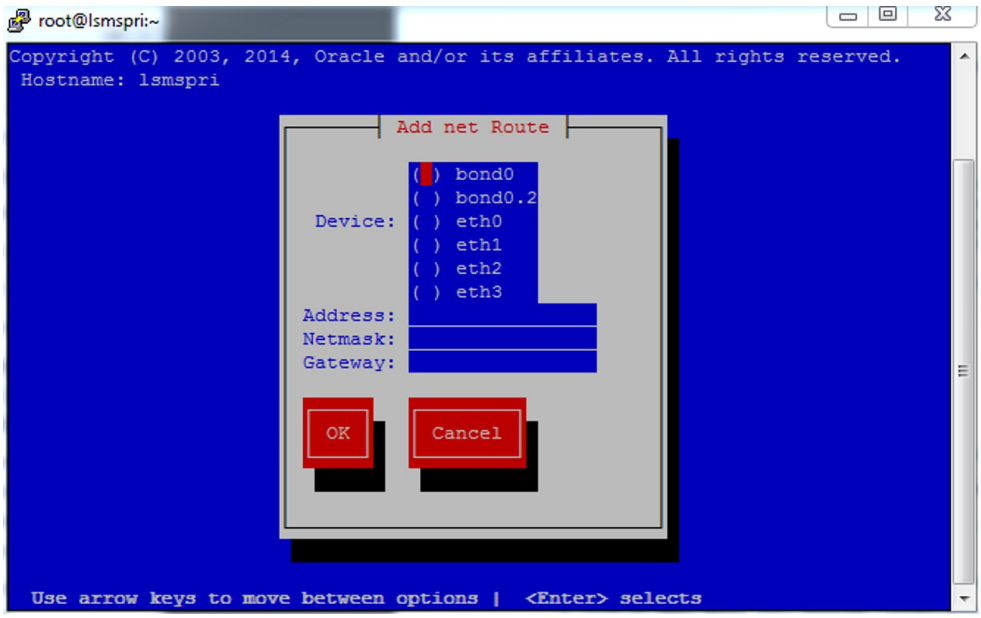
Figure 2-10 Specifying a New System Route



7. In the **Add net Route** screen, you can define the server port, **Address**, **Netmask**, and **Gateway** for the new route you are adding.

   Select the device port to be used, and then fill in the additional fields in the display.

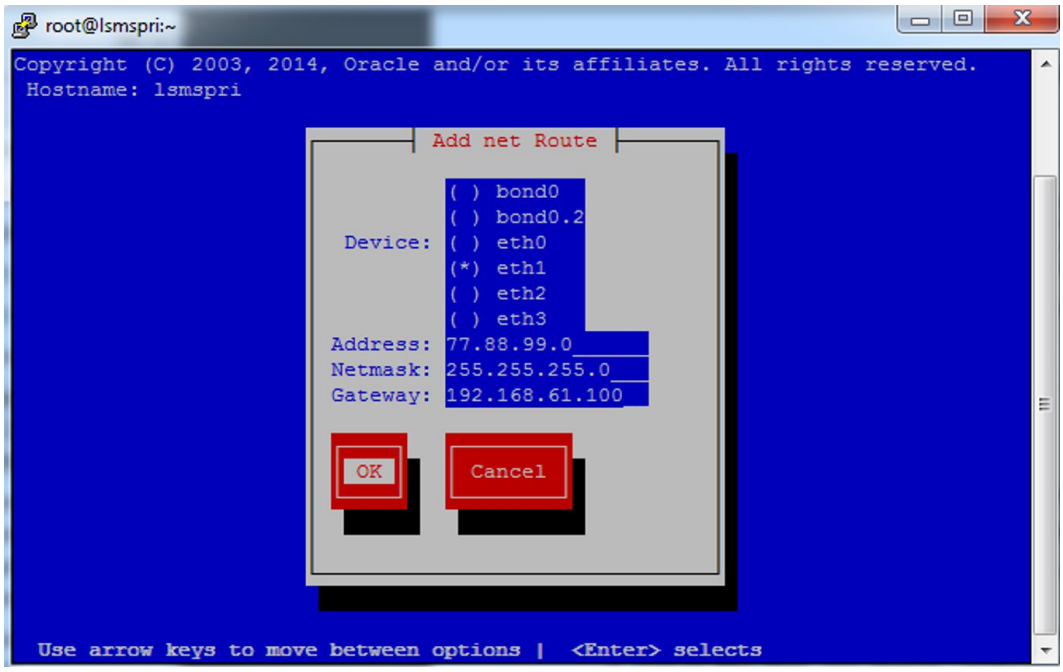
Figure 2-11 Displaying the Add net Route Screen



8. Figure 2-12 shows the fields you defined to add the new route.

Review and be certain your entries are accurate. When you are satisfied with this entry, click the **OK** button to accept your newly defined route.

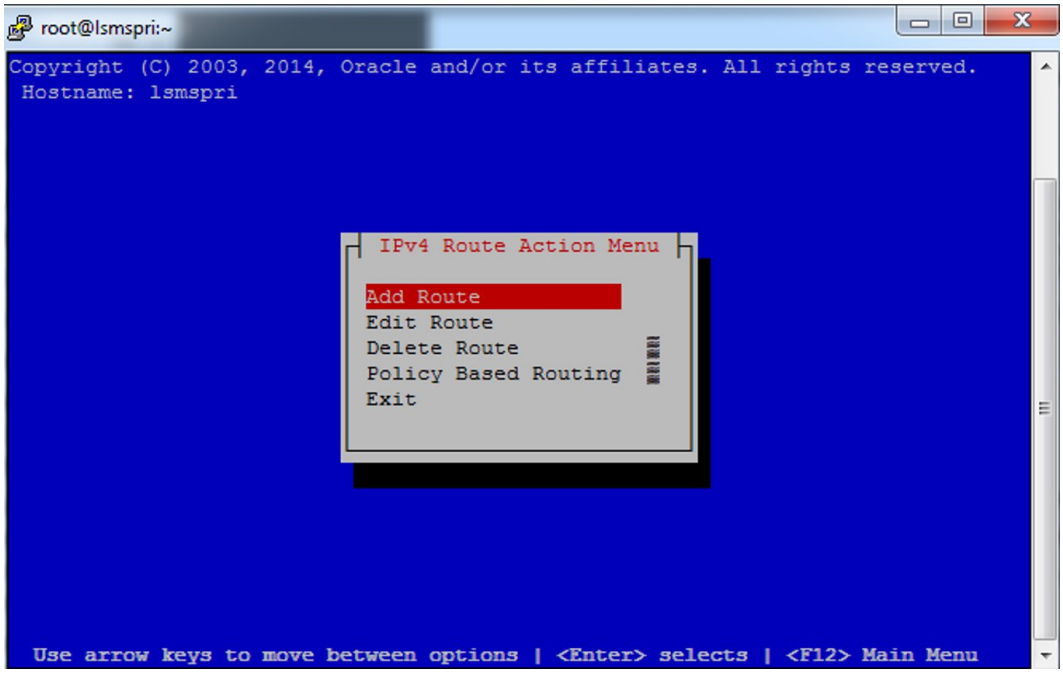
Figure 2-12 Entering a New Add net Route Screen



9. Once a new route is entered and accepted, the display returns to the **Route Action Menu**.

   At this point you can either continue adding more routes by clicking **Add Route** or you can press the **Exit** button and see the definition you have entered.

Figure 2-13 Returning to the Route Action Menu Screen



10. When you press **Exit** on the preceding screen, the system displays the currently defined routes, including the one you just entered.

    At this point you can click **Edit** to change existing routes or click **Exit** to return to the **Network Configuration Menu**.

Understanding Firewall and Router Filtering

Firewall protocol filtering for the various interfaces is defined in the following table:

Table 2-7 LSMS External Ports and Their Use

Interface	TCP/IP Port	Use	Inbound	Outbound
To **NPAC** 100BASE-**TX** (eth0)	102	**OSI** - **TSAP**	Yes	Yes
	20	**FTP** data[1]	No	Yes
	21	**FTP**[1]	No	Yes
	22	**TCP** (ssh, sftp)	Yes[2]	Yes
To EMS 100BASE-TX (eth0)	1030	TCP	Yes	Yes
	22	**TCP** (ssh, sftp)	Yes[4]	Yes
	123	NTP	Yes	Yes
	80	Apache	Yes	No
	8001	suEXEC	Yes	No
	443	HTTPS/Apache	Yes	No
	8473	GUI Server	Yes	Yes
	1030	LSMS Bulk Download and High Speed Audit	Yes	Yes
	7483	LSMS Provisioning Data	Yes	Yes
	9691	Watcher Port (diagnostics)	Yes	Yes
To Application Network 100BASE-TX (eth0)	123	NTP (time synchronization)	Yes	Yes
	102	OSI - TSAP[3]	Yes	Yes
	22	TCP (ssh, sftp)	Yes[4]	Yes
	162	SNMP Trap	No	Yes
	N/A	X Window Packets	Yes	Yes
	20	FTP data[2]	No	Yes
	21	FTP[2]	No	Yes
	162	SNMP Trap	No	Yes
	7079	Web GUI	Yes	Yes
	7080	Web GUI	Yes	Yes
	8200	Application	Yes	Yes

Table 2-7 (Cont.) LSMS External Ports and Their Use

Interface	TCP/IP Port	Use	Inbound	Outbound
To Query Server (only if Query Server Package is enabled)	3306	**LSMS Database** Replication	No	Yes

[1]**FTP** data normally is received from the **NPAC**. The option is left for the **LSMS** to transfer data with the **NPAC** and **EMS**. This assumes the firewall automatically opens the high numbered return port (the default behavior of firewalls such as Firewall-1). If you are using a basic packet filtering router, contact My Oracle Support (MOS)).
[2]The two-way **TCP** communication channel endpoints are the port number 22 and the Server spawned random port value.
[3]OSI transactions on the application network are used only to support Service Assurance.
[4]The two-way TCP communication channel endpoints are the port number 22 and the Server spawned random port value.

> **Note:**
>
> For a segmented configuration, eth1 is used for EMS/APP connections.

Changing Additional Network Information

There are additional changes to the network information that you may wish to define, including:

- Changing LSMS System IP Addresses - If there are conflicts with defaults of IP addresses assigned to private networks, you can modify the system IP addresses.
- Modifying a Netmask - If the netmask for a given network is different from the default for that network class (i.e., 255.255.255.0 for a Class C network), you can modify the netmask.
- Configuring Critical Network Interfaces - Specify any network interface as a critical interface. Whenever the Surveillance feature determines that a critical interface on the active server cannot be reached, the automatic switchover feature switches over to the standby server (for more information, refer to the *Alarms and Maintenance Guide*).

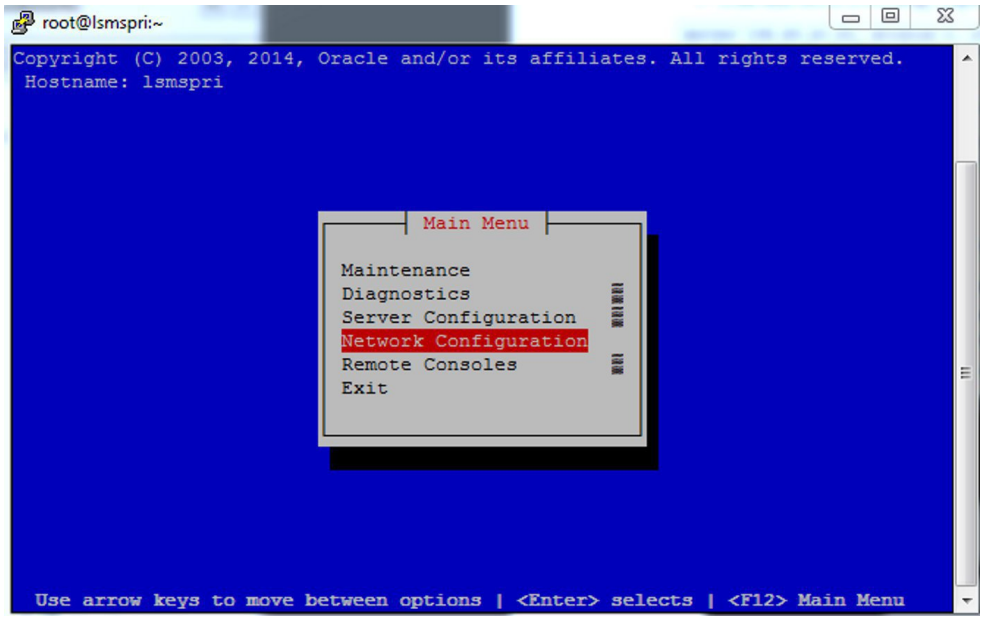
To make any of these changes to your network information, use the following procedure (the entry of data changes occurs in 6)

1. Log in to the active server with username **lsmsmgr**.

   (For more information about logging into a server, refer to Using Login Sessions.)

2. From the **Main Menu**, select **Network Configuration** and press **Enter**.

Figure 2-14 Selecting the Network Configuration Menu

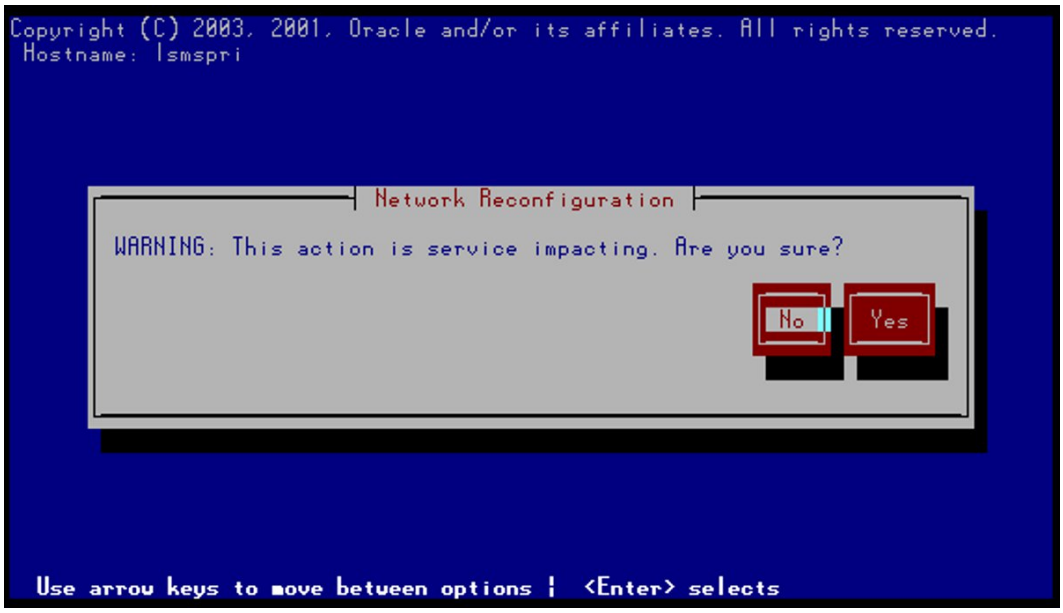


3. From the **Network Configuration Menu**, select **Network Reconfiguration** and press **Enter** to configure your network.

Figure 2-15 Selecting Network Reconfiguration

4. Click **Yes** to confirm that you are initiating network configuration and are aware that this activity does impact service operations.

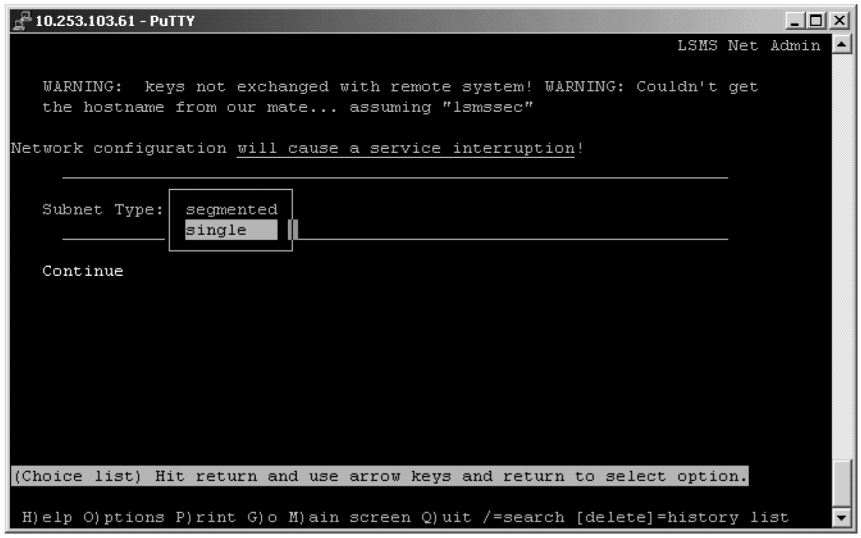
Figure 2-16 Confirming Network Configuration Start-Up



5. Select the appropriate subnet type you want to configure: Single Subnet or Segmented.

   Figure 2-17 illustrates a Single Subnet configuration. A single subnet network configuration is recommended because it is easier to configure and to maintain.

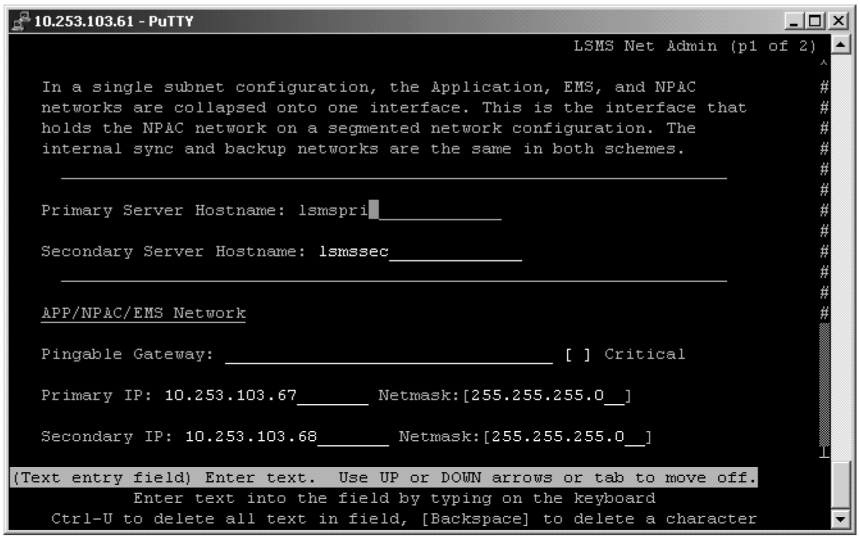
Figure 2-17 Selecting the Subnet Type - Single or Segmented



6. Enter text for the IP addresses for each network, the **VIP** (virtual IP) address where necessary, the default gateway, and the **NTP** server IP address. Press **Enter**.

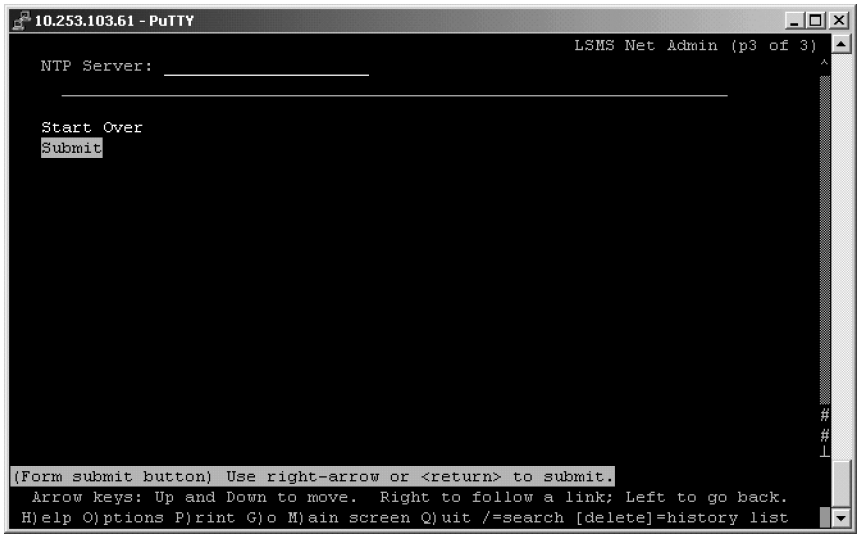
> **Note:**
>
> You must supply a valid **NTP** server IP address to maintain a 5-minute synchronization with the NPAC.

Figure 2-18 Entering Configuration Data



7. Submit the entered text you entered for checking by the lsmsnetAdm script.

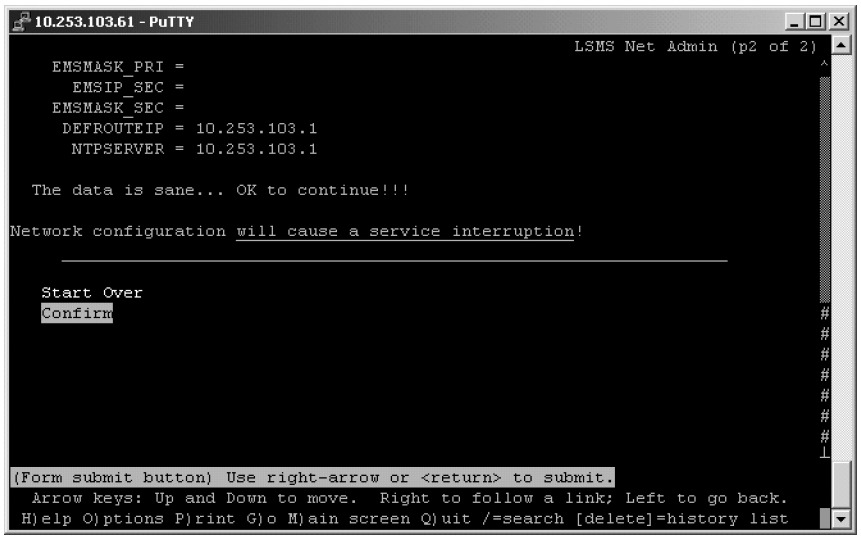
Figure 2-19 Submitting Network Information



8. Review the information for accuracy, as shown in Figure 2-20.

   You may select **Confirm** if correct, or you may change the data by selecting **Start Over**.

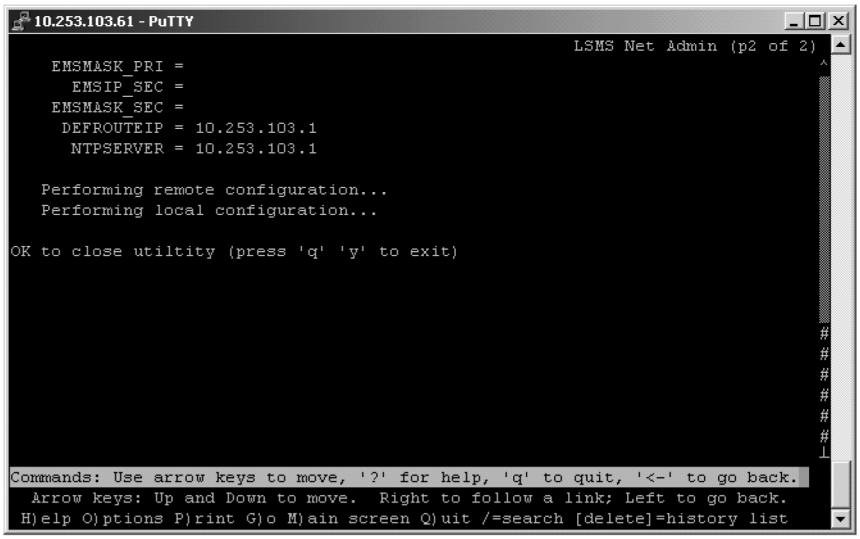
Figure 2-20 Reviewing Entered Network Information



9. Figure 2-21 displays the confirmed data for the configuration.

   When the configuration is completed, enter **q** to quit and then **y** to confirm.

Figure 2-21 Entering a New Add net Route Screen



You will return to the Network Configuration menu.

You have now completed this procedure.

3

Completing Configuration and Starting Connections

This chapter explains how to create and start databases, configure Service Provider contact information, work with key lists, and configure and start **NPAC** components, **EMS** components, **LSMS** components.

Overview

This chapter explains how to create and start databases, configure Service Provider contact information, work with key lists, and configure and start **NPAC** components, **EMS** components, **LSMS** components.

Currently, the following **NPAC** (Number Portability Administration Center) regions serve the United States and Canada:

- Midwest
- MidAtlantic
- Northeast
- Southeast
- Southwest
- Western
- WestCoast
- Canada

LSMS can support all eight **NPACs** simultaneously. The **LSMS** acts as the interface between one or more **NPACs** and one or more network elements (**NEs**). Each **NE** is accessed through its Element Management System (**EMS**).

After you have installed the **LSMS** (for more information, refer to the **LSMS** *Hardware Reference Manual*) and integrated it into your network (see Integrating EAGLE Application B Card (E5-APP-B) into the LSMS Network), perform the remaining configuration procedures, as shown in Table 3-1 and Table 3-2.

Completing Configuration

Perform the procedures shown in Table 3-1 in the order shown, depending on whether you are installing **LSMS** for the first time or adding an **NPAC** region at a later time. In either case, the last step in Table 3-1 directs you to perform the steps in Table 3-2.

Table 3-1 Recommended Order of Configuration Procedures

Recommended Order for Initial Installation	Recommended Order for Adding New Region After Installation	Procedures
1 (Only if needed)	1	"Creating Databases"
2	(Not needed)	Log into the **LSMS GUI** for the first time (see "Starting an LSMS GUI Session" in the *Alarms and Maintenance Guide*).
3	(Not needed)	Create a service provider entry for the **LSMS** owner in the **LSMS** database by performing the procedure "Adding Service Provider Contact Information".
4	(Not needed)	Select **User/Session**, and then **Change Service Provider** and log in with the **SPID** you created in the previous step.
5	2 (if needed)	For each additional **SPID** that you desire to allow access to **LSMS** data, create a supported service provider entry in the **LSMS** database by performing the procedure "Adding Service Provider Contact Information".
6	(Not needed)	Modify the **LSMS** component by performing the procedure Modifying LSMS Configuration Components.
7	(Not needed)	For each **EMS** to be supported, create an **EMS** component by performing the procedure Creating an EMS Configuration Component.
8	3	For each **NPAC**, perform the list of procedures described in Table 3-2.
9	4	If desired, change the default **TT**/**SSN** values by performing the procedure "Modifying Default **TT**/**SSN** Values".

Completing Configuration and Associating with Each NPAC Region

Either as part of initial installation or to add an additional region after the initial installation, perform the procedures in the order shown below *once for each* **NPAC** *region* you need to support.

Table 3-2 Configuring and Associating Each NPAC Region

Step	Procedure to Perform
1	Perform the procedure "Generating a Key List". Select **Keys**, and then **NPAC Keys** to load the **NPAC** public key list into the **LSMS** database by performing the procedure Loading an NPAC Key List.
2	For the **Key File** field, type the following value in the **Key List File** field, where `<ListName>` is the value used in the procedure described in "Generating a **Key** List" (or you can click the **Browse** button and select this file name): `/usr/TKLC/lsms/<ListName>.public` Select **Keys**, and then **LSMS Keys** to load the **LSMS** private key list into the **LSMS** database by performing the procedure Loading an LSMS Key List.
3	For the **Key File** field, type the following value in the **Key List File** field, where `<ListName>` is the value used in the procedure described in "Generating a **Key** List" (or you can click the **Browse** button and select this file name): `/usr/TKLC/lsms/<ListName>.private` Select **Configure**, and then **LNP System**, and then **NPAC** , and then **Modify**, and then **Secondary** to create a secondary **NPAC** component and enter the information described in "Modifying an **NPAC** Component". Ensure that the Activate Region checkbox is empty.
4	For the **Component ID** field, a value that is one greater than the value entered in the procedure in row 5 is suggested. Click the icon that corresponds to this region so that the icon is highlighted, and select **Configure**, and then **LNP System**, and then **NPAC** , and then **Modify**, and then **Primary** to create a primary **NPAC** component. Enter the information described in "Modifying an **NPAC** Component".
5	Ensure that the Activate Region checkbox is filled in. When you click the **OK** button, the *sentry* utility will automatically attempt to associate with the **NPAC**.

Creating Databases

If you are adding a region to be supported, use the following procedure to create the database for the new region:

1. Log in to the active server with the username **lsmsadm**.

   (For more information about logging into a server, refer to the *Alarms and Maintenance Guide*)

2. Change to the $**LSMS**_DIR directory by entering the following command:

   ```
   $ cd $LSMS_DIR
   ```

3. For each new region, enter the following command to create the regional database, where `<region>` is the name of the **NPAC** region:

   ```
   $ npac_db_setup create <region>
   ```

   If an error that indicates that the database already exists is returned, enter the following command to remove the database and then repeat this step.

   ```
   $ npac_db_setup remove <region>
   ```

Service Provider Contact Information

Use the following procedures to add, modify, view, and delete service provider contact information.

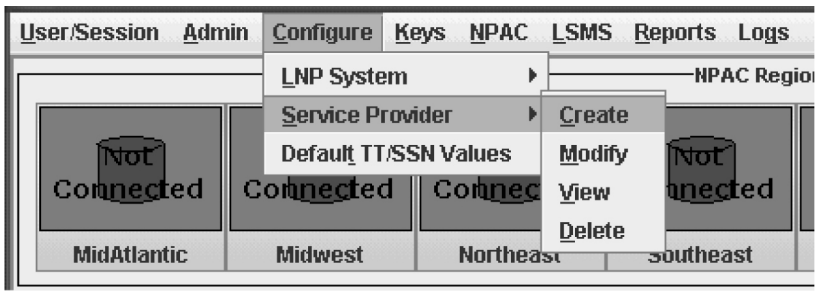
- Adding Service Provider Contact Information
- Modifying Service Provider Contact Information
- Viewing Service Provider Contact Information
- Deleting Service Provider Contact Information

Adding Service Provider Contact Information

To add service provider contact information into the LSMS database, use the following procedure.

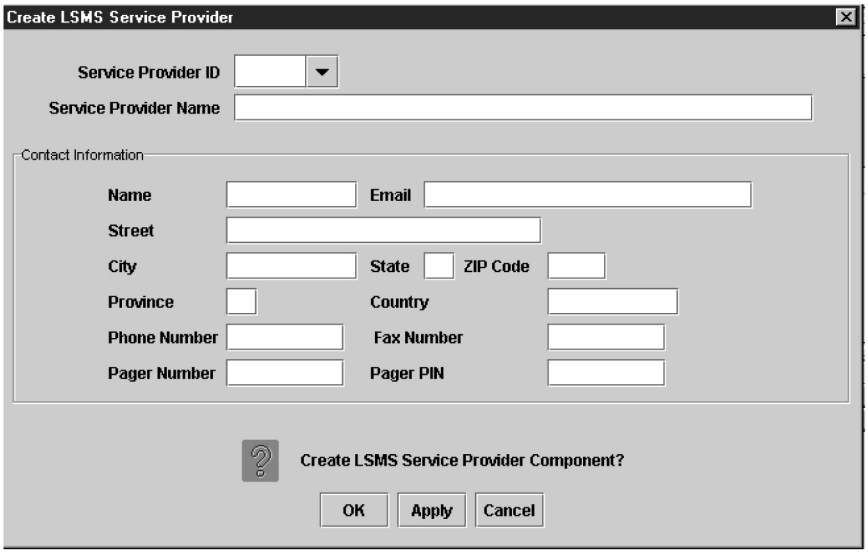
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the **LSMS Console** window, select **Configure**, and then **Service Provider**, and then **Create**.

Figure 3-1 Configure Service Provider Selection



The **Create LSMS Service Provider** window displays.

Figure 3-2 Create LSMS Service Provider Window



3. Enter the Service Provider **ID** (four alphanumeric characters).
4. Enter the Service Provider Name (maximum 40 printable characters).
5. Enter the following Contact Information items:
   - *Name* – name of the person to contact for service provider network information (maximum 40 alphanumeric characters)
   - *Email* – email address for the service provider network contact (maximum 60 alphanumeric characters)
   - *Street* – street address of the service provider network contact (maximum 40 alphanumeric characters)
   - *City* – city address of the service provider network contact (maximum 20 alphanumeric characters)
   - *State* – state address of the service provider network contact (two-letter uppercase abbreviation).
     If you use the *Province* field, enter **--** (the default).
   - **ZIP** *Code*– postal zip code of the service provider network contact (five numeric characters)
   - *Province* – province of the service provider network contact (two-letter uppercase abbreviation).
     If you use the *State* field, enter **--** (the default).
   - *Country* – country of the service provider network contact (maximum 20 alphanumeric characters)
   - *Phone Number* – phone number of the service provider network contact (ten numeric characters)
   - **FAX** *Number* – **FAX** number of the service provider network contact (ten numeric characters)
   - *Pager Number* – pager number for the service provider network contact (ten numeric characters)

- *Pager* **PIN**– pager **PIN** number for the service provider network contact (maximum ten numeric characters)

6. When finished, click **OK** to apply the changes and return to the **LSMS Console** window, or **Apply** to apply the changes and remain in the current window.

   Click **OK** in the message window:

Figure 3-3 Create Successful

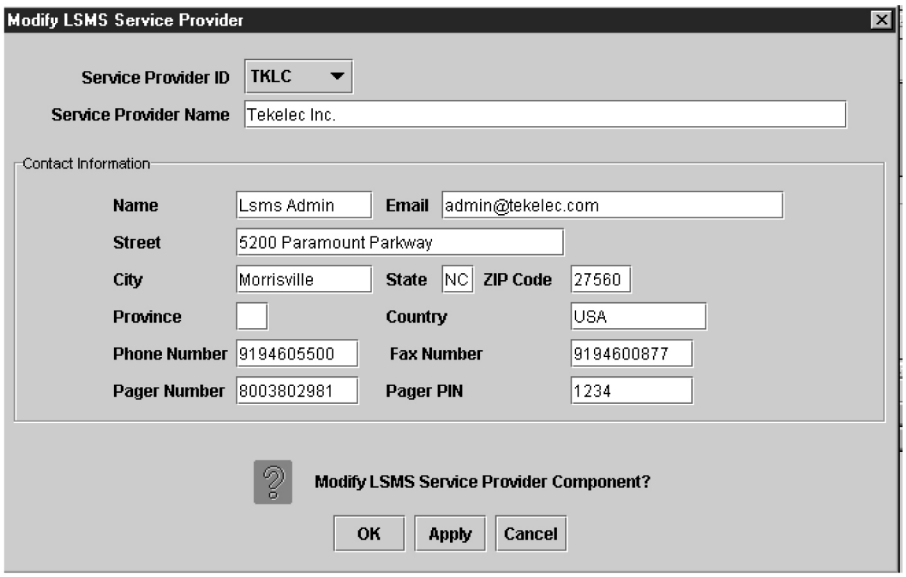
7. If you clicked **Apply** in 6, repeat steps 3 through 6.

Modifying Service Provider Contact Information

To modify service provider contact information, use the following procedure.

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the **LSMS** Console window, select **Configure**, and then **Service Provider**, and then **Modify**.

Figure 3-4 Modify LSMS Service Provider Window



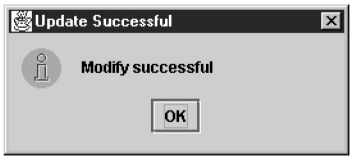
3. Enter the Service Provider **ID** (4 alphanumeric characters) or click the down arrow and select the desired Service Provider **ID** from the listbox.
4. Modify the service provider contact information as required.

   See “Adding Service Provider Contact Information” for detailed information.

5. When finished, click **OK** to apply the changes and return to the **LSMS Console** window, or **Apply** to apply the changes and remain in the current window.

Click **OK** in the message window:

Figure 3-5 Modify Successful



6. If you clicked **Apply** in 5, repeat steps 3 through 5.

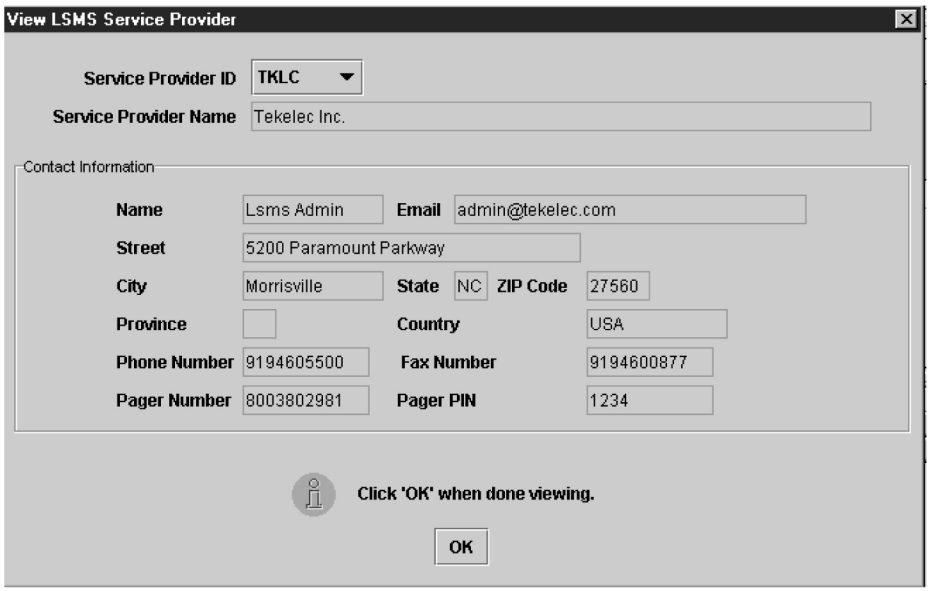
Viewing Service Provider Contact Information

To view service provider contact information, use the following procedure.

1. Log in as a user in the `lsmsview`, `lsmsuser`, `lsmsuext`, or `lsmsadm` group.
2. From the **LSMS Console** window, select **Configure**, and then **Service Provider**, and then **View**.

   The information in this window is read-only and cannot be modified.

Figure 3-6 View LSMS Service Provider Window



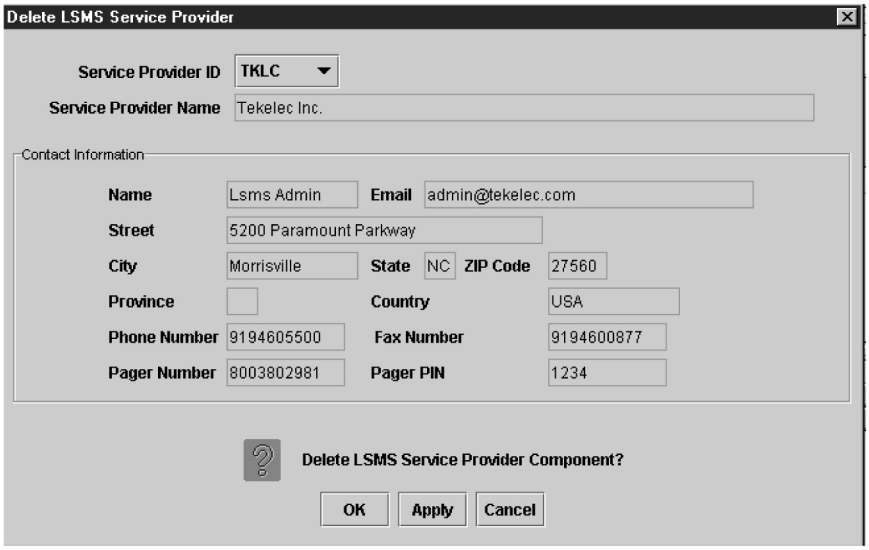
3. When finished viewing the information, click **OK** to return to the **LSMS Console** window.

Deleting Service Provider Contact Information

To delete service provider contact information, use this procedure.

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the **LSMS Console** window, select **Configure**, and then **Service Provider**, and then **Delete**.

Figure 3-7 Delete LSMS Service Provider Window



3. If the Service Provider that you wish to delete is not displayed in the Service Provider **ID** field, click the down arrow to the right of that field and select the Service Provider **ID** that you wish to delete.
4. Verify that this is the Service Provider that you wish to delete.
5. When finished, click **OK** to apply the changes and return to the **LSMS Console** window, or **Apply** to apply the changes and remain in the current window.

   In either case, the **Delete Confirmation** window displays.

Figure 3-8 Delete Confirmation Window

6. Click **Yes** or **No** to end this procedure.

LSMS Configuration Components

Use the following procedures to manage **LSMS** configuration components:

- Modifying LSMS Configuration Components
- Viewing a Configured LSMS Component

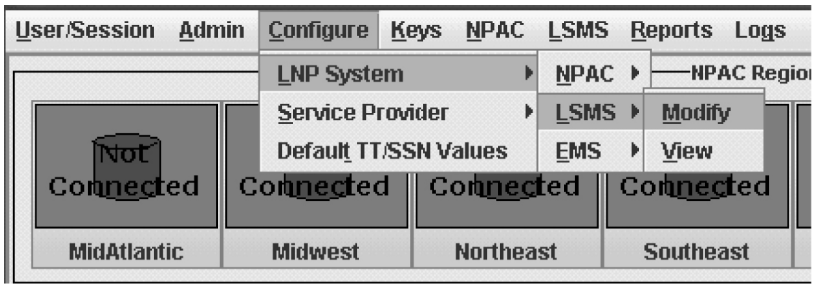
Modifying LSMS Configuration Components

Use the following procedure to create or modify **LSMS** configuration components.

1. Log in as a user in the `lsmsadm` or `lsmsall` group.

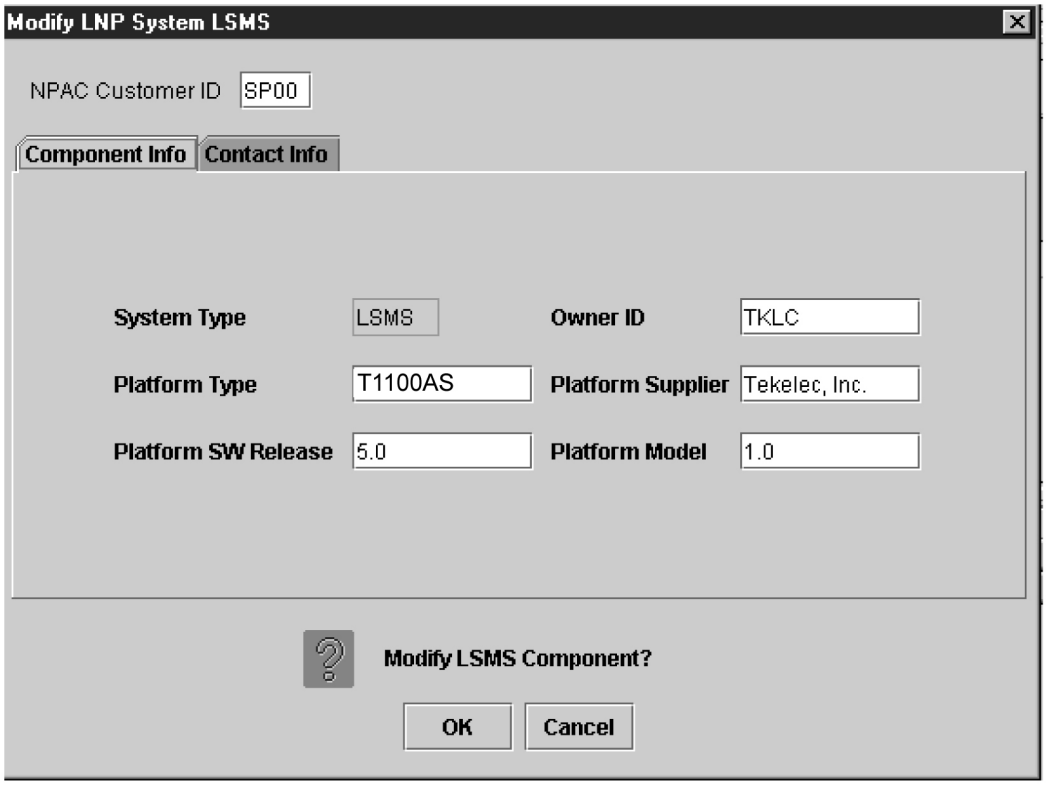
2. From the main menu, select **Configure**, and then **LNP System**, and then **LSMS**, and then **Modify**.

Figure 3-9 LNP System Menu – Modify LSMS



The **Modify LNP System LSMS** window displays. In this example, the **Primary** was selected. The window usually opens with the Component Info tab displayed; if the Component Info tab is not displayed, click its tab to display it.

Figure 3-10 Modify LNP System LSMS Component Info Tab



3. In the **NPAC** Customer **SPID** field, enter the identification (four alphanumeric characters) by which the **LSMS** owner is known to the **NPACs**.

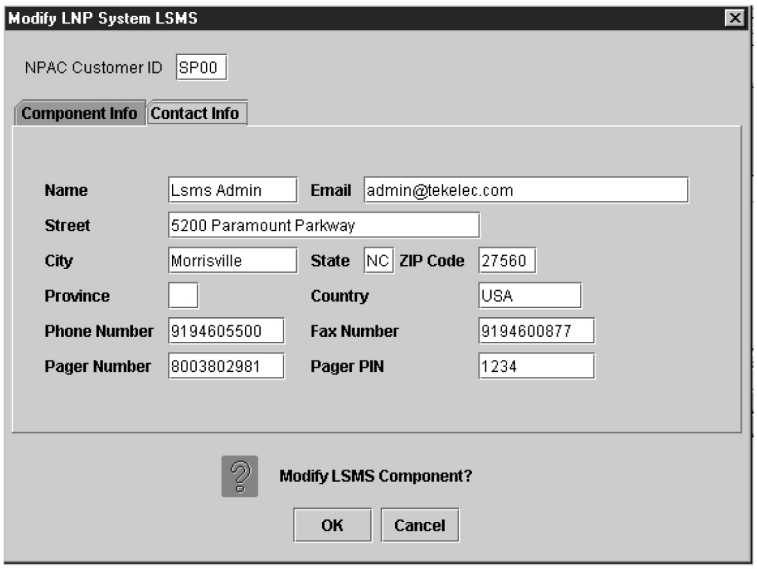
   This required field will be used when the **LSMS** associates with the **NPAC**.

4. Enter the **LSMS** Component Info data as follows (all fields in the Component Info tab must contain data):

- *Owner* **ID** – **ID** of the **LSMS** owner (maximum 20 alphanumeric characters)
- *Platform Type* – hardware platform of the **LSMS** (maximum 20 alphanumeric characters)
- *Platform Supplier* – name of the supplier of the **LSMS** hardware platform (maximum 20 alphanumeric characters)
- *Platform* **SW** *Release* – release level of the software running on the **LSMS** platform (maximum 20 alphanumeric characters)
- *Platform Model* – model number of the **LSMS** platform (maximum 20 alphanumeric characters)

5. Click the **Contact Info** tab.

Figure 3-11 Modify LNP System LSMS Contact Info



6. All fields in the **Contact Info** tab are optional.

   If you wish to enter **LSMS** Contact Info data, do so as follows:

   - *Name* – name of the person to contact for **LSMS** information (maximum 40 alphanumeric characters)
   - *Email* – email address of the **LSMS** contact person (maximum 60 alphanumeric characters)
   - *Street* – street address of the **LSMS** contact person (maximum 40 alphanumeric characters)
   - *City* – city address of the **LSMS** contact person (maximum 20 alphanumeric characters)
   - *State* – state address of the **LSMS** contact person (two-letter uppercase abbreviation).
     If you use the *Province* field, enter **--** (the default).
   - **ZIP** *Code* – postal zip code of the **LSMS** contact person (five numeric characters)
   - *Province* – province of the **LSMS** contact person (two-letter uppercase abbreviation).

If you use the *State* field, enter **--** (the default).

- *Country* – country of the **LSMS** contact person (maximum 20 alphanumeric characters)
- *Phone Number* – phone number of the **LSMS** contact person (ten numeric characters required)
- **FAX** *Number* – **FAX** number of the **LSMS** contact person (ten numeric characters required)
- *Pager Number* – pager number of the **LSMS** contact person (ten numeric characters required)
- *Pager* **PIN** – pager **PIN** number of the **LSMS** contact person (ten numeric characters maximum)

7. When finished, click **OK** to apply the changes.
   - If the following message appears, click **OK** in the message window and the **GUI** will return to the main console window.

Figure 3-12 Modify Successful

   - If a message similar to the following appears, a mandatory field is empty or a field is not properly configured.

Figure 3-13 More Fields Needed

Click **OK** in the message window and correct the appropriate field. Repeat this step until the message in Figure 3-12 displays.

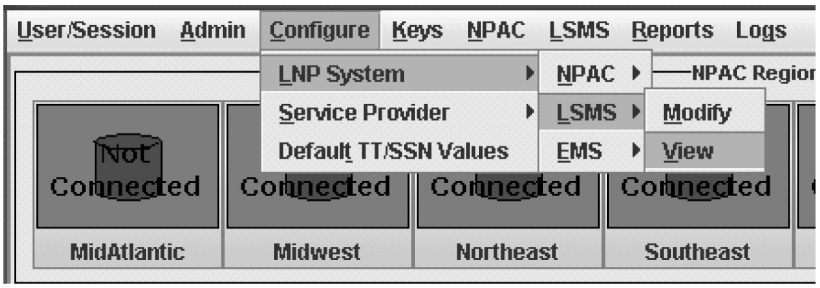
You have now completed this procedure.

Viewing a Configured LSMS Component

To view configured **LSMS** component information, use the following procedure.

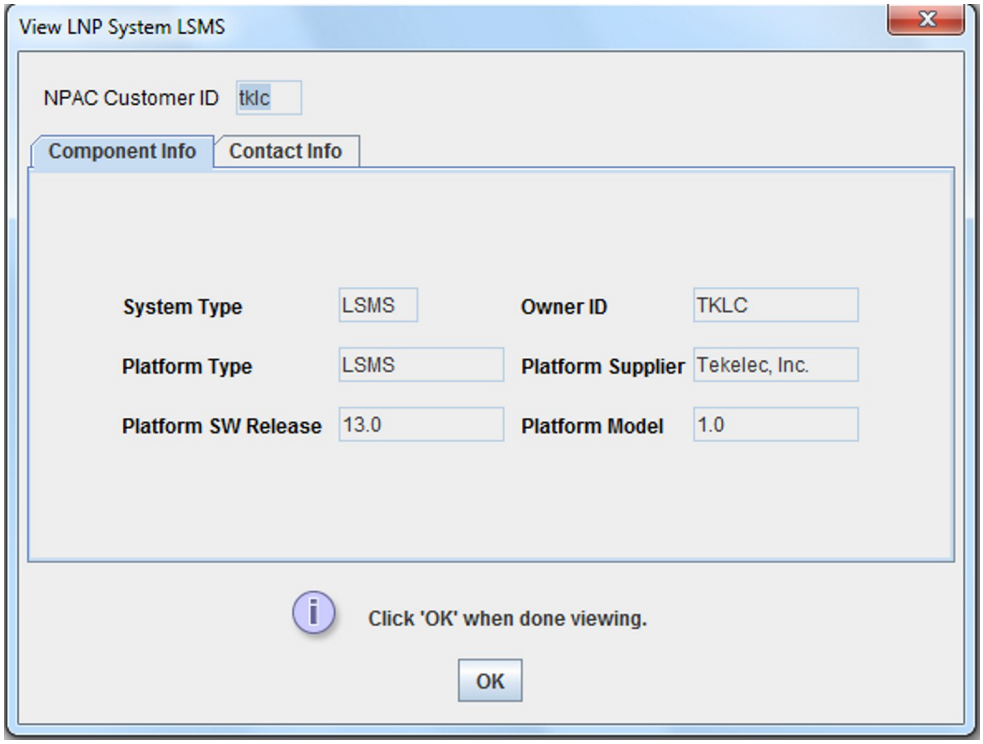
1. Log in as a user in the `lsmsadm`, `lsmsuser`, `lsmsuext`, `lsmsview`, or `lsmsall` group.
2. From the main menu, select **Configure**, and then **LNP System**, and then **LSMS** , and then **View**.

Figure 3-14 LNP System Menu – View LSMS



The **View LNP System LSMS** window displays. The window usually opens with the Component Info tab displayed.

Figure 3-15 View LNP System LSMS Window



3. To view a different tab, click on the tab.

   For information about the fields displayed in any of the tabs, see their description in the procedure defined in Modifying LSMS Configuration Components.

4. When finished viewing this window, click **OK** to return to the main **LSMS** console window.

You have now completed this procedure.

EMS Configuration Component

Use the following procedures to manage TekPath or ELAP **EMS** configuration components:

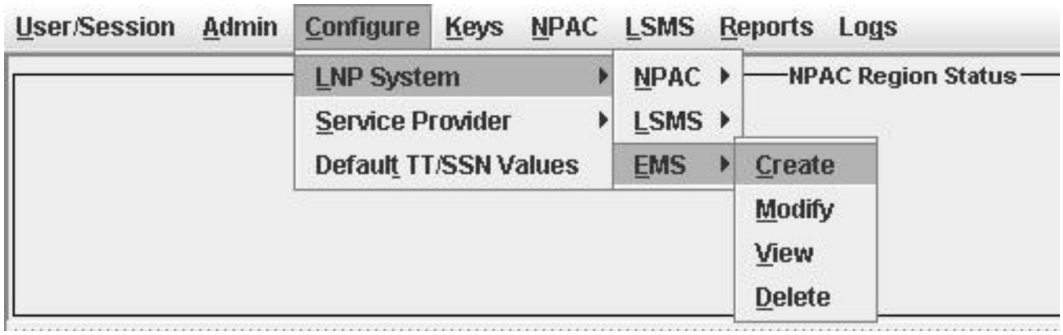
Creating an EMS Configuration Component

For each network element to be supported by the **LSMS**, create an **EMS** configuration component using the following procedure.

> **Note:**
>
> For each EMS configuration created, you must perform a bulk download to the associated EMS/network element. Refer to the *LNP Database Synchronization User's Guide* for bulk loading procedures.

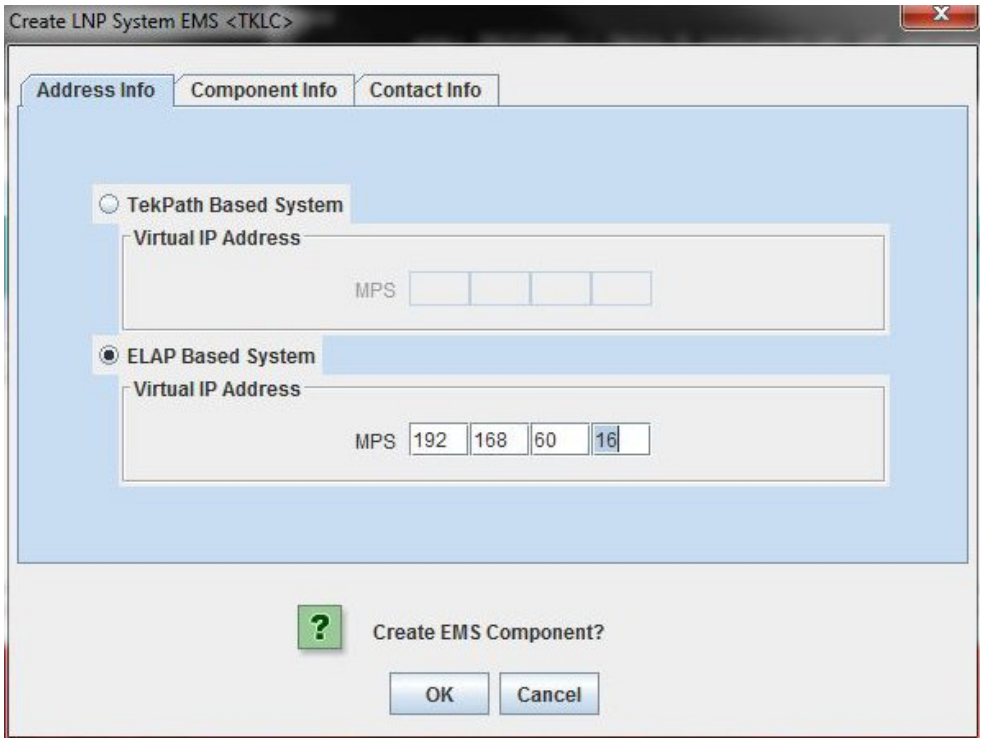
1. Log into the **LSMS** as a user in the `lsmsadm` or `lsmsall` group.
2. From the LNP System menu, shown in Figure 3-16, select **Configure**, and then **LNP System**, and then **EMS**, and then **Create**.

Figure 3-16 LNP System Menu – Create EMS



The EMS Configuration Component window, Figure 3-17 displays. The window usually opens with the **Address Info** tab displayed; if the **Address Info** tab is not displayed, click its tab to display it.

Figure 3-17 Create LNP System EMS Address Info Tab



3. Ensure that the radio button for an **ELAPMPS** or a TekPath **MPS** is selected. For an **ELAPMPS** (ELAP version 7 or older), enter the **IP** addresses for **MPS** A and **MPS** B (enter a value from 0 to 255 in each of the first three octets and a value from 0 to 254 in the forth octet). For a TekPath **MPS**, enter the **IP** address for **MPS** A only.

> **Note:**
>
> The **LSMS** no longer supports connections to **OAPs**.

4. Select one of the following radio buttons for the **Verify MPS with PING** field to specify whether the **LSMS** uses **PING** to monitor the connectivity between the **LSMS** and the **MPS**.

> **Note:**
>
> With either selection, the **LSMS** always monitors connectivity with the keep alive function.

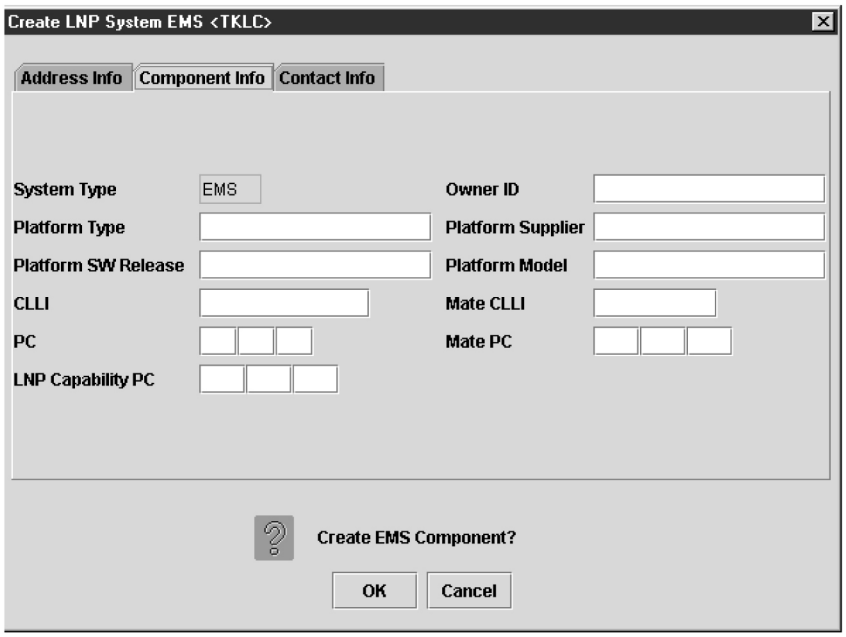
- **Enabled** to monitor the **MPS** by sending **PING**s over the **UDP** port. This selection requires an additional port to be open (which can be a security concern), but supports previously available function.
- **Disabled** to monitor the **MPS** using only the keep alive function. This selection reduces the number of ports required to be open inbound to the **ELAP** network. Security is increased when the number of open ports is decreased.

> **Note:**
>
> The **LSMS/EMS PING** Enhancement feature provides the following functionality:

- Prevents intermediate devices (for example, routers and switches) from closing idle **HSOP** connections
- Detects low level network faults that were previously not detectable using the **TCP/IP** stack alone.

5. Click the **Component Info** tab, shown in Figure 3-19.

Figure 3-18 Create LNP System EMS Component Info

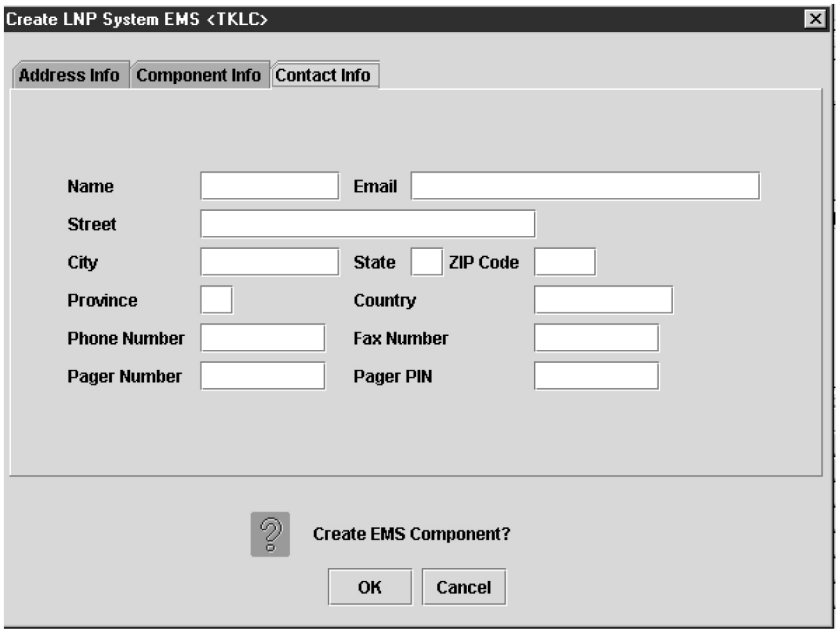


6. Enter the **Component Info** data as follows (all fields in this tab must contain data):
   - *Owner* **ID** – **ID** of the network element owner (maximum 20 alphanumeric characters)
   - *Platform Type* – hardware platform of the network element (maximum 20 alphanumeric characters)
   - *Platform Supplier* – name of the supplier of the network element hardware platform (maximum 20 alphanumeric characters)
   - *Platform* **SW** *Release* – release level of the software running on the network element platform (maximum 20 alphanumeric characters)
   - *Platform Model* – model number of the network element platform (maximum 20 alphanumeric characters)
   - **CLLI** – **CLLI** code of the network element (maximum 11 numeric and uppercase alphabetic characters)
   - *Mate* **CLLI**– **CLLI** of the mate **EMS** component (maximum 11 numeric and uppercase alphabetic characters)

- **PC** – point code of the **EMS** component (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)
- *Mate* **PC** – point code of the mate **EMS** component (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)
- **LNP** *Capability* **PC** – **LNP** capability point code of the network element (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)

7. Click the **Contact Info** tab, shown in Figure 3-18.

Figure 3-19 Create LNP System EMS Contact Info



8. All fields in this tab are optional. If you wish to enter the **Contact Info** data, do so as follows:
   - *Name* – name of the person to contact for network element information (maximum 40 alphanumeric characters)
   - *Email* – email address of the network element contact person (maximum 60 alphanumeric characters)
   - *Street* – street address of the network element contact person (maximum 40 alphanumeric characters)
   - *City* – city address of the network element contact person (maximum 20 alphanumeric characters)
   - *State* – state address of the network element contact person (two-letter uppercase abbreviation). If you use the *Province* field, enter **--** (the default).
   - **ZIP** *Code* – the postal zip code of the network element contact person (five numeric characters)

- *Province* – the province of the network element contact person (two-letter uppercase abbreviation). If you use the *State* field, enter **--** (the default).
- *Country* – country of the network element contact person (maximum 20 alphanumeric characters).
- *Phone Number* – phone number of the network element contact person (ten numeric characters required).
- **FAX** *Number* – **FAX** number of the network element contact person (ten numeric characters required).
- *Pager Number* – pager number of the network element contact person (ten numeric characters required)
- *Pager* **PIN**– pager **PIN** number of the network element contact person (ten numeric characters maximum)

9. When finished, click **OK** to apply the changes.
   - If the Update Successful dialog, Figure 3-20 appears, click **OK**. The **GUI** returns to the main console window.

Figure 3-20 Update Successful Dialog

   - When a mandatory field is empty or a field is not properly configured, the Field Required Figure 3-21 dialog displays.

Figure 3-21 Field Required Dialog

   Click **OK** and correct the appropriate field.

   Repeat this step until you receive an Update Successful notification.

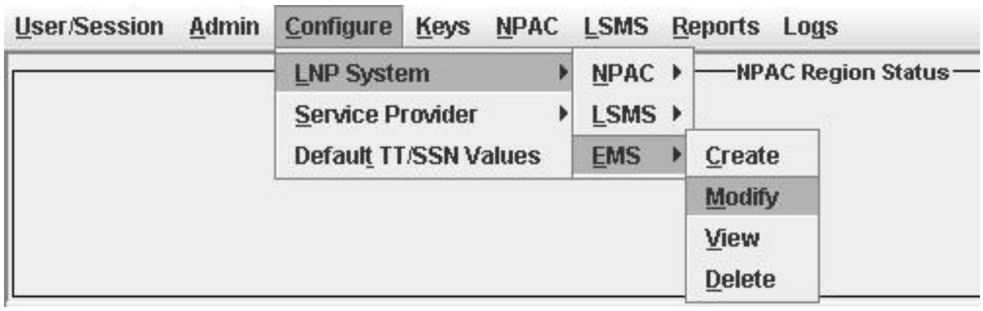
Modifying an EMS Configuration Component

To modify an existing EMS configuration component, use the following procedure.

> **Note:**
>
> For each EMS configuration created, you must perform a bulk download to the associated EMS/network element. Refer to the *LNP Database Synchronization User's Guide* for bulk loading procedures.

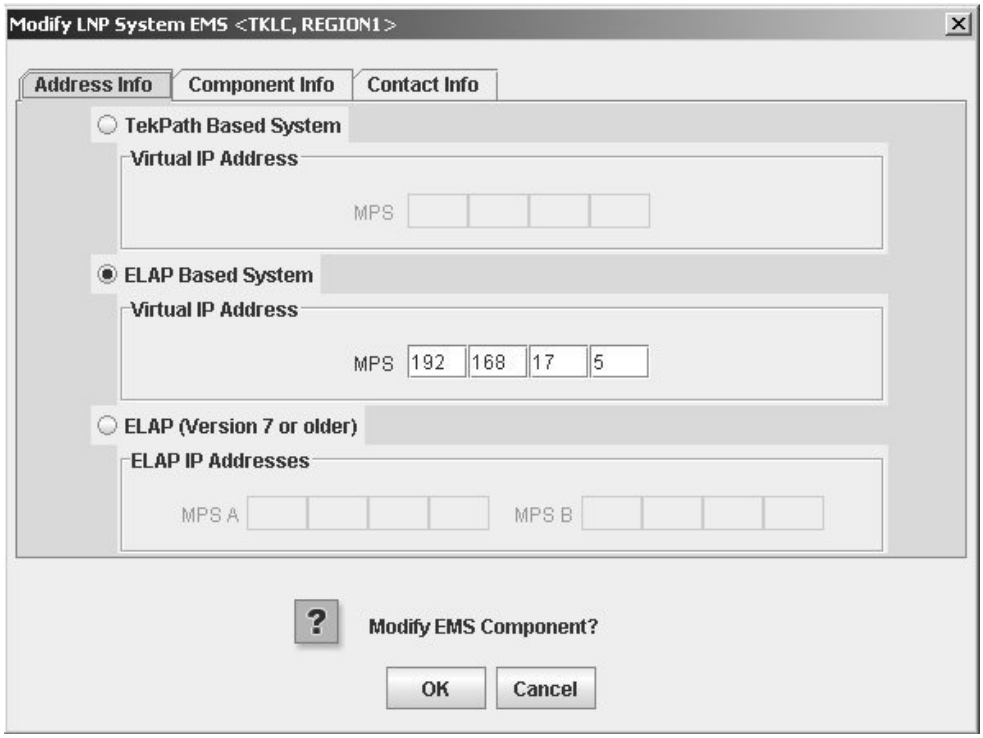
1. Log into the LSMS as a user in the `lsmsadm` or `lsmsall` group.
2. Click the **EMS status** icon for the EMS you wish to modify so that the icon is highlighted.
3. From the **Main Menu**, select **Configure**, and then **LNP System**, and then **EMS**, and then **Modify**, as shown in Figure 3-22.

Figure 3-22 LNP System Menu – Modify EMS



The Modify LNP System EMS window, Figure 3-23, appears.

Figure 3-23 Modify LNP System EMS Window



The window usually opens with the **Address Info** tab displayed; if the **Address Info** tab is not displayed, click its tab to display it.

4. Modify the **EMS** data as required.

   See Creating an EMS Configuration Component for detailed field information.

5. Click **OK**.

   The EMS Routing dialog appears, Figure 3-24 .

Figure 3-24 EMS Routing Dialog

Click **OK**.
The Update Successful dialog displays, Figure 3-25.

Figure 3-25 Update Successful Dialog

You have completed this procedure.
If a mandatory field is empty or a field is not properly configured, the More Fields Needed message is displayed, Figure 3-26.

Figure 3-26 More Fields Needed Dialog

Click **OK** and correct the appropriate field.

Repeat this step until you receive an Update Successful notification.

> **Note:**
>
> Changes do not take effect until the `eagleagent` is restarted (refer to "Manually Verifying and Restarting the Eagle Agents" in the *Alarms and Maintenance Guide*).

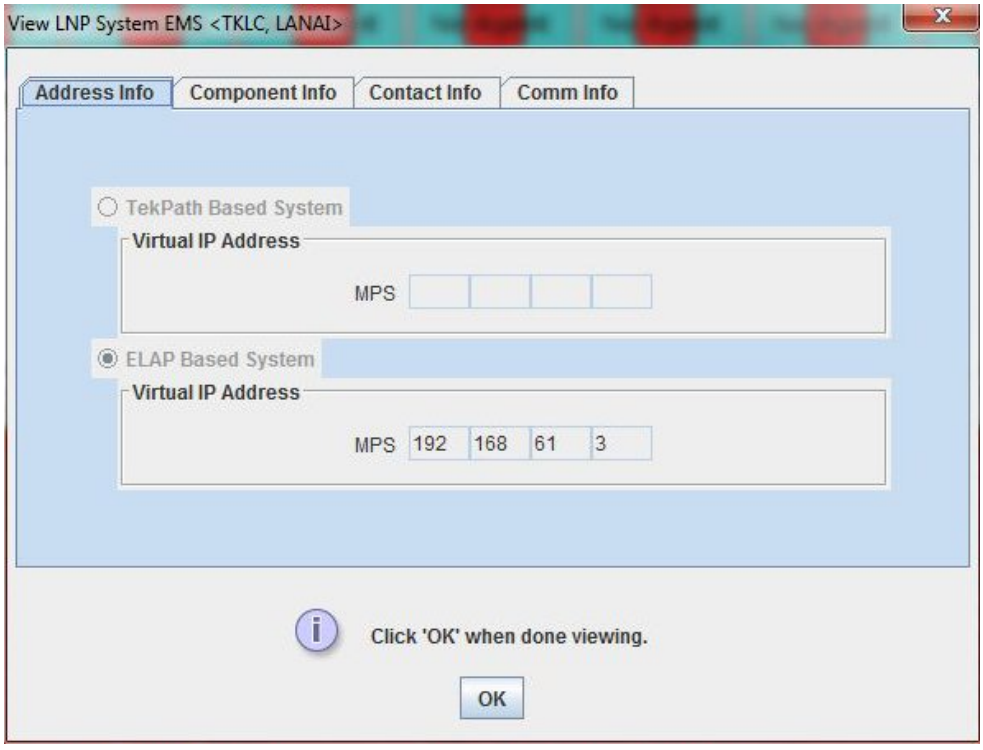
Viewing an EMS Configuration Component

To view EMS configuration component information, use the following procedure.

1. Log into the LSMS as a user in the `lsmsview`, `lsmsuser`, `lsmsuext`, or `lsmsadm` group.
2. Click the **EMS status** icon for the EMS you wish to view (highlight the icon).
3. From the **Main Menu**, select **Configure**, and then **LNP System**, and then **EMS**, and then **View**.

   The View LNP System EMS dialog displays, Figure 3-27.

Figure 3-27 View LNP System EMS Dialog



4. Click on any of the tabs to view additional information.

   For more information about the meaning of the fields on any of the tabs, see Creating an EMS Configuration Component.

> **Note:**
>
> You cannot modify information in any of the tabs.

5. When finished viewing, click **OK**.

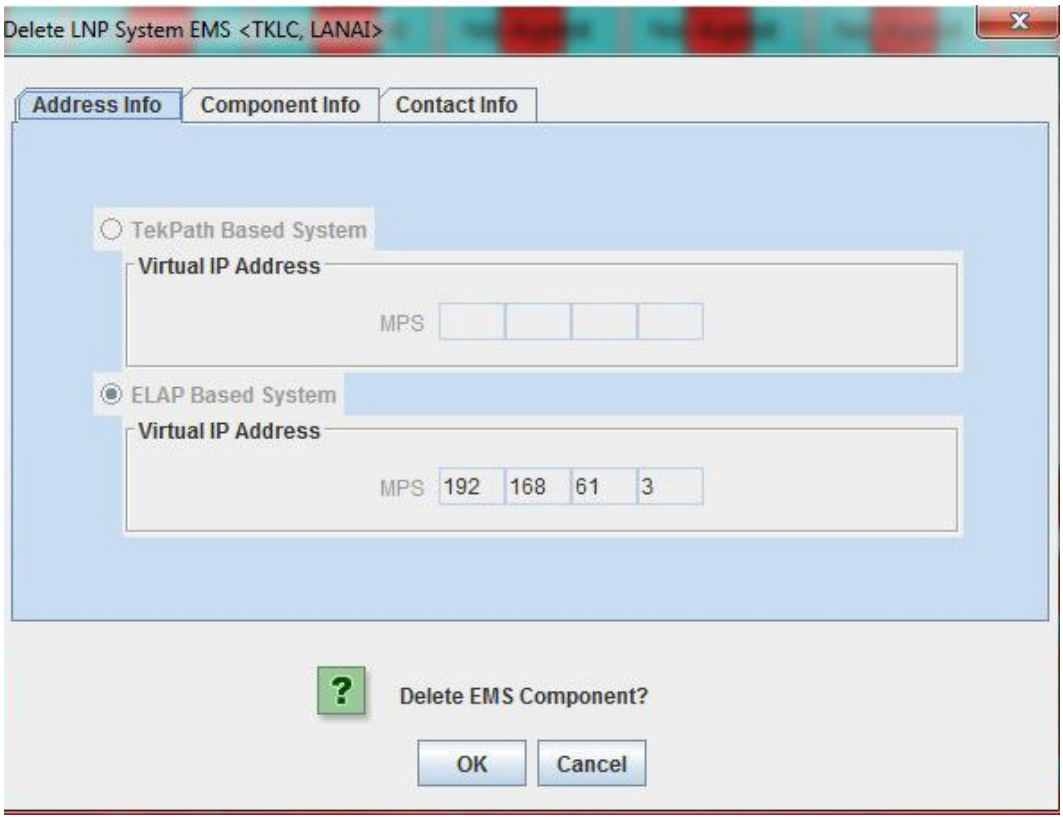
Deleting an EMS Configuration Component

To delete an EMS configuration component, use the following procedure.

1. Log into the LSMS as a user in the `lsmsadm` or `lsmsall` group.
2. Click the **EMS Status** icon for the EMS you wish to delete (highlight the icon).
3. From the **Main Menu**, select **Configure**, and then **LNP System**, and then **EMS**, and then **Delete**.

   The Delete LNP EMS dialog displays, Figure 3-28.

Figure 3-28 Delete LNP System EMS Dialog



4. View the information in this window to verify that this is the EMS you wish to delete.

   Click on any of the tabs to view additional information. For more information about the meaning of the fields on any of the tabs, see Creating an EMS Configuration Component. You cannot modify information in any of the tabs.

5. Click **OK** or **Cancel**.

- If you click **Cancel**, you are returned to the **LSMS** console window.
- If you click **OK**, the Update Successful dialog displays, Figure 3-29.

Figure 3-29 Update Successful Dialog

6. Click **OK**.

Using Key Lists

LSMS maintains a list of keys for each **NPAC** Service Management System. You use a key list to secure encrypted communications between the **LSMS** and its associated **NPACs**.

Key lists are loaded whenever one of the following occurs:

- **LSMS** is initially configured
- The system administrator issues the appropriate key list commands

The **LSMS** system administrator can view any key list in his system. **Key** lists can be exchanged off-line to ensure security. Each key list has an assigned expiration date.

During an **LSMS GUI** session configuration, you load these lists as directed by the **LSMS** system administrator. You must fully configure one **GUI** session (including loading key lists) for each **NPAC** associated with the **LSMS**.

Use the following procedures to generate a key list, load an **NPAC** key list, and load an **LSMS** key list.

- Generating a Key List
- Loading an NPAC Key List
- Loading an LSMS Key List

Generating a Key List

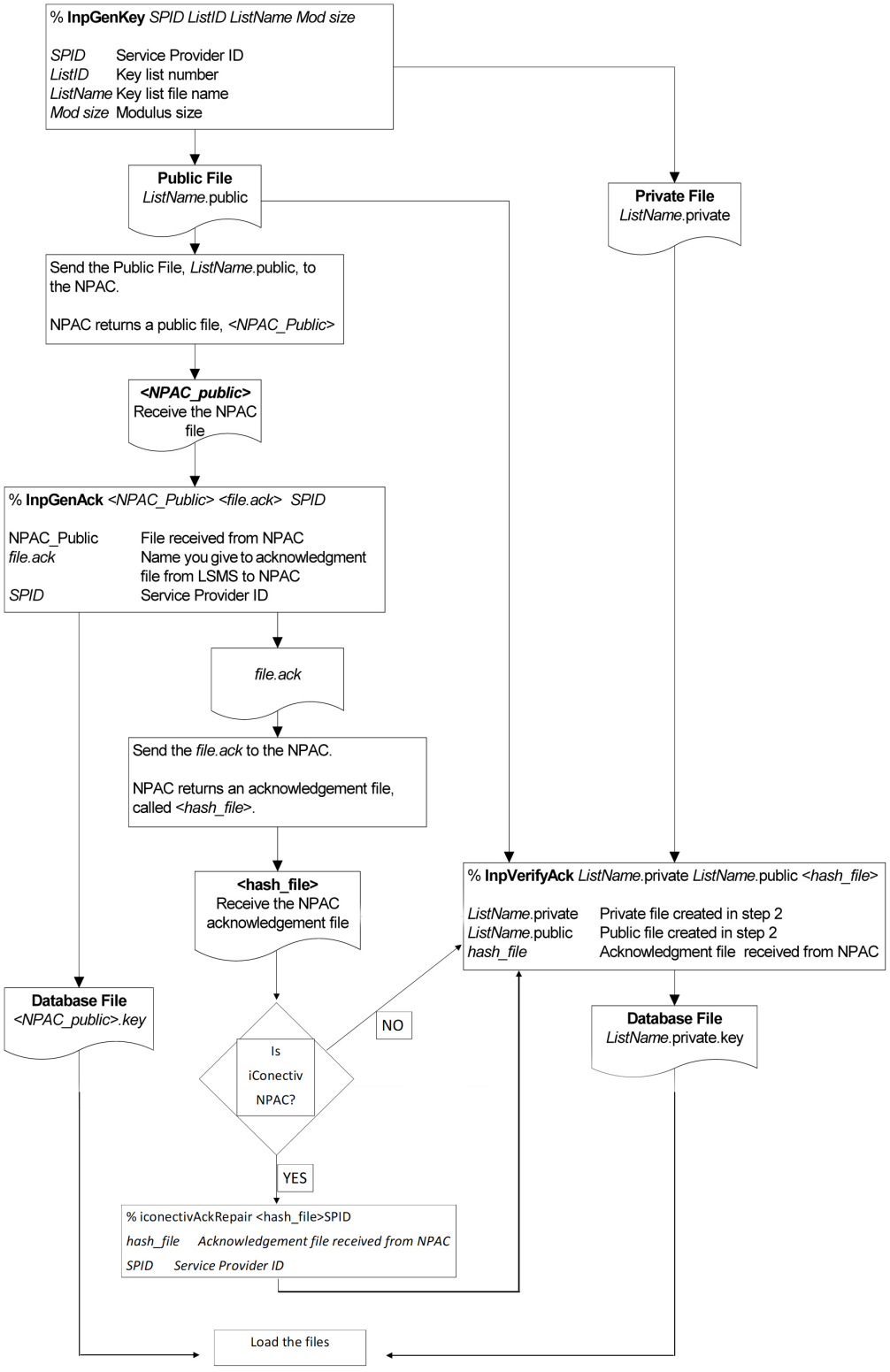
Each **NPAC** and **LSMS** generates a key list for use by the other side. That is, each **NPAC** generates a key list to be transferred to **LSMS** for decrypting the message signature sent from **NPAC**. The **LSMS** generates key lists that are transferred to the **NPAC** for decrypting **LSMS** message signatures sent from **LSMS**.

The keys in a key list are actually the public key component of a private/public key pair. The originating side keeps the private key component for encrypting the signature when transferred to the receiving side.

A key list contains exactly 1000 keys. Before an originating side can communicate with a receiving side, the receiving side must acknowledge the keys within a key list. For example, if **LSMS** sends a set of keys to the **NPAC**, the **NPAC** creates a file with a checksum for each of the 1000 keys in the list. This newly created file can then be used to acknowledge the keys in the list that were sent to the **NPAC**.

The following procedure explains how to generate a key list for the **NPAC**. An overview of the key list creation process is shown below.

Figure 3-30 Flowchart for Generating a Key List



1. Log in to the primary server with a username of `lsmsadm`.

(For information about logging into an **LSMS** server, refer to the *Alarms and Maintenance Guide*)

2. Change to the tools directory:

   ```
   $ cd $LSMS_TOOLS_DIR
   ```

3. Type the `lnpGenKey` command, and use the following instructions.

   ```
   $ ./lnpGenKey <SPID> <ListID> <ListName> <Modulus>
   ```
   where:

   <SPID>
   Service provider **ID**—use the same value as specified for the **NPAC** Customer **SPID** in step 3 in the procedure described in Modifying LSMS Configuration Components.

   <ListID>
   List **ID**—a digit indicating which set of key lists is being created. For the first list use 1, and increment this value by 1 each time you create a new set of key list files.

   <ListName>
   Name of the key list—give the key list a name that helps identify the contents of the files. For example, **KEYLIST_TKLC_2** would identify the resulting files as second key list files created for the service provider **TKLC**.

   <Modulus>
   Modulus size in bytes. Specify one of the following:

   - 80 for 640-bit keys
   - 128 for 1024-bit keys

   This command generates two new files, one for public use and one for private use. For example, if you specified the `<ListName>` as KEYLIST_TKLC_2, you would receive two files called KEYLIST_TKLC_2.public and KEYLIST_TKLC_2.private.

4. Send the public file that was created in the previous step to the **NPAC**. (For example, you would send the **KEYLIST_TKLC_2**.public to the **NPAC**.)

   The key files are binary files. You must use **SFTP** or e-mail facilities to exchange key list files between the **LSMS** and the **NPAC**. You can use the **FTP** client on an **LSMS** server, and **FTP** from **LSMS** to the **NPAC**. If you use **FTP**, be sure to use binary mode so that the files are not corrupted.
   NPAC sends you a corresponding **NPAC** public key file. The **NPAC** determines the actual file name of this file. Store the **NPAC** public key file in the `$LSMS_TOOLS_DIR` directory.

5. Use the `lnpGenAck` command to prepare an acknowledgment of the **NPAC** public key file by typing the following:

   ```
   $ ./lnpGenAck <NPAC_public> <file>.ack <SPID>
   ```
   where, <`NPAC_public`> is the name of the file you received from the **NPAC**, <*file*>.ack is the name of the acknowledgment file you are creating, and < **SPID** > is your service provider **ID**. This command generates two files: an acknowledgment file and a file for the LSMS database.

   Following is an example of the above command:

   ```
   $ ./lnpGenAck NPAC_public TKLC.ack TKLC
   ```

   This command produces an acknowledgment file, called **TKLC**.ack in this example, and a database file, called `<NPAC_public>.key`.

6. Send the **TKLC**.ack to the **NPAC** and receive the corresponding **NPAC** acknowledgment file, called `hash file`, into the `$LSMS_TOOLS_DIR` directory.
7. If NPAC is iconectiv, then repair the NPAC acknowledgment file. If NPAC is not iconectiv, skip to the next step.

   ```
   $ ./iconectivAckRepair <hash_file> <SPID>
   ```
   Where <hash_file> is the acknowledgement file received from the iconectiv NPAC and <SPID> is same as used in step 3.

   This command repairs the iconectiv acknowledgment file and replaces the NPAC region ID with the SPID. Example:

   ```
   $ ./iconectivAckRepair VL07-psel-1.keys.Public.ACK VL07
   ```
8. Verify the received NPAC acknowledgment and generate the private key file with the command below:

   ```
   $ ./lnpVerifyAck <ListName>.private <ListName>.public <hash file>
   ```
   This command generates the second file to be loaded into the database, `<ListName>.private.key`.
9. Copy `<NPAC_public>.key` and `<ListName>.private.key` to /var/TKLC/lsms/free.

   ```
   $ cp <ListName>.private.key <NPAC_public>.key /usr/TKLC/lsms/free
   ```
10. Load the key files to the LSMS GUI. The key files are located in the /var/TKLC/lsms/free directory.

    See "Loading an NPAC Key List" and "Loading an LSMS Key List" for instructions about how to load the key files to the LSMS GUI.

Loading an NPAC Key List

To load an **NPAC** public key list into the **LSMS** database, use either of the procedures described in the following sections:

- Using the keyutil Command to Load an NPAC Key List
- Using the GUI to Load an NPAC Key List

Using the keyutil Command to Load an NPAC Key List

To use the `keyutil` command to load an **NPAC** public key list into the **LSMS** database, use this procedure. Use this command once for the active server; the standby server will be updated with the replicated list automatically.

1. Log into the active server with the user name `lsmsadm`.
2. Enter the following command, where is `<region>` the name of the **NPAC** region and `<NPAC_public>` is the name of the file received from the **NPAC**.

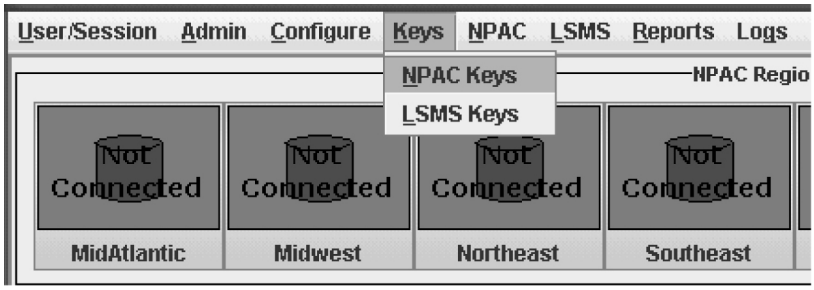
   ```
   $ keyutil -r <region> -k public -l <NPAC_public>.key
   ```

Using the GUI to Load an NPAC Key List

To use the **GUI** to load an **NPAC** public key list into the **LSMS** database, use this procedure.

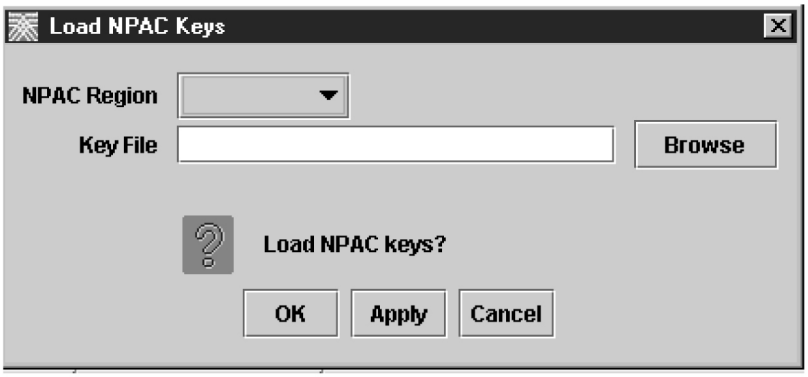
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Keys**, and then **NPAC Keys**.

Figure 3-31 Keys System Menu – Load NPAC



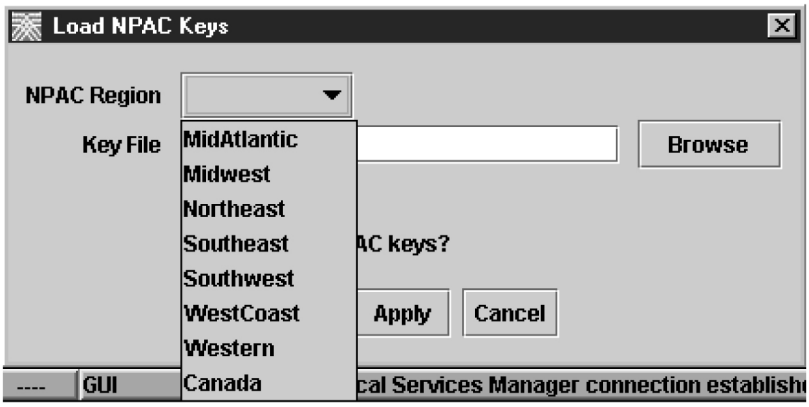
The **Load NPAC Keys** window displays.

Figure 3-32 Load NPAC Keys Window



3. Click the down arrow shown in the **NPAC** Region field to display the regions. Then click the region for which you want to load keys.

Figure 3-33 Load NPAC Keys, Select Region Window



4. Enter the name of the **Key** File that you created in the procedure described in "Generating a Key List".

   (Alternatively, click the **Browse** button to display all the keys files for this region, then click the file name, and then click **Open**; the file name then appears in the **Key** File field.)

5. Click **OK** to load the selected key list file and return to the main **LSMS** console window or click **Apply** to load the selected key list file and keep the Load **NPAC** Keys window open.

Loading an LSMS Key List

To load an **LSMS** public key list into the **LSMS** database, use either of the procedures described in the following sections:

- Using the keyutil Command to Load an LSMS Key List
- Using the GUI to Load an LSMS Key List

Using the keyutil Command to Load an LSMS Key List

To use the `keyutil` command to load an **NPAC** public key list into the **LSMS** database, use the following procedure.

1. Log into the active server as `lsmsadm`.
2. Enter the following command, where is `<region>` the name of the **NPAC** region and `<ListName>` is the name of the private key file generated by the `lnpGenKey` command.

   ```
   $ keyutil -r <region> -k private -l <ListName>.private.key
   ```

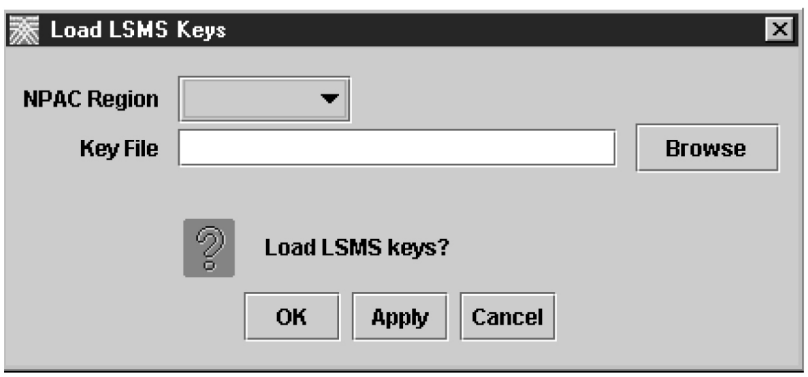
Using the GUI to Load an LSMS Key List

To use the **GUI** to load an **LSMS** private key list into the **LSMS** database, use the following procedure.

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Keys**, and then **LSMS Keys**.

   The **Load LSMS Keys** window displays.

Figure 3-34 Load LSMS Keys Window



3. Click the down arrow shown in the **NPAC** Region field to display the regions.

   Then click the region for which you want to load keys.

Figure 3-35 Load LSMS Keys, Select Region Window

4. Enter the name of the **Key** File that you created in the procedure described in "Generating a **Key** List".

   (Alternatively, click the **Browse** button to display all the keys files for this region, then double-click the desired file name or click the file name, and then click **Open**; the file name then appears in the **Key** File field.)

5. Click **OK** to load the selected key list file and return to the main **LSMS** console window or click **Apply** to load the selected key list file and keep the Load **NPAC** Keys window open.

NPAC Component Configuration

Use the following procedures to manage **NPAC** component configuration:

- Configuring iconectiv NPAC
- Modifying an NPAC Component
- Viewing a Configured NPAC Component
- Removing a Region

Configuring iconectiv NPAC

The iconectiv NPAC compatibility feature makes the LSMS compatible with the iconectiv NPAC. Configurable options allow the user to specify if a region is connected to Neustar or iconectiv NPAC. The default value of the new configuration option is "N" to signify Neustar NPAC. The end user is able to set the value of the new configuration option per region to Y (for iconectiv).

The format is as follows: <Region Name>_ICONECTIV (for example, MIDWEST_ICONECTIV). To enable a region to connect to iconectiv NPAC, complete the following steps:

1. Use the `dbcfginternal` utility and set the corresponding configuration value to yes (Y):

```
$ dbcfginternal <Region Name>_ICONECTIV Y
```

For example, to connect the Midwest region to iconectiv NPAC, set MIDWEST_ICONECTIV to Y:

```
$ dbcfginternal MIDWEST_ICONECTIV Y
Note: npacagent has to be restarted for this feature to take
effect.
Update complete.
```

2. Restart the `npacagent` for the Midwest region as:

```
$ lsms stop Midwest
$ lsms start Midwest
```

There is an audit script to identify the number of NPACs that are connected to iconectiv and Neustar. See *Database Administrator's Guide* for the NPAC Audit Report.

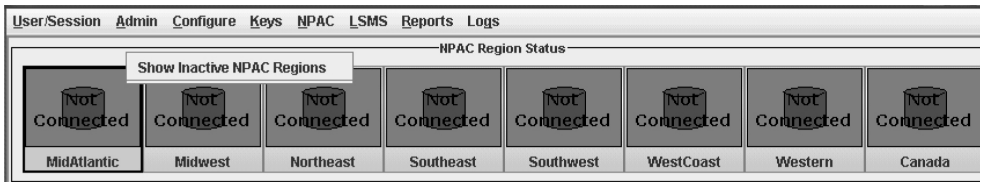
Modifying an NPAC Component

Use the following procedure to create or modify component configuration for an **NPAC**. Create components for both the primary **NPAC SMS** and the secondary **NPAC SMS** of the regional **NPAC**.

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. If you are creating an **NPAC** for the first time, perform this step and step 3.

   (Otherwise, skip to step 4.) Right-click anywhere in the **NPAC** status area; the pop-menu shown in Figure 3-36 displays.

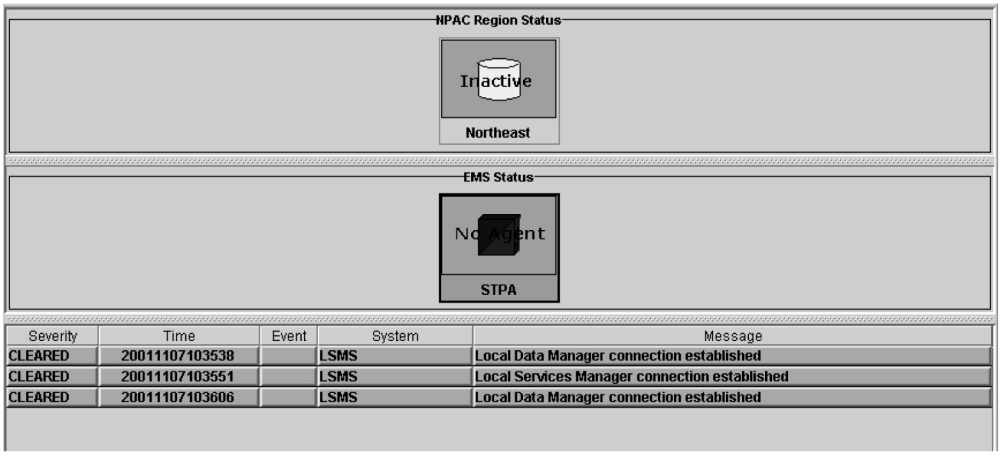
Figure 3-36 Displaying Inactive Regions



3. Click a region for which you have purchased support.

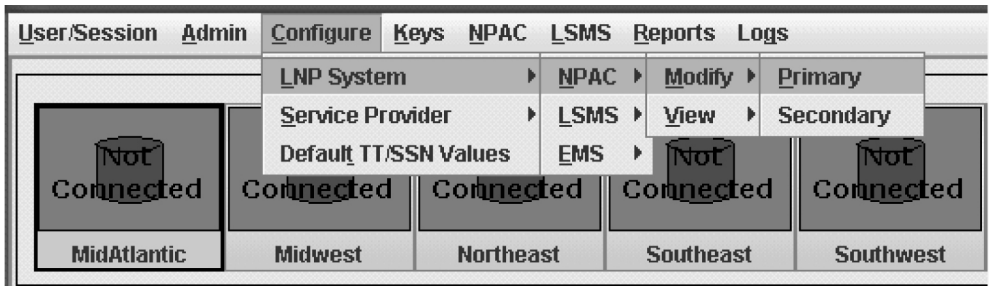
   The main console window displays.

Figure 3-37 NPAC Status Icons Displayed



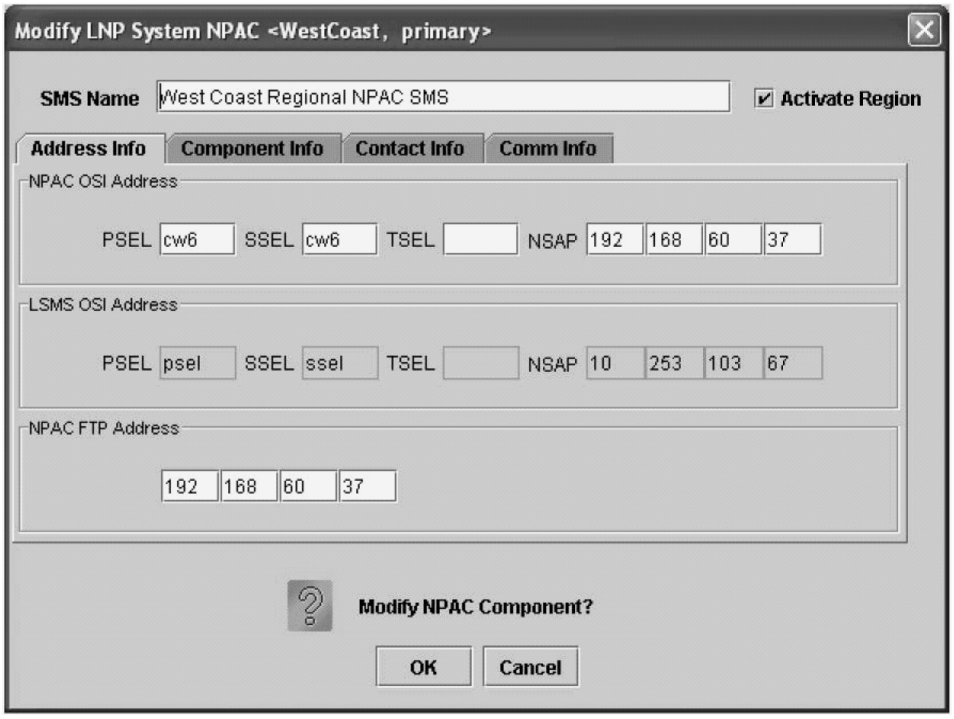
4. Click the icon that represents the **NPAC** you wish to create or modify so that the icon is highlighted.
5. From the main menu, select **Configure**, and then **LNP System**, and then **NPAC** , and then **Modify**, and then **Primary** or **Configure**, and then **LNP System**, and then **NPAC** , and then **Modify**, and then **Secondary**.

Figure 3-38 LNP System Menu – Modify NPAC



The **Modify LNP System NPAC** window displays. In this example, the **Primary** was selected. The window usually opens with the Address Info tab displayed; if the Address Info tab is not displayed, click its tab to display it.

Figure 3-39 Modify LNP System NPAC Address Info Tab



6. Enter the **SMS** Name which represents the name by which the **NPAC** knows this region (maximum of 40 characters)
7. Click the Activate Region checkbox to make this region active.

> **Note:**
>
> Ensure that you have loaded the keys for this region before performing this step. When the Activate Region checkbox is checked, the sentryd process will automatically launch the **NPAC** agent for this region and attempt to associate with the **NPAC**. If the keys have not been loaded, the association will fail.

8. Enter the Address information as follows (all fields in the Address Info tab, except the **TSEL** fields, must contain data):

> **Note:**
>
> Changes on this tab will take effect only after you reassociated with the **NPAC**.

- Enter the **NPAC OSI** Address elements with values that you have obtained from the **NPAC**:
  - **PSEL** – presentation address (one to four alphanumeric characters)
  - **SSEL** – session address (one to four alphanumeric characters)

- **TSEL** – transport address (zero to four alphanumeric characters)
- **NSAP** – network address.
  This value is the **IP** address of the **NPAC**. Example: For an **IP** address of **198.89.35.235**, enter **0xc65923eb**, as shown below:

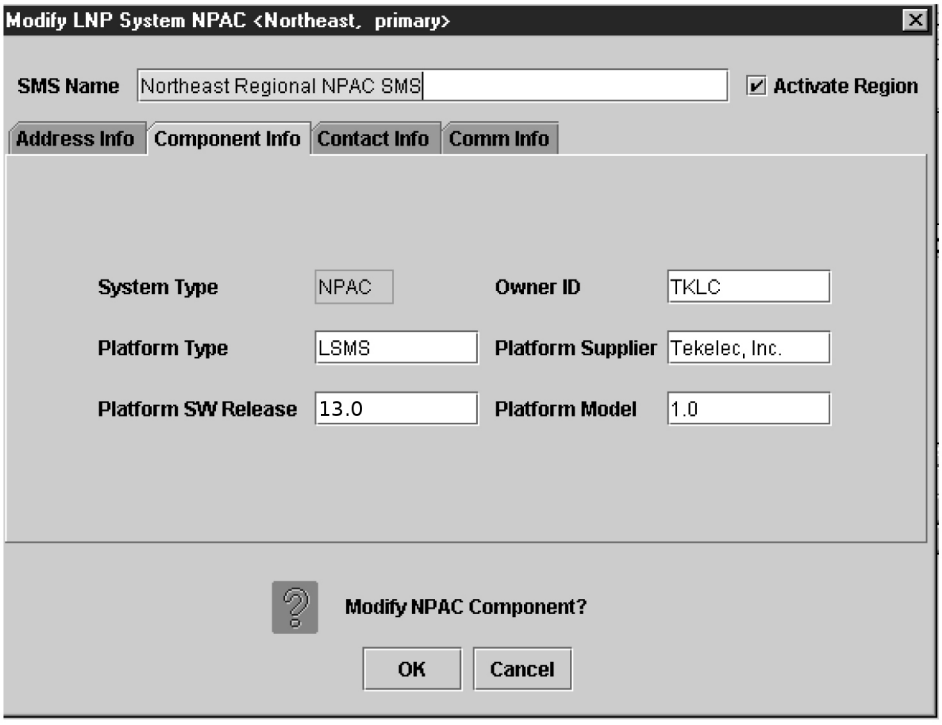
Table 3-3 Decimal to Hexadecimal Conversion

Decimal		198	89	35	235
Hexadecimal	0x	c6	59	23	eb

- The display of the **LSMS OSI** Address elements is for your information (user input is not accepted for these elements):
  - **PSEL** – presentation address (one to four alphanumeric characters)
  - **SSEL** – session address (one to four alphanumeric characters)
  - **TSEL** – this field must be blank
  - **NSAP** – network address. Enter **rk6**
- Enter the **NPAC FTP** address as follows:
  - **FTP** *Address* – the **FTP** address (**IP** address) of this **NPAC** component (enter a value from 0 to 255 in each of the first three octets and a value from 0 to 254 in the fourth octet)

9. Click the Component Info tab.

Figure 3-40 Modify LNP System NPAC Component Info

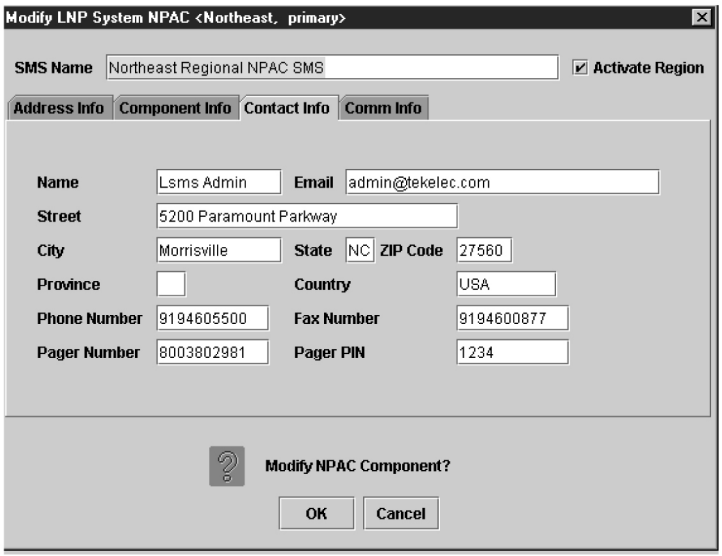


10. Enter the **NPAC** Component Info items as follows (all fields in the Component Info tab must contain data):

- *Owner* **ID** – **ID** of the **NPAC** owner (maximum 20 alphanumeric characters)
- *Platform Type* – hardware platform of the **NPAC** (maximum 20 alphanumeric characters)
- *Platform Supplier* – name of the supplier of the **NPAC** hardware platform (maximum 20 alphanumeric characters)
- *Platform* **SW** *Release* – release level of the software running on the **NPAC** platform (maximum 16 alphanumeric characters): enter 3.0 to connect an **LSMS** region with any **NANC** 3.x compliant **NPAC**
- *Platform Model* – model number of the **NPAC** platform (maximum 20 alphanumeric characters)

11. Click the **Contact Info** tab.

Figure 3-41 Modify LNP System NPAC Contact Info



12. All fields in the Contact Info tab are optional.

    If you wish to enter **NPAC** Contact Info data, do so as follows:

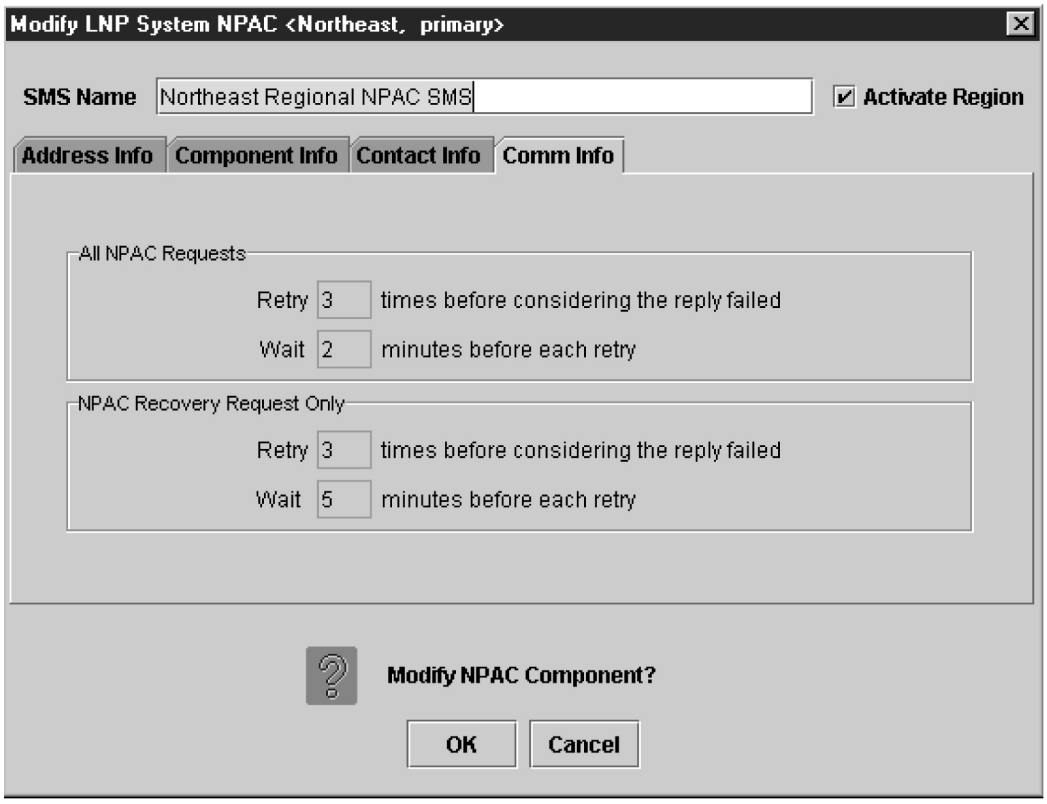
    - *Name* – name of the person to contact for **NPAC** information (maximum 40 alphanumeric characters)
    - *Email* – email address of the **NPAC** contact person (maximum 60 alphanumeric characters)
    - *Street* – street address of the **NPAC** contact person (maximum 40 alphanumeric characters)
    - *City* – city address of the **NPAC** contact person (maximum 20 alphanumeric characters)
    - *State* – state address of the **NPAC** contact person (two-letter uppercase abbreviation).
      If you use the *Province* field, enter **--** into this mandatory field.
    - **ZIP** *Code* – postal zip code of the **NPAC** contact person (five numeric characters)

- *Province* – province of the **NPAC** contact person (two-letter uppercase abbreviation). If you use the *State* field, enter **--** (the default) into this mandatory field.
- *Country* – country of the **NPAC** contact person (maximum 20 alphanumeric characters)
- *Phone Number* – phone number of the **NPAC** contact person (ten numeric characters required)
- **FAX** *Number* – **FAX** phone number of the **NPAC** contact person (ten numeric characters required)
- *Pager Number* – pager number of the **NPAC** contact person (ten numeric characters required)
- *Pager* **PIN** – pager **PIN** number of the **NPAC** contact person (ten numeric characters maximum)

13. The Comm Info tab is for display purposes only to provide the following information.

    You cannot modify these fields.

Figure 3-42 Modify LNP System NPAC Communication Info



- All **NPAC** Requests
  - *Retry*—How many times the **LSMS** will retry a request that the **NPAC** fails to respond to
  - *Retry*—How long the **LSMS** will wait for the **NPAC** respond to a request

- **NPAC** Recovery Request Only
  - *Retry*—How many times the **LSMS** will retry a recovery request that the **NPAC** fails to respond to
  - *Retry*—How long the **LSMS** will wait for the **NPAC** respond to a recovery request

14. When you are finished, click **OK** to apply the changes and return to the **LSMS Console** window.
15. When finished, click **OK** to apply the changes.
    - If the following message appears, click **OK** in the message window and the **GUI** will return to the main console window.

Figure 3-43 Modify Successful

- If a message similar to the following appears, a mandatory field is empty or a field is not properly configured.

Figure 3-44 More Fields Needed

Click **OK** in the message window and correct the appropriate field. Repeat this step until the message in Figure 3-43 displays.

> **Note:**
>
> If you changed values on the Address Info tab, you must abort and reassociate the **NPAC** association in order for the modifications to take effect.

You have now completed this procedure.

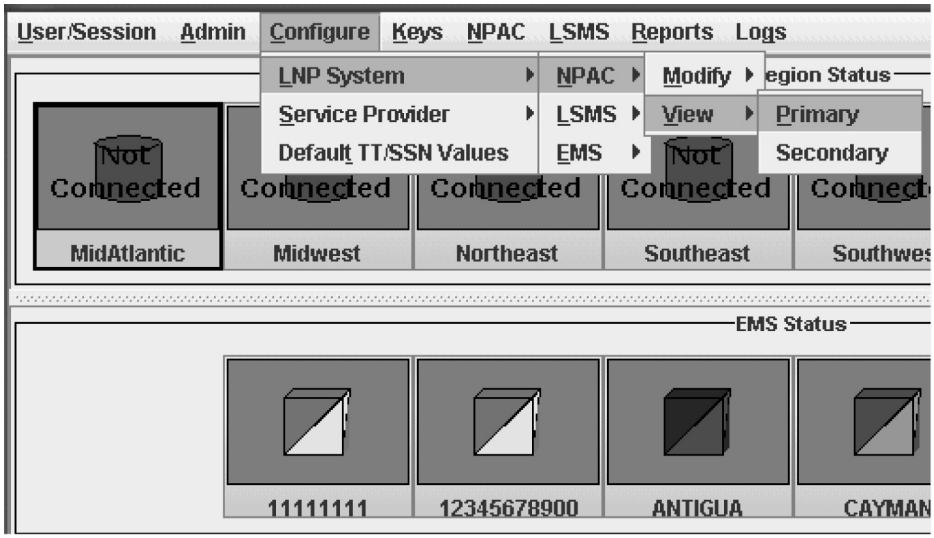
Viewing a Configured NPAC Component

To view configured **NPAC** component information, use the following procedure.

1. Log in as a user in the `lsmsadm`, `lsmsuser`, `lsmsuext`, `lsmsview`, or `lsmsall` group.

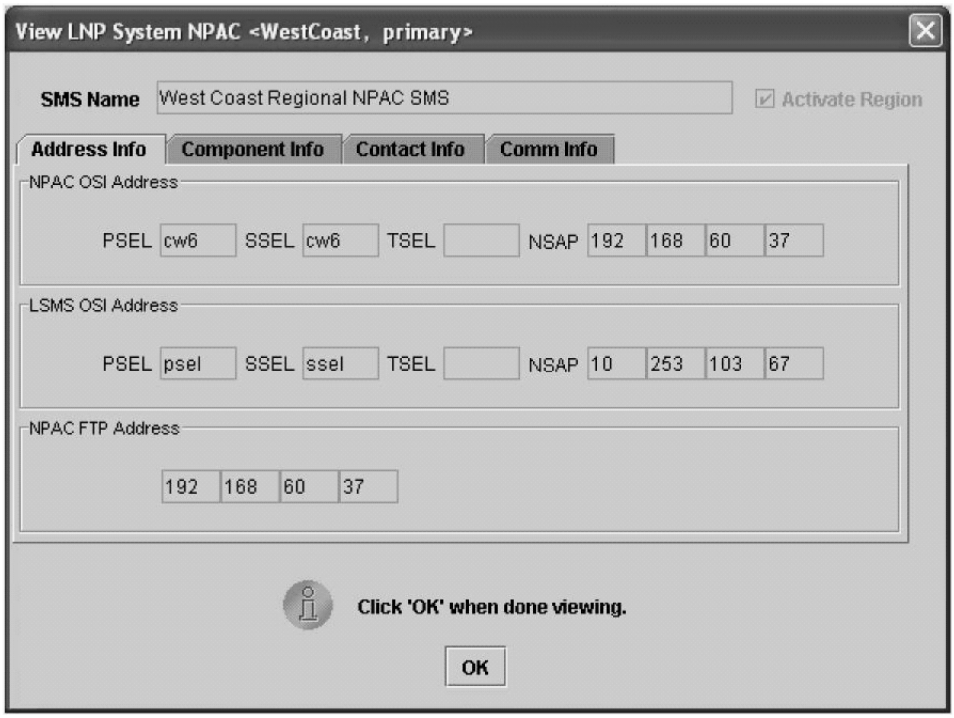
2. Click the icon that represents the **NPAC** you wish to view so that the icon is highlighted.
3. From the main menu, select **Configure**, and then **LNP System**, and then **NPAC** , and then **View**, and then **Primary** or **Configure**, and then **LNP System**, and then **NPAC** , and then **View**, and then **Secondary**.

Figure 3-45 LNP System Menu – View NPAC



The **View LNP System NPAC** window displays. In this example, the **Primary** was selected. The window usually opens with the Address Info tab displayed.

Figure 3-46 View LNP System NPAC Window



4. To view a different tab, click on the tab.

   For information about the fields displayed in any of the tabs, see their description in the procedure defined in “Modifying an **NPAC** Component”.

5. When finished viewing this window, click **OK** to return to the main **LSMS** console window.

Removing a Region

> **Note:**
>
> All the examples are shown for the Southeast region. Southeast can be replaced with <Region name>, which you want to remove.

Perform the following steps to remove a region from the LSMS system:

1. Verify that the NPAC database exists for the region that we want to delete using the following command:

```
$ lsmsdb -c counts | grep Southeast
0 ............. SoutheastDB.NumberPoolBlock
0 ............. SoutheastDB.ServiceProvLRN
0 ............. SoutheastDB.ServiceProvNPA_NXX
0 ............. SoutheastDB.ServiceProvNPA_NXX_X
2 ............. SoutheastDB.ServiceProvNetwork
0 ............. SoutheastDB.SubscriptionVersion
7 ............. supDB.SoutheastNpacMeasurements
1,000 ......... supDB.SoutheastPrivateKey
1,000 ......... supDB.SoutheastPublicKey
```

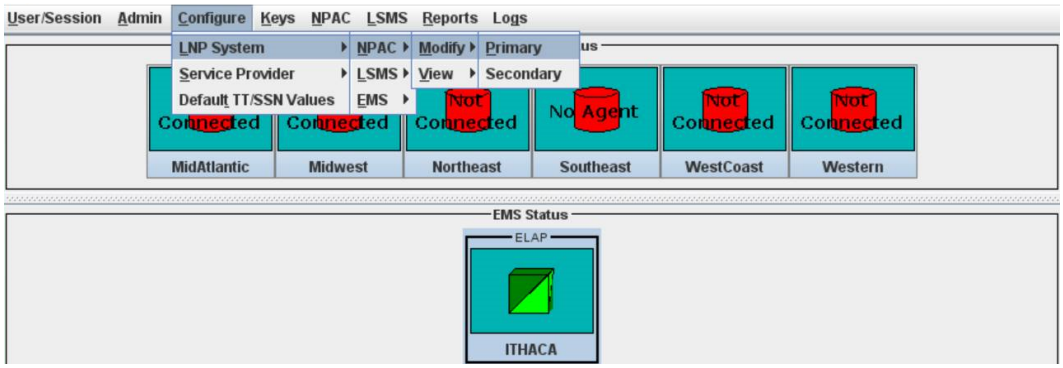
2. Stop the region using the following command:

```
$ lsms stop Southeast

Checking if npacagent is running....Yes.

Stopping npacagent....
OK.

npacagent stopped:  Wed Aug  4 08:16:02 2021

Command complete.
```

3. Deactivate the region from the LSMS GUI:

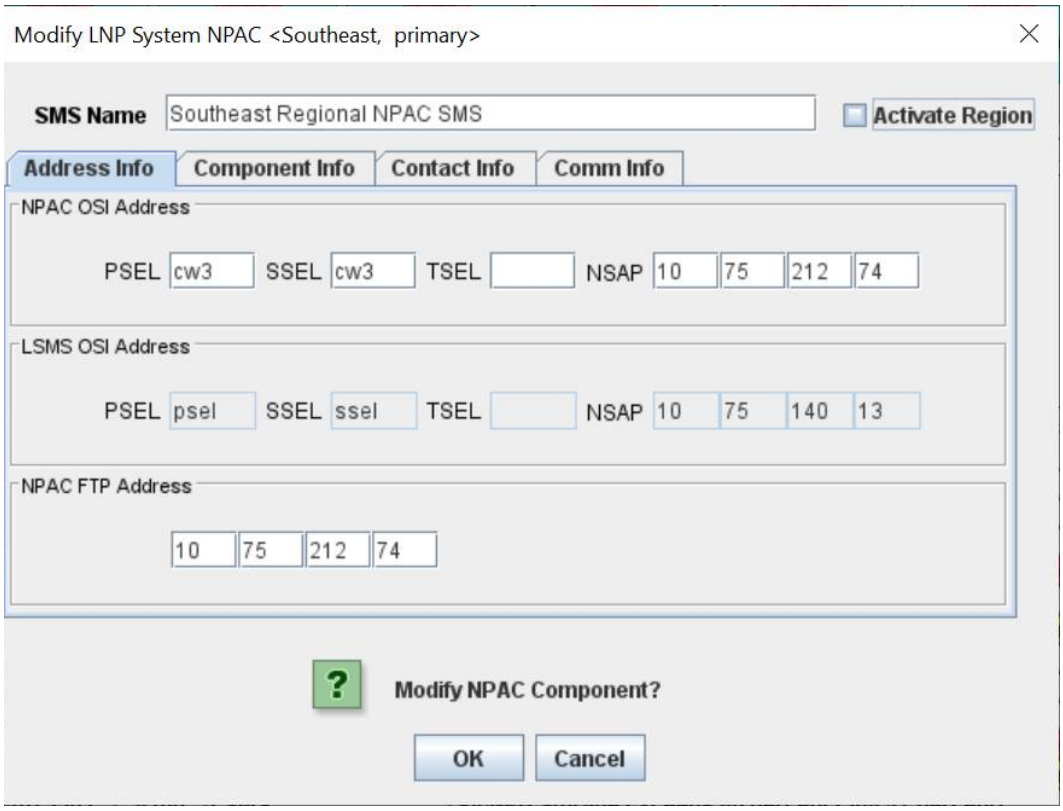
   Modify the NPAC configuration:

Figure 3-47 LSMS Console



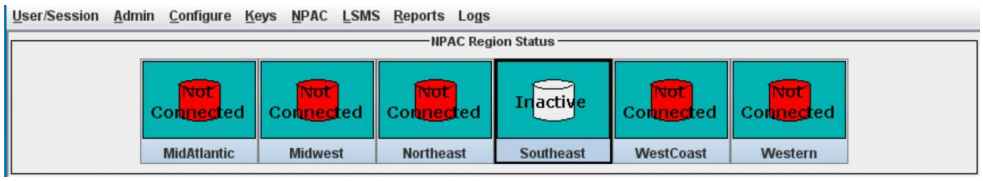
Uncheck **Activate region** and press **OK**

Figure 3-48 Modify LNP System NPAC



The NPAC region status will get changed to **Inactive**.

Figure 3-49 NPAC Region Status



4. Delete the NPAC database for the region using the following command:

```
$ npac_db_setup remove Southeast
------------------------------------------------------------
NPAC Region Database Setup Script

The Region Database name is SoutheastDB

WARNING: NPAC region database SoutheastDB is about to be removed.
        All data in this database will be lost.
        Do you want to continue? [Y/N]Y

Removing NPAC region database ...SoutheastDB
```

5. Verify that the NPAC database is deleted for the region using the following command:

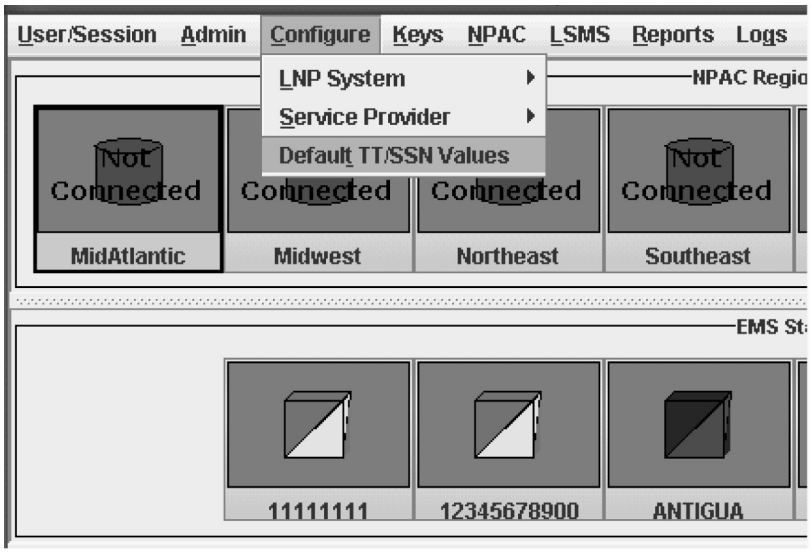
```
$ lsmsdb -c counts | grep Southeast
7 ............. supDB.SoutheastNpacMeasurements
1,000 ......... supDB.SoutheastPrivateKey
1,000 ......... supDB.SoutheastPublicKey
```

Modifying Default TT/SSN Values

If desired, use the following procedure to modify the default **Translation Type** (**TT**) and **SS7 Subsystem Number** (**SSN**) values for a given **GTT** group. Using default settings can simplify the amount of data entry required when creating Default **GTTs** and Override **GTTs** (for information about managing Default **GTTs** and Override **GTTs**, refer to the *Database Administrator's Guide*).

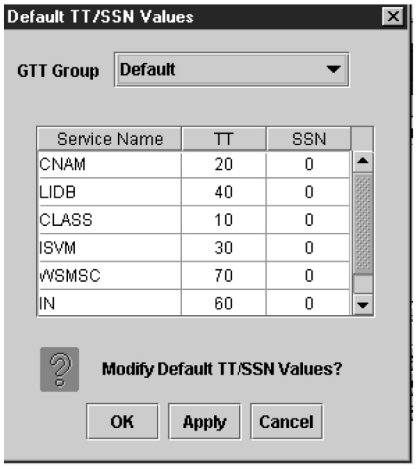
1. Log in as a user in the `lsmsadm`, `lsmsall`, or `lsmsuext` group (if you are logging in as a user in the `lsmsuext` group, you are authorized to modify only Default **TT**/**SSN** values for **GTT** groups that are assigned to the **SPID** you used when you logged in).
2. From the main menu, select **Configure**, and then **Default TT/SSN**.

Figure 3-50 Modify Default TT/SSN Values



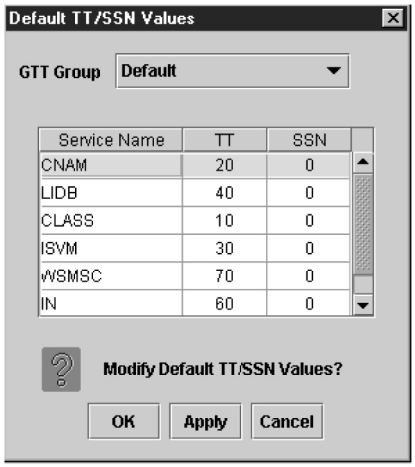
The **Default TT/SSN Values** window displays.

Figure 3-51 Default TT/SSN Values Window



3. If the **GTT** Group whose default values you wish to modify is not displayed in the **GTT** Group field, click the down arrow at the right of the field and select the desired **GTT** Group.
4. To change any **TT** or **SSN** value, click in the desired table cell; the cell is highlighted while the rest of the row displays in a darker shade, as shown in the example in Figure 3-52.

Figure 3-52 Changing Default TT/SSN Values



The **TT** and **SSN** values must be as follow:

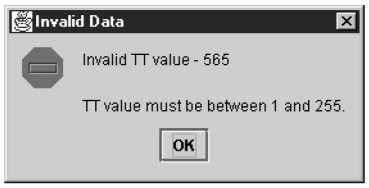
- **TT** —Range 1–255
- **SSN** —Range 0–255, excluding 1 (0 indicates no **SSN** translation)

5. Repeat 4 for any other **TT** or **SSN** values that you wish to change.
6. When you are finished, click **Apply** to apply the changes and stay in this window, or click **OK** to apply the changes and return to the **LSMS Console** window.
   - If the following message appears, click **OK** in the message window and the **GUI** will return either to the Default **TT**/**SSN** Values window or to the main console window.

Figure 3-53 Modify Successful

- If a message similar to the following appears, a mandatory field is empty or a field is not properly configured.

Figure 3-54 More Fields Needed



Click **OK** in the message window and correct the appropriate field. Repeat this step until the message in Figure 3-53 displays.

Working with NPAC Associations

Ordinarily, **NPAC** associations are managed automatically by the *sentry* utility, according to the setting of the Activate Region checkbox in the Modify **LNP** System **NPAC** window (see Figure 3-39). This section explains how to manually create or abort **NPAC** associations. You can use the **LSMS GUI** interface to perform both of these procedures. You can also use the command line utility, *lsmsclaa*, to create and abort **NPAC** associations.

The following topics are covered in this discussion of the **NPAC** associations:

- Creating an NPAC Association
- Aborting an NPAC Association

Creating an NPAC Association

To create an **NPAC** association with the **LSMS**, see either of the following:

- "Creating an NPAC **Association** Using GUI"
- "Creating an NPAC Association Using Command-Line Interface"

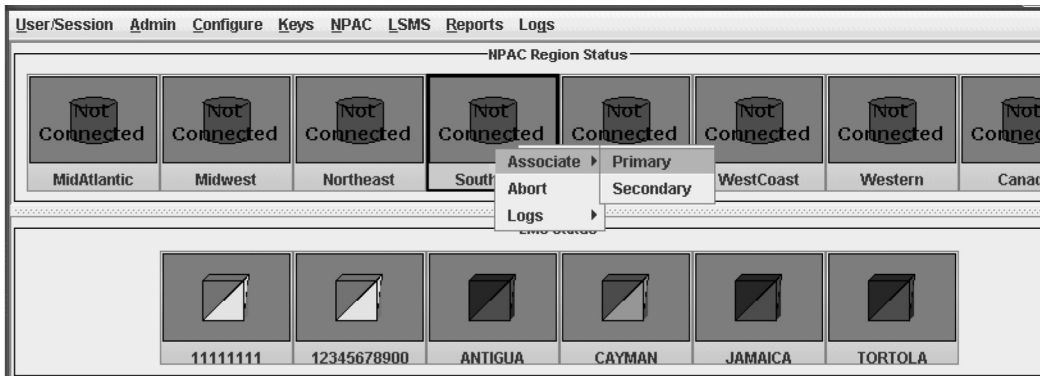
For either procedure, you must be logged in to the **LSMS** as an lsmsadm or lsmsall user.

Creating an NPAC Association Using GUI

To create an **NPAC** association with the **LSMS** using the **GUI**, perform the following procedure:

1. Log in to **LSMS** as a member of the permission group that is authorized to perform this operation.
2. Click the icon that represents the **NPAC** that you wish to associate with; then right-click and select **Associate**.

Figure 3-55 Associate with NPAC



When the **LSMS** has finished associating with the **NPAC**, the **NPAC** status icon displays the text "Associated."

Creating an NPAC Association Using Command-Line Interface

To create an **NPAC** association with the **LSMS** using the optional command-line interface, perform the following procedure:

1. Ensure that the command-line interface was started for the region to association with by a user logged in as `lsmsadm` or `lsmsall` (for more information about starting the command-line interface, see "Starting the Command Line Interface").

   The following prompt indicates that the command-line interface is started:

   ```
   Enter command ->
   ```

2. Enter the following at the command-line interface prompt:`Enter Command -> ASSOCIATE <NPAC>`

   where `<NPAC>` is either **PRIMARY** or **SECONDARY**. The command-line interface utility translates this value to the proper **NPACID**.The command-line interface displays a message to indicate whether the association was successful. For more information about the possible messages, refer to the *Alarms and Maintenance* manual.

3. If desired, you can verify the association by entering the following commands:

   - Exit the command-line interface by entering the following command:
     `Enter Command -> EXIT`

     The standard Linux prompt appears.

   - Verify the status of the association by entering the following command, where `<REGION>` is the same value as you used to start the command-line interface:
     `$LSMS_DIR/lsms status <REGION>`

   Output similar to the following example indicates that the association was successful:

   ```
   Checking if npacagent is running....Yes.
   npacagent Canada: mem= 24424 kbytes : pcpu 0.0 %
   Log Directory: /usr/LSMS/logs/Canada
   Connected to primary NPAC
   Command complete.
   ```

Aborting an NPAC Association

The abort function breaks the association attempt between the **LSMS** and the **NPAC** by transmitting the *abort* command to the **NPAC**.

To abort an **NPAC** association attempt, see either of the following:

- "Aborting an **NPAC Association** Using **GUI**"
- "Aborting an **NPAC Association** Using Command-Line Interface"

For either procedure, you must be logged in to the **LSMS** as an `lsmsadm` or `lsmsall` user.

Aborting an NPAC Association Using GUI

To abort an **NPAC** association with the **LSMS** using the **GUI**, perform the following procedure:

1. Log in to **LSMS** as a member of the permission group that is authorized to perform this operation.
2. Click the icon that represents the **NPAC** whose association you wish to abort; then right-click and select **Abort**.
3. When the **LSMS** has finished aborting the association with the **NPAC**, the **NPAC** status icon displays the text “Not Connected.”

Aborting an NPAC Association Using Command-Line Interface

To abort an **NPAC** association with the **LSMS** using the optional command-line interface, perform the following procedure:

1. Ensure that the command-line interface was started for the region to abort the association with by a user logged in as `lsmsadm` or `lsmsall` (for information about starting the command-line interface, see “Starting the Command Line Interface”).

   The following prompt indicates that the command-line interface is started:

   ```
   Enter command ->
   ```

2. Enter the following at the command-line interface prompt:

   ```
   Enter Command -> ABORT
   ```

3. The command-line interface displays a message to indicate whether the abort was successful.

   For more information about the possible messages, refer to the *Alarms and Maintenance Guide*.

4. If desired, you can verify the aborted association by entering the following commands:

   - Exit the command-line interface by entering the following command:
     ```
     Enter Command -> EXIT
     ```
     The standard Linux prompt appears.
   - Verify the status of the association by entering the following command, where `<REGION>` is the same value as you used to start the command-line interface:
     ```
     $LSMS_DIR/lsms status <REGION>
     ```

     ```
     Checking if npacagent is running....Yes.
     npacagent Canada: mem= 24424 kbytes : pcpu 0.0 %
     Log Directory: /usr/LSMSlogs/Canada
     No connection to NPAC.
     Command complete.
     ```

Postfix

Postfix is an alternative mail program to the Sendmail program.

> **Note:**
>
> The Postfix **daemon** must be restarted manually after any operation that causes the host to reboot. Postfix is disabled by default.

The normal configuration of Postfix requires **DNS** (**Domain** Name System). Postfix uses fully qualified hostnames for source and destination resolution.

> **Note:**
>
> The Postfix configuration affects only the local server.

The following topics are covered in this discussion of Postfix.

- Configuring Postfix.
- Starting and Stopping Postfix
- Postfix Online Help

Configuring Postfix

Modifications to the Postfix configuration files or aliases database require the Postfix utility to be restarted. To configure Postfix, perform the following procedure:

> **Caution:**
>
> Loss of data can result if you do not properly configure Postfix. For technical assistance, call the Customer Care Center.

1. Add the **LSMS** host to the private **DNS** space.
2. To configure Postfix, the `/etc/resolv.conf` file needs to be modified if the nameserver is needed to resolve hostnames.

   Here is an example of `/etc/resolv.conf` modifications.

Table 3-4 Table of Domain and Name Server Addresses

Information Type	Sample Addresses
`domain`	`nc.tekelec.com`
`nameserver`	`10.20.1.11`

3. The Postfix `main.cf` configuration file specifies a small subset of all parameters that control the operation of the Postfix mail system.

   Parameters not explicitly specified remain at their default values. The main.cf file, which is self-documenting, requires a fully qualified hostname. Table 3-5 shows the minimum required settings for the `/etc/postfix/main.cf` configuration file parameters.

Table 3-5 Table of Postfix Configuration Parameters

Parameter	Sample Addresses
`myhostname`	`localhost`
`#myhostname`	`virtual.domain.tld`
`inet_interfaces`	`all` (or specific network Ethernet port)
`mydestination`	`lsmspri.localhost`
relayhost	smtp.tekelec.com
#relayhost	$mydomain
#relayhost	[gateway.my.domain]
#relayhost	[mailserver.isp.tld]
#relayhost	uucphost
#relayhost	[an.ip.add.ress]
(optional)	

4. When you have performed the previous steps and recorded the indicated information, you have completed the required parameters.

   You may specify optional parameters if desired. Call the Customer Care Center for assistance, if needed.

> **Note:**
>
> For complete Postfix details, refer to the *man* pages on the **LSMS** system.

Starting and Stopping Postfix

To start Postfix, use this command:

```
# /usr/sbin/postfix start
```

To stop Postfix, use this command:

```
# /usr/sbin/postfix stop
```

> **Note:**
>
> The user must be `root` to start and stop Postfix.

Postfix Online Help

Refer to the following Internet address for Postfix online help:

http://www.postfix.org

4
Configuring the NAS

This section provides steps for initial configuration of the Oracle Communications LSMS Network Attached Storage (NAS), which is performed on the LSMS server.

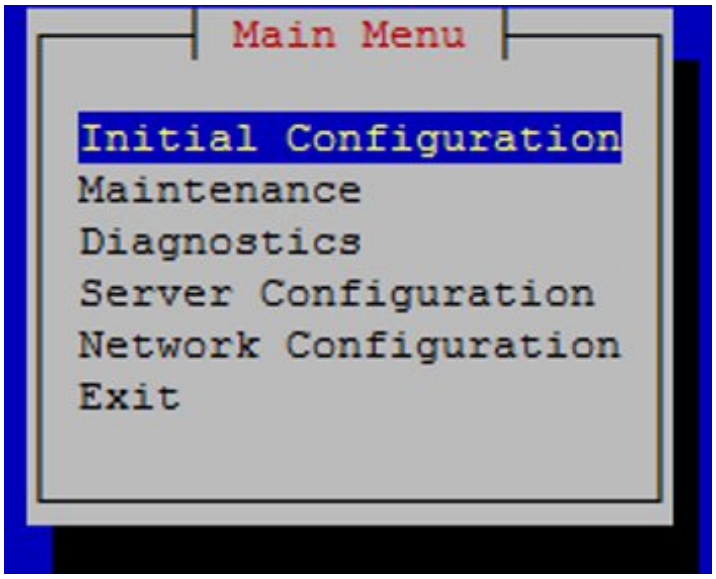
Initial Configuration

The Oracle Communications LSMS Network Attached Storage (NAS) configuration is performed on the LSMS server through the `lsmsmgr` utility.

The initial configuration is performed on the LSMS server after the fresh installation. If the NAS is connected with the LSMS for the first time, or the TPD has been re-installed on the NAS, the initial configuration is required for the NAS. The NAS will be configured initially through the primary LSMS using tty serial terminal.

1. From the `lsmsmgr` menu, select the **Initial Configuration** option.

Figure 4-1 User Interface Main Menu



2. Select **yes** for **Run All** option if all configuration scripts are to be executed. Otherwise, select **no** and then select the configuration scripts.

Figure 4-2 Select Running Option

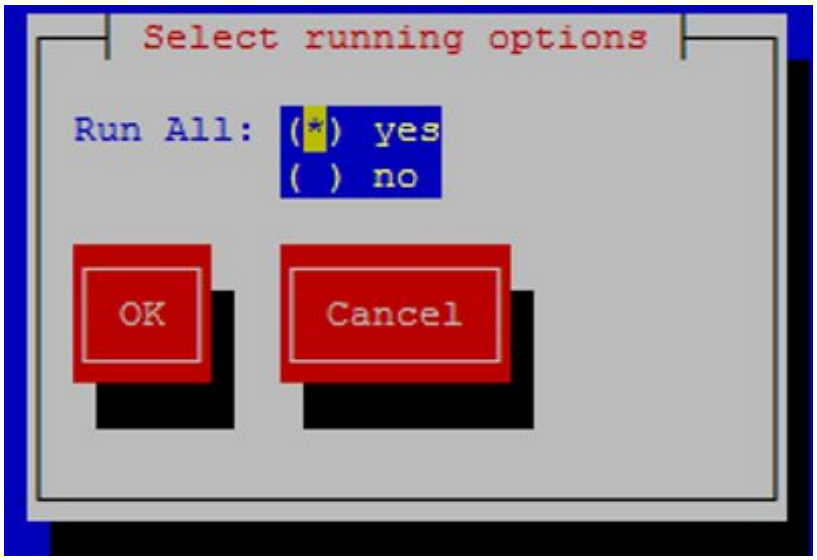
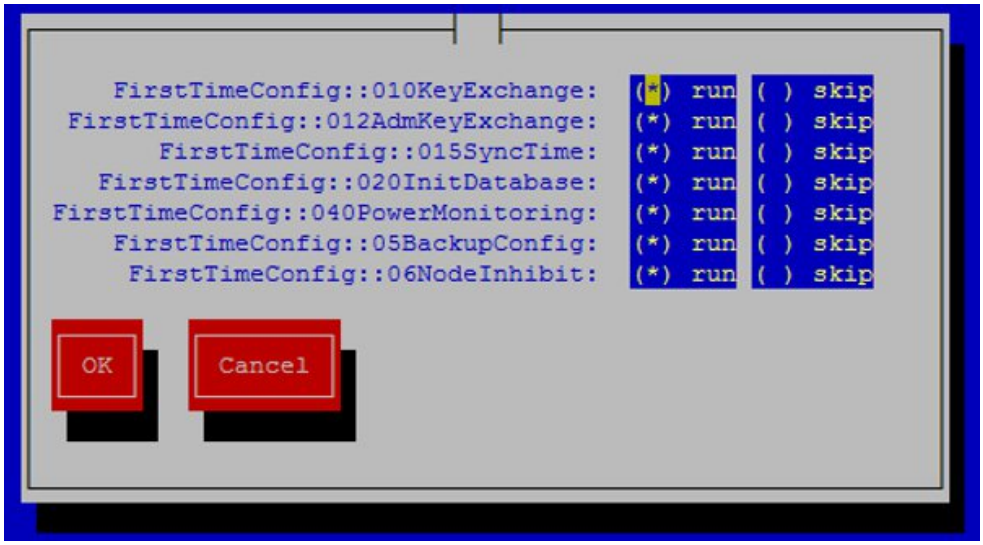


Figure 4-3 Select Configuration Option



3. The number of backups scheduled on the NAS is currently 4. The `configBackup` script allows the user to reduce the number of backups ranging from 2 to 4 by entering the following command:

   ```
   configBackup [status] [<number of backups>]
   ```

   Where [status] displays the number of backups configured and <number of backups> is a number from 2 to 4.

5

Configuring Optional Features

This chapter describes configuration procedures that need to be performed one time only for various optional features.

Introduction

Other chapters in this book describe the configuration activities that you must perform to get the **LSMS** up and running. This chapter describes configuration procedures that need to be performed one time only for various optional features. Some optional features must be activated and configured before you perform the configuration procedures described in Completing Configuration and Starting Connections

Understanding How to Activate and Configure Optional Features

Starting with LSMS 13.0, all optional features are now customer configurable.

Some optional features do not require activation or additional configuration; those features are not described in this manual.

Increase Maximum Allowed SPID Procedure

Standard **LSMS** support allows you to configure up to 32 **SPID**s for supported service providers; support for additional **SPID**s, in groups of 16, can be enabled. To increase the maximum allowed SPID, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal MAX_SPIDS <new spid limit>`.

   Where `<new spid limit>` is a number from 32 to 512 in increments of 16.
3. The value of MAX_SPIDS will be updated in the database. LSMS software will allow customers to configure additional service provider IDs.

Enable Number Pooling EDR

Number Pooling Efficient Data Representation (EDR) allows ported telephone numbers to be assigned to supported service providers in blocks of 1000. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal EDR <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of EDR will be updated in the database.

4. For each region that starts sending of EDR object, modify NPAC configuration and set NPAC platform release to 3.0 or higher. LSMS will now start requesting EDR objects as part of NPAC recovery procedure.
5. Shutdown the instances of the LSMS Npacagent using the command:

   ```
   $ lsms stop <region Name>
   ```
6. LSMS is now ready to accept new EDR objects (NumberPoolBlock and NPA-NXX-X) from NPAC.
7. Notify NPAC region administrator to initiate sending of EDR objects.
8. Receive bulk data download files from NPAC for NumberPoolBlocks and use import utility to import Number pool data in to regional database
9. Restart the instances of the LSMS Npacagent using the command:

   ```
   $ lsms start <region Name>
   ```
10. Repeat step 5 through 9 for each region as they become EDR capable.

Enable Remote Monitoring

Remote monitoring allows the **LSMS** to report certain events to up to five remote locations. To enable this feature, perform this procedure:

> **Note:**
>
> See *Database Administrator's Guide* for additional information.

1. Login to the ACTIVE LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal SNMP <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of SNMP will be updated in the database.
4. Use the LSMS GUI to configure the NMS. See "Configuring the SNMP Agent" in *LSMS Alarms and Maintenance* for more information.
5. Create $LSMS_DIR/../config/snmp.cfg configuration file to configure the location/address of SNMP manager application.
6. Issue the command:

   ```
   scp $LSMS_DIR/../config/snmp.cfg
   lsmsadm@<STANDBY_LSMS>:$LSMS_DIR/../config/
   ```
7. Execute "sentry register -n1 lsmsSNMPagent -pl"

LSMS begins sending traps to the SNMP manager application when events enabled for traps occur.

Enable Automatic File Transfer

Automatic File Transfer allows the user to schedule automatic transfers of specified files. To enable this feature, perform this procedure:

> **Note:**
>
> See *Database Administrator's Guide* for additional information.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal AFT <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of AFT will be updated in the database.

Enable Reception of WSMSC data from NPAC

Wireless Short Message Service Center (WSMSC) Support allows the **LSMS** to store **WSMSC** data received from NPACs and forward WSMSC data to network elements (**NE**s) that have had the equivalent feature activated. To enable this feature, perform this procedure:

> **Note:**
>
> In order to receive WSMSC data from the NPAC, the customer must also update their user profile with the NPAC to include transmission of WSMSC data.

> **Note:**
>
> See *Database Administrator's Guide* for additional information.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal WSMSC <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of WSMSC will be updated in the database.
4. Stop and restart each NPAC Agent for each region.

LSMS is now ready to receive WSMSC data from NPAC and store it in the regional database.

Enable Sending of WSMSC data to EAGLE

Wireless Short Message Service Center (WSMSC) Support allows the **LSMS** to store **WSMSC** data received from NPACs and forward WSMSC data to network elements (**NE**s) that have had the equivalent feature activated. To enable this feature, perform this procedure:

> **Note:**
>
> See *Database Administrator's Guide* for additional information.

1. Ensure all EAGLEs connected with LSMS are capable of receiving WSMSC data.

2. Login to the LSMS as `lsmsadm`.
3. Issue the command `dbcfginternal WSMSC_TO_EAGLE <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
4. The value of WSMSC_TO_EAGLE will be updated in the database.
5. Stop and restart each NPAC Agent for each region.

LSMS will now forward WSMSC data to EAGLEs.

Update Maximum Supported GUI Users

Support for additional users allows up to 25 simultaneous users. This feature has a prerequisite of the Enabling IP GUI feature. To increase the maximum supported users, perform this procedure:

> **Note:**
>
> For more information, see Support of Multiple Users.

1. As "root" user, use the `syscheck` command to determine that the necessary hardware is available to support the new user limit.
2. Login to the LSMS as `lsmsadm`.
3. Issue the command `dbcfginternal MAX_USERS <new user limit>`.

   Where <new user limit> is 8 to 25.
4. The value of MAX_USERS will be updated in the database.

LSMS will now allow additional GUI sessions.

Enable Enhanced Filtering

Enhanced LSMS Filters allows the user to filter data to be sent to **NE**s by NPAC region or by GTT group. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal ENHANCED_FILTERS <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of ENHANCED_FILTERS will be updated in the database.

The user can now use the Enhanced Filtering feature as described in *Database Administrator's Guide*.

Update Maximum Supported EAGLE pairs

Support for additional EAGLE pairs allows up to 16 pairs. To increase the maximum supported EAGLES, perform this procedure:

1. Login to the LSMS as `lsmsadm`.

2. Issue the command `dbcfginternal MAX_EAGLES <new EAGLE pair limit>`.

   Where <new EAGLE pair limit> is a number from 8 to 16.

3. The value of MAX_EAGLES will be updated in the database.

LSMS will now allow configuration of additional EMSes.

Enable Report Generator

Report Generator allows the user to create a wide variety of reports beyond those available through the **LSMS GUI**. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal REPORT_GEN <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.

3. The value of REPORT_GEN will be updated in the database.

The user is now capable of using the Report Generator feature as described in *Database Administrator's Guide*.

Enable NANC 3.2 Enhancements Feature

The NANC 3.2 Enhancements Feature enhances the recovery download functionality of the NpacAgent, providing increased flexibility and efficiency in the recovery mechanism, as well as enhanced capabilities of Bulk Data Download (BDD) and mass updates of SPIDs. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal NANC_3_2_ENHANCEMENTS <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.

The user can now perform all NANC 3.2 functionality.

Enable Customizable Login Message Feature

The Customizable Login Message Feature supports the display of a customized login message for Linux and **GUI** logins. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal LOGIN_MSG <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.

3. The login message text must be added to the `/etc/issue` file by editing this file as "root" user.

The user can now perform all functionality described in the "Logging Into the LSMS Console Window" section in *Alarms and Maintenance Guide*.

Enable Log Time for Successful EAGLE Response Feature

The Log Time for Successful EAGLE Response Feature supports the recording of timestamps for successful EAGLE responses. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal LOG_EAGLE_SUCCESS_RESP <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of LOG_EAGLE_SUCCESS_RESP will be updated in the database.
4. Restart each running EAGLEagent for changes to take effect.

Now the EAGLEagent will start (for "Y") /stop (for "N") recording the timestamp for successful EAGLE response in the Translog.

Enable ResyncDB Query Server Feature

The ResyncDB Query Server feature enables the LSMS to directly host the ResyncDB Query Server. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal RESYNCDB_QUERY_SERVER <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of RESYNCDB_QUERY_SERVER will be updated in the database.

After setting the values to "Y," the ResyncDB Query Server can now be configured according to procedures contained in the Query Server Feature Technical Reference, TR005579.

Configure/Update LSMS Quantity Keys

LSMS Quantity Keys support the modification of `lsmsdb` capacity from 120 million to 756 million. To enable this feature, perform this procedure:

> **Note:**
>
> The SERVDI feature will be automatically enabled upon the update of an LSMS quantity key to a value greater than 228. After SERVDI is automatically enabled, the feature will not be available within a GUI instance until the GUI is restarted.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal MAX_RECORDS <new LSMS Quantity Limit>`.

   Where <new LSMS Quantity Limit> is a number from the set of 120, 132, 144, 156, 168, 180, 192, 204, 216, 228, 240, 252, 264, 276, 288, 300, 312, 324, 336, 348, 360, 372, 384, 396, 408, 420, 432, 444, 456, 568, 480, 492, 504, 516, 528, 540, 552, 564, 576, 588, 600, 612, 624, 636, 648, 660, 672, 684, 696, 708, 720, 732, 744 and 756.
3. If the following prompts are displayed, answer "yes" to each (these are only displayed if the LSMS Quantity Keys are being set for the first time on the system):

   MAX_RECORDS does not exist. Add it?
4. The value of MAX_RECORDS will be updated in the database.

Enable Support ELAP Reload Via Database Image (SERVDI)

SERVDI performs BDDs that significantly reduces the time needed to reload an ELAP database. To enable this feature, perform this procedure:

> **Note:**
>
> Once SERVDI is activated, the feature will not be available within a GUI instance until the GUI is restarted.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal SERVDI_ENABLED <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. If the following prompt is displayed, answer "yes" to it (this is only displayed if the SERVDI feature is being set for the first time on the system and an entry is not already in the supported database):

   SERVDI_ENABLED does not exist. Add it?
4. The value of SERVDI_ENABLED will be updated in the database.
5. Stop and restart each LSMS GUI from which an SERVDI load will be initiated.

LSMS is now ready to initiate SERVDI loads to ELAP.

SERVDI Process

SERVDI has the following utilities:

- `lsms2ridb` - the default utility invoked when SERVDI is initiated from the LSMS GUI. This utility generates the SERVDI image for the 756M schema and is only compatible with ELAP 10.2 and later. If executed with ELAP 10.1, the file generation will be successful at the LSMS, but the restoration of that SERVDI file/image will fail on ELAP.
- `lsms2ridb_504m` - the default utility invoked when SERVDI is initiated from the LSMS GUI. This utility generates the SERVDI image for the 504M schema and is only compatible with ELAP 10.1 and later. If executed with ELAP 10.0, the file generation will be successful at the LSMS, but the restoration of that SERVDI file/image will fail on ELAP.
- `lsms2ridb_384m` - this utility generates the SERVDI image for the 384M schema and is only compatible with ELAP 10.0. If executed with ELAP 10.1 or later, the file generation will be successful at the LSMS, but the restoration of that SERVDI file/image will fail on ELAP. The user invokes this process through the command line by executing the following command:

1. Login to the LSMS as `lsmsadm`.
2. Enter `$ lsms2ridb_384M ---zip ---system lsms ---clli <CLLI Name> ---ofile /var/TKLC/lsms/free/data/servdi/<SERVDI file name>`.

   Where the SERVDI file name format is as follows:

   `servdiDownload_<LSMS server hostname>_<YYYYMMDDhhmmss>`

Enable NANC 3.3 Feature Set

The **NANC** 3.3 Feature Set provides new capabilities for recovery, notifications, application level error codes, recovery of **SPID**, and support for the “Service Provider Type” field. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal NANC_3_3_FEATURE_SET <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of NANC_3_3_FEATURE_SET will be updated in the database and, if enabled, then two features which depend only on this setting will be enabled, namely the Notifications bulk data download file (NANC 3.3 Change Order 348) and the recovery of SPID data (NANC 3.3 Change Order 352, except Canada (see Enable SPID Recovery Feature). Other features depend on this and another setting (see Enable Service Provider Type Feature, Enable SWIM Recovery Feature, Enable NANC 3.3 Error Codes Feature, and Enable SPID Recovery Feature).

Enable Service Provider Type Feature

The Service Provider Type Feature supports . To enable this feature, perform this procedure:

> **Note:**
>
> This feature can only be enabled if the NANC 3.3 Feature Set has already been enabled.

1. Contact NPAC to agree on a time for them to change the Service Provider Type LSMS Indicator.
2. As that time approaches, make sure there are **no** regions currently associated with NPAC.
3. Login to the LSMS as `lsmsadm`.
4. Issue the command `dbcfginternal SERVICE_PROV_TYPE <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
5. The value of SERVICE_PROV_TYPE will be updated in the database.
6. Verify with NPAC that the Service Provider Type Indicator has been changed to match that value.
7. Re-associate npacagents with NPAC.

LSMS can now accept the Service Provider Type field in Service Provider messages from NPAC if it is set to "Y."

Enable SWIM Recovery Feature

The SWIM Recovery Feature supports enabling the SWIM (Send What I Missed) based recovery from NPAC as an alternative to time based recovery. To enable this feature, perform this procedure:

> **Note:**
>
> This feature can only be enabled if the NANC 3.3 Feature Set has already been enabled.

1. Contact NPAC to agree on a time for them to change the SWIM Recovery Indicator.
2. As that time approaches, make sure **all** regions used by your LSMS system are associated with NPAC.
3. Login to the LSMS as `lsmsadm`.
4. Issue the command `dbcfginternal SWIM_RECOVERY <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
5. The value of SWIM_RECOVERY will be updated in the database.
6. Verify with NPAC that the SWIM Recovery Indicator has been changed to match that value.

Now the recovery will be SWIM-based if is is set to "Y."

Enable NANC 3.3 Error Codes Feature

The NANC 3.3 Error Codes Feature supports updating the database for the values of two sets of errors, i.e., `ERROR_CODES_FOR_ACTIONS` and `ERROR_CODES_FOR_NON_ACTIONS`. To enable this feature, perform this procedure:

> **Note:**
>
> This feature can only be enabled if the NANC 3.3 Feature Set has already been enabled.

1. Contact NPAC to agree on a time for them to change both the "Lsms Action Application Level Errors Indicator" and the "LSMS Non-Action Application Level Errors Indicator."
2. If this feature will be enabled, obtain the file containing the error code data from the NPAC and put the file in the `/var/TKLC/lsms/free/data/npacftp` directory.
3. As that time approaches, make sure that there are **no** regions currently associated with NPAC.
4. Login to the LSMS as `lsmsadm`.
5. Issue the command `dbcfginternal NANC_3_3_ERROR_CODES <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.

6. If you are enabling this feature, the command will prompt for the name of the file containing the error code data.
   - If you are enabling this feature, enter the error code file name.
   - If you are enabling this feature, enter the password of "lsmsadm" at the mate LSMS server.
7. The values for both ERROR_CODES_FOR_ACTIONS and ERROR_CODES_FOR_NON_ACTIONS will be updated in the database.
8. Verify with NPAC that both the "LSMS Action Application Level Errors Indicator" and the "LSMS Non-Action Application Level Errors Indicator" have been changed to match that value.
9. Restart all npacagents to use the new values and associate with NPAC. If enabled, then application level error codes will be displayed using the corresponding error text from the error code file.

Increase Verify Npacagent Timeout

Verify Npacagent Timeout allows you to configure the timeout value if data or latency on the server is in excess and npacagent cannot start within a timeout of 10 seconds (default).

To increase the timeout, perform the following procedure:

1. Login to LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal VERIFY_NPAC_AGT_TIMEOUT <new timeout vaue>` where `<new timeout value>` is an integer from 10 to 300 in an increasing order of 1.

   The value of `VERIFY_NPAC_AGT_TIMEOUT` is updated in the database.

Configuring a Network Time Protocol Client

Number Portability Administration Centers (**NPACs**) require that the system time at the **LSMS** be within five minutes of the **NPAC** time. If the times are not within five minutes of each other, the following **GUI** notification is likely to be posted:

```
[Critical]:  <Timestamp> 2003: NPAC <primary|secondary> Connection
Aborted by PEER : Access Control Failure
```

To synchronize the time between the **LSMS** and **NPACs**, you can configure the **LSMS** as an industry-standard Network Time Protocol (**NTP**) client that communicates with one or more **NTP** servers elsewhere in your network. **NTP** is an Internet protocol used to synchronize clocks of computers to Universal Time Coordinated (**UTC**) as a time reference. In **NTP**, a time server's clock is read, and the reading is transmitted to one or more clients, with each client adjusting its clock as required.

If you choose to implement the **LSMS** as an **NTP** client, you must set up one or more **NTP** servers in your own network (or synchronize with some portion of the existing **NTP** subnet that runs on the Internet) and configure the **LSMS** to contact those **NTP** servers. (If you prefer not to configure the **LSMS** as an **NTP** client, you can manually reset the **LSMS** time when it drifts out of synchronization with the **NPAC** time.)

Understanding Universal Time Coordinated

Universal Time Coordinated (**UTC**) is an official standard for determining current time. The **UTC** second is based on the quantum resonance of the cesium atom. **UTC** is more accurate than Greenwich Mean Time (**GMT**), which is based on solar time.

The term universal in **UTC** means that this time can be used anywhere in the world; it is independent of time zones. To convert **UTC** to your local time, add or subtract the same number of hours as is done to convert **GMT** to local time.

The term coordinated in **UTC** means that several institutions contribute their estimate of the current time, and the **UTC** is calculated by combining these estimates.

UTC is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks. Special-purpose receivers are available for many time-dissemination services, including the Global Position System (**GPS**) and other services operated by various national governments.

Generally, it is too costly and inconvenient to equip every computer with a **UTC** receiver. However, it is possible to equip a subset of computers with receivers; these computers in turn disseminate the time to a larger number of clients connected by a common network. Some of those clients can also disseminate the time, in which case they become lower stratum servers. The industry-standard Network Time Protocol is an implementation of this time dissemination method.

Understanding the Network Time Protocol

The Network Time Protocol (**NTP**) is an Internet protocol used to synchronize clocks of computers using **UTC** as a time reference. **NTP** primary servers provide their clients time accurate within a millisecond on a **Local Area Network** (**LAN**) and within a few tens of milliseconds on a Wide Area Network (**WAN**). This first level of dissemination is called stratum-1. At each stratum, the client can also operate as a server for the next stratum.

A hierarchy of **NTP** servers is defined with stratums to indicate how many servers exist between the current server and the original time source external to the **NTP** network, as follows:

- A stratum-1 server has access to an external time source that explicitly provides a standard time service, such as a **UTC** receiver.
- A stratum-2 server receives its time from a stratum-1 server
- A stratum-3 server receives its time from a stratum-2 server
- And so on; the **NTP** supports up to 15 strata

Normally, client workstations that do not operate as **NTP** servers and **NTP** servers with a relatively small number of clients do not receive their time from a stratum-1 server. At each stratum, it is usually necessary to use redundant **NTP** servers and diverse network paths in order to protect against broken software, hardware, or network links.

NTP works in one or more of the following association modes:

- Client/server mode, in which a client receives synchronization from one or more servers, but does not provide synchronization to the servers
- Symmetric mode, in which either of two peer servers can synchronize to the other, in order to provide mutual backup

- Broadcast mode, in which many clients synchronize to one or a few servers, reducing traffic in networks that contain a large number of clients. **IP** multicast can be used when the **NTP** subnet spans multiple networks.

The **LSMS** supports only client/server mode and functions as a client.

Obtaining an NTP Server

The most important factor in providing accurate, reliable time is the selection of modes and **NTP** servers to be used in your **NTP** configuration file. It is recommended that you configure at least three stratum-2 or stratum-3 **NTP** servers.

Specifying three or more **NTP** servers allows the protocol to apply an agreement algorithm to detect insanity on the part of any one of the servers. Normally, when all **NTP** servers are in agreement, the protocol chooses the best available server, where the best is determined by a number of factors, including the lowest stratum number, lowest network delay, and claimed precision.

Many public and private **NTP** servers are currently running on the Internet. If you do not already have an **NTP** server in your network, you can obtain synchronization services from some portion of the **NTP** subnetwork that runs on the Internet. However, you may want to consider creating your own **NTP** server so that you can more carefully control security and reliability. If you need to create an **NTP** server, refer to the following resources for more information:

- The following Internet sites:
  - http://docs.sun.com (search for **ntp**, or choose the *Network Time Protocol User's Guide*)
  - http://www.ntp.org

Verifying NTP Service

Use the following procedure to verify that the time server is working.

- Log in to lsmspri as `root` and enter the following command:

  ```
  $ ntpdate -q ntpserver1
  ```

  - If the time server is working, output similar to the following displays:

    ```
    server 198.89.40.60, stratum 2, offset 106.083658, delay 0.02632
    22 May 14:23:41 ntpdate[7822]: step time server 198.89.40.60
    offset 106.083658 sec
    ```

  - If the time server is not working or is unavailable, output similar to the following displays:

    ```
    server 198.89.40.60, stratum 0, offset 0.000000, delay 0.000000
    22 May 14:33:41 ntpdate[7822]: no server suitable for
    synchronization found
    ```

Configuring the LSMS to Use an NTP Server

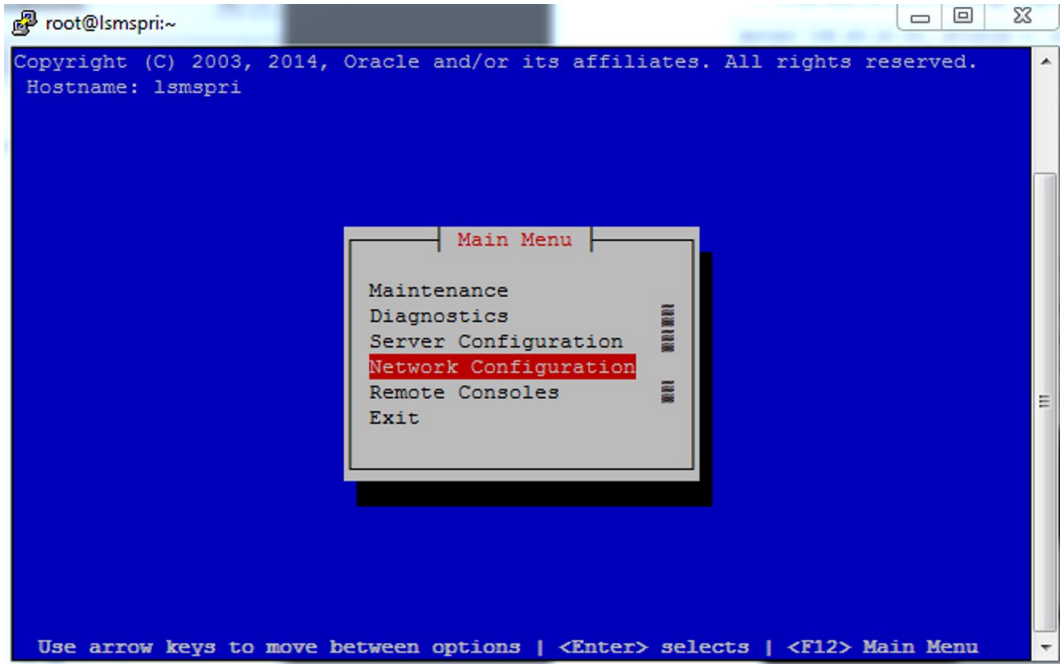
To add an **NTP** server to the **LSMS** configuration, perform this procedure:

1. Log in to the active server with username `lsmsmgr`.

   (For more information about logging into a server, refer to Using Login Sessions.)

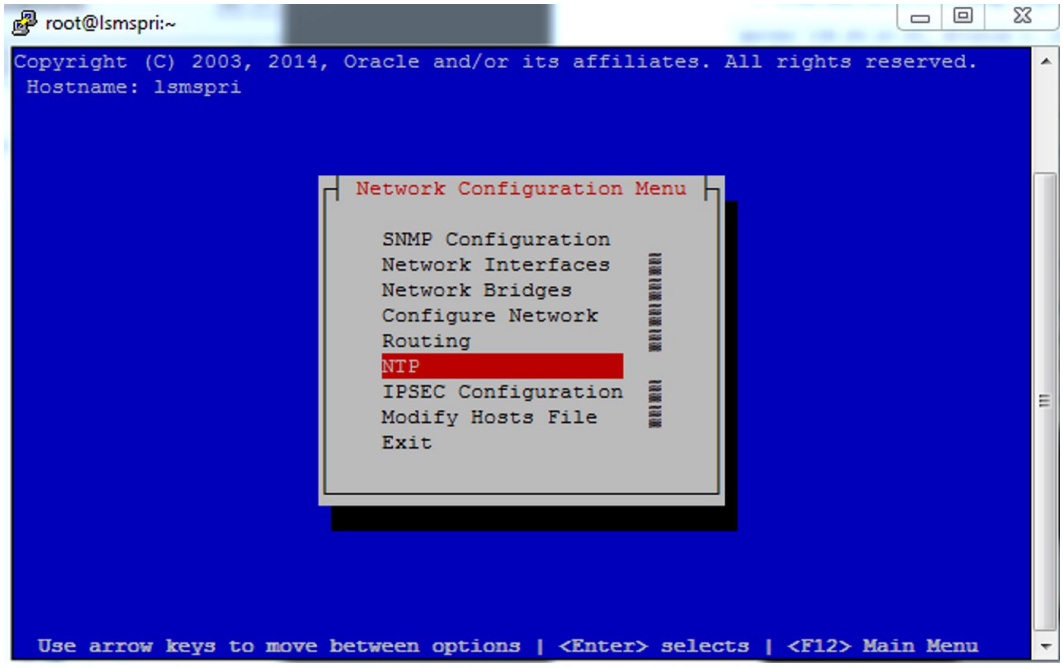
2. From the **Main Menu**, select **Network Configuration** and press **Enter**.

Figure 5-1 Selecting the Network Configuration Menu



3. From the **Network Configuration Menu**, select **NTP** and press **Enter** to select the network time protocol screen.

Figure 5-2 Selecting the NTP Menu

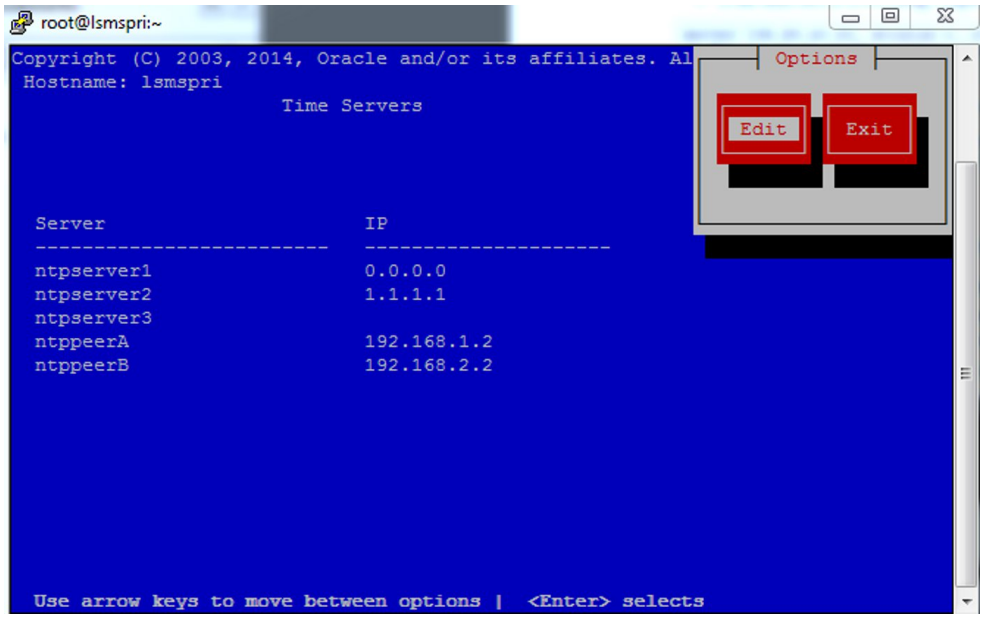


4. The Time Servers screen displays the **NTP** servers available to the **LSMS**.

   Examine the screen for available **NTP** servers. In the sample figure, `ntpserver2` is available as the **NTP** server to select. Click the **Edit** button to define an **NTP** server for this **LSMS**.

> **Note:**
>
> Do not change any netpeer address.

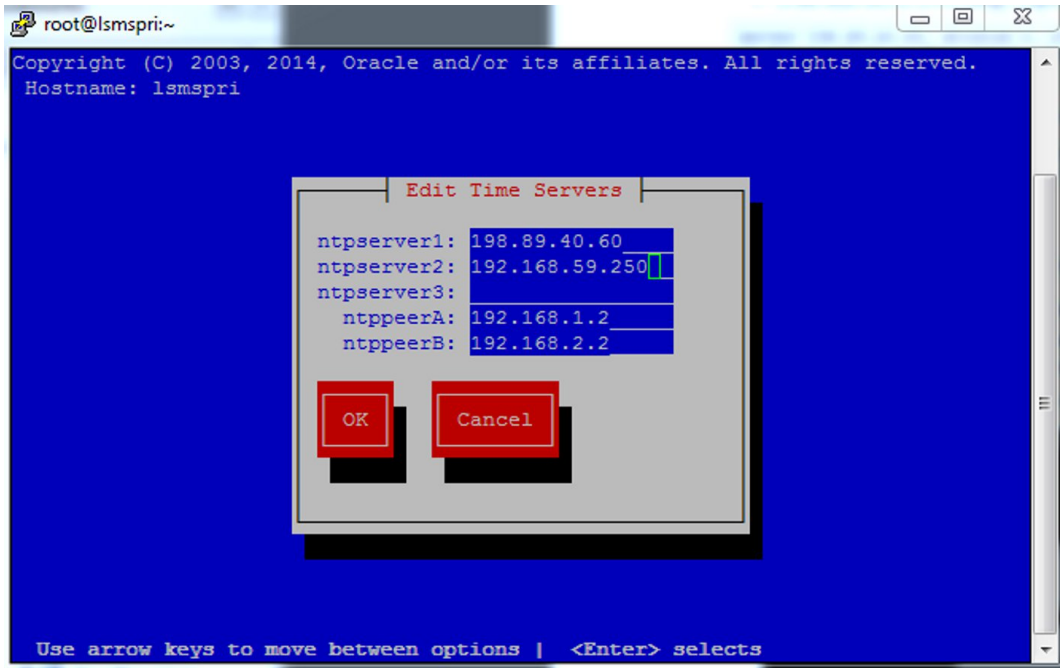
Figure 5-3 Displaying NTP Time Servers Screen



5. To add an **NTP** server to the **LSMS** configuration, type the **IP** address for the available **NTP** server to use for your **LSMS**.

   Choose the server with the lowest number, which provides the highest stratum of quality of time, and press the **OK** button.

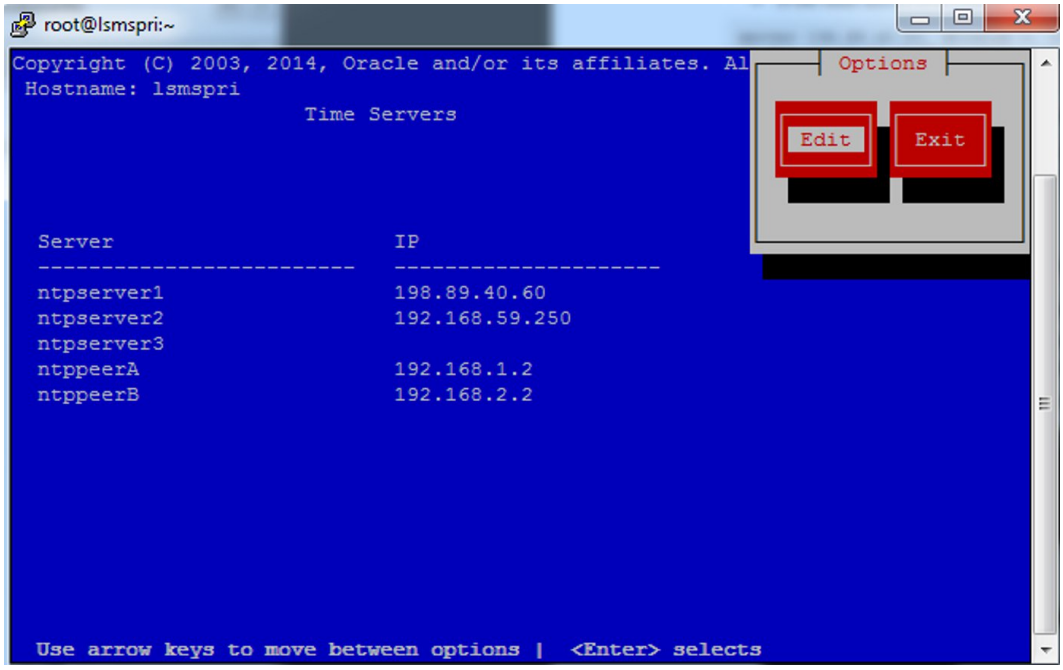
Figure 5-4 Assigning an NTP Server to the LSMS



6. The Time Server screen now reappears to confirm your entry for `netserver2` as assigned to the **LSMS** port you specified.

   You can now **Edit** the existing routes or **Exit** back to the **Network Configuration Menu**.

Figure 5-5 Specifying a New System Route



Configuring the Service Assurance Feature

The Service Assurance feature allows an external system to access subscription version data from the **LNP** databases in the **LSMS**. This information is useful in verifying correct porting of data, and helps in troubleshooting problems. There is one LNP database for each of the **NPAC**s associated with the LSMS.

The external system uses Service Assurance Manager (**SAM**) application to initiate service assurance data requests and associations. Single or multiple **SAM**s may exist on the external computer system. The SAM communicates with the LSMS through the Service Assurance Agent (**SAA**) application in the LSMS. The SAM application is not Oracle Communications software and is resides only on the external system.

The SAA decodes the queries from the SAM and then accesses the LNP database. The SAA forms the subscription version data into a message and forwards that message to the SAM making the query.

Service Assurance works in conjunction with the Surveillance feature. The Surveillance feature issues the command to start the Service Assurance agent, and it monitors the status of the Service Assurance agent. A maximum of four SAM/SAA sessions are allowed at one time.

External Network Connections

External network connections should be on physically separate network segments and address spaces. During a system switchover, IP addresses will change if used on a single subnet network configuration.

Firewall Requirements

The customer should have a firewall between the Service Assurance system and the LSMS.

Figure 5-6 Service Assurance Firewall

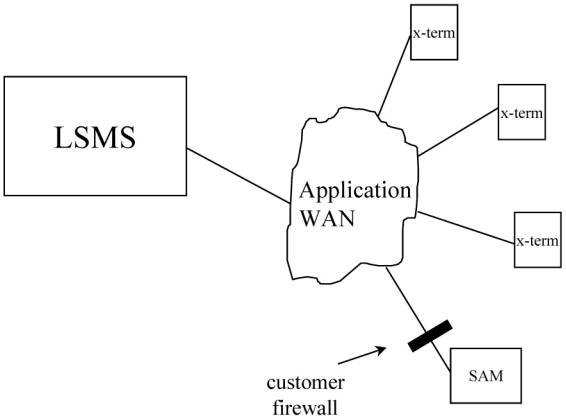


Table 5-1 identifies the firewall parameters used to accept expected functions and to block unauthorized functions.

Table 5-1 Firewall Parameters for Service Assurance

Interface	TCP/IP Port	Use	Inbound	Outbound
Service Assurance to Application **WAN**	102	**OSI** - **TSAP** [1]	Yes	Yes

[1] The OSI stack determines the Ethernet port assignments.

The customer is responsible for setting the firewall parameters. The firewall can be alternatively located between the **LSMS** and the X-terminal **WAN**. If that is the case, the allowed functions specified in Table 5-1 should be used in addition to any other firewall parameters required for X-terminal access to the **LSMS**.

Configuring the LSMS for Service Assurance

To configure the **LSMS** for the Service Assurance feature, the **LSMS** system administrator must create a file that contains the *systemName* and the *npacName* of each allowed **SAM**/**LNP** database association. A single **SAM** can associated with more than one database, but each association must be listed in a separate line in the file. Each line of the file consists of the name of the user application (*systemName*) and the name of the **LNP** database (*npacName*) separated by a colon (:).

Many **SAM**/**LNP** database associations can be listed in the configuration file, but only four of these associations may be active at one time.

The configuration file must be saved as:

```
/usr/TKLC/lsms/config/sa.cfg
```

The following is an example of a configuration file using the user application names of “Service System” and “headquarters.” “Service System” is associated with one **LNP** database and “headquarters” is associated with two **LNP** databases.

```
Service System:Mid-Atlantic Regional NPAC SMS
headquarters:Midwest Regional NPAC SMS
headquarters:Mid-Atlantic Regional NPAC SMS
```

Enable Service Assurance Feature

To enable this feature, perform this procedure:

1. As LSMS `lsmsadm` user, execute "sentry register -n1 sacw-rc 190 -pl".
2. Execute "Saagent allow".
3. Create $LSMS_DIR/../config/sa.cfg file with information on Service Assurance Managers as described in this section.

To configure the **LSMS** for the Service Assurance feature, the **LSMS** system administrator must create a file that contains the *systemName* and the *npacName* of each allowed **SAM**/**LNP** database association. A single **SAM** can associated with more than one database, but each association must be listed in a separate line in the file. Each line of the file consists of

the name of the user application (*systemName*) and the name of the **LNP** database (*npacName*) separated by a colon (:).

Many **SAM**/**LNP** database associations can be listed in the configuration file, but only four of these associations may be active at one time.

The configuration file must be saved as:

```
/usr/TKLC/lsms/config/sa.cfg
```

The following is an example of a configuration file using the user application names of “Service System” and “headquarters.” “Service System” is associated with one **LNP** database and “headquarters” is associated with two **LNP** databases.

```
Service System:Mid-Atlantic Regional NPAC SMS
headquarters:Midwest Regional NPAC SMS
headquarters:Mid-Atlantic Regional NPAC SMS
```

Configuring SPID Security for Locally Provisioned Data

Without this optional feature, any user is able to log in using any Service Provider Identifier (**SPID**) that is defined on the **LSMS**. The user is able to view any data for any **SPID**, and depending on which user privileges were assigned to that username, might even be able to change data associated with any **SPID**.

This optional feature allows the **LSMS** administrator to assign only certain usernames to be allowed to log on with a specified **SPID**. In addition, the **LSMS** administrator can assign a username to be given access to all **SPIDs**; such a user is called a “golden user.”

This feature is especially useful for **LSMS** customers that act as service bureaus, offering **LSMS** services to other service providers. The service bureau may administer locally provisioned data for a client and may choose to allow the client to administer or view its own data without allowing that client to view or change data belonging to other clients.

Types of Data Protected by SPID Security

Association of a username with a **SPID** allows the **LSMS** system administrator to restrict access to the following types of locally provisioned data:

- Default **GTT** (global title translation)
- Override **GTT**
- **GTT** Groups
- **TN** (telephone number) filters
- Assignment of **GTT** groups and **TN** filters to an **EMS** (element management system). For more information, refer to *Database Administrator's Guide*.

Accessibility to these types of data are protected by **SPID** security for any access method (for example, through the **GUI**, through input data by file, audit, and reconcile).

Enable SPID Security Feature

> **Note:**
>
> For customers that have been upgraded directly from **LSMS** Release 4.x to Release 6.1, all **EMS** components created in the prior release must be deleted and recreated under its appropriate **SPID**.

Once the feature is activated, the following actual usernames (not user group names) are defined to be “golden users” having access to all **SPID** and all other usernames are defined to have no access to any **SPID**s:

- `lsmsadm`
- `lsmsview`
- `lsmsall`
- `lsmsuser`
- `lsmsuext`

After the feature has been activated, the **LSMS** administrator (`lsmsadm`) is advised to immediately define associations between usernames and **SPID** using a new command, `spidsec`, as described in the following procedure:

1. To enable the feature, login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal SPID_SECURITY <new spid limit>`.

   Where `<new spid limit>` is a number from 32 to 512 in increments of 16.
3. The command will prompt for a "Customer Service ID:"
4. Enter the value `823543`.
5. The value of SPID_SECURITY will be updated in the database. LSMS software will allow customers to configure additional service provider IDs.

   The user will now be able to use the SPID Security feature as described in Configuring SPID Security for Locally Provisioned Data.
6. To activate the feature, log in as `lsmsadm` on the administrative console.
7. If you do not wish the username `lsmsuext` to have access to all **SPID**, enter the following command to remove the username from golden access:

   ```
   $ spidsec -r -u lsmsadm -s golden
   ```
8. If desired, repeat 7 for usernames `lsmsview`, `lsmsall`, `lsmsuser`, and `lsmsadm`.

> **Note:**
>
> It is recommended that the username lsmsadm always be allowed golden access.

9. Use *admintool* to display all the usernames currently defined on the **LSMS** (for more information, see “Displaying All **LSMS** User Accounts” in any release of *Alarms and Maintenance Guide*).
10. For each displayed username, determine which **SPID**s you wish to allow this user access to and enter the following command to authorize this username for the specified SPID:

    ```
    $ spidsec -a -u <username> -s {<spid>|golden}
    ```

    The following parameters and options apply to this command:

    `<username>` A valid **LSMS** username that has been provisioned using admintool

    `<spid>` A valid **SPID** defined on the **LSMS** (alternatively, you can enter `golden` to allow this username access to all SPIDs defined on the **LSMS**)

    To authorize this username to multiple SPIDs, but not for all SPIDs, you must enter the command once for each **SPID**.
11. Repeat 10 for each user displayed in 9.

Enabling SV Type and Alternative SPID

To enable SV type and alternative SPID, perform this procedure:

> **Note:**
>
> These features can only be enabled with LSMS 10.0 or later. Once SV type is activated, the field is required. Therefore, it is strongly recommended that a bulk download from the NPAC be performed to obtain values for the new SV type field. Failure to perform a bulk download will result in inconsistent data between the NPAC and the LSMS. Although alternative SPID can be activated separately from SV type, it is recommended that both fields be activated at the same time so values for both fields can be obtained during one bulk download. In this procedure, it is assumed that both SV type and alternative SPID will be enabled at the same time.

1. Contact NPAC to arrange a time for NPAC to simultaneously update the SV type indicator and the alternative SPID indicator.
2. If SVType and alternative SPID are set to Y, it is strongly recommended that a bulk download be performed to obtain **SV** and **NPBBDD** files using the new settings.
3. Login to the LSMS as `lsmsadm`.
4. Stop each instance of the LSMS npacagent by entering the following command:

    ```
    $ lsms stop <region>
    ```
5. For each feature being activated, issue the command: `dbcfginternal <FEATURE> <Y|N>`.

    Use SV_TYPE or ALT_SPID for <FEATURE>

    Use the value Y to enable and the value N to disable the feature
6. The value of SV_TYPE and/or ALT_SPID has been updated in the database.
7. If SV_TYPE is being set to Y, then, for each region, import the SV and NPB bulk data download files that were created using the new setting(s). This step is not

required, but since the SVType is a required field (when enabled) this step is recommended. Note that completion of this bulk data import from the NPAC then also requires a bulkload from the LSMS to the ELAP.

8. Verify with NPAC that the NPAC Customer LSMS SV Type Indicator and/or NPAC Customer LSMS Alternative SPID Indicator has been changed to match the corresponding configuration Boolean.
9. Restart each instance of the LSMS npacagent by entering the following command:

   ```
   $ lsms start <region>
   ```

LSMS will now require SV type data in SV and NPB objects from NPAC if SV_TYPE is set to "Y" and allow Alternative SPID data if ALT_SPID is set to "Y."

Enable SPID Recovery Feature

SPID Recovery Feature allows. To enable this feature, perform this procedure:

> **Note:**
>
> For Canada only, use `CANADA_SPID_RECOVERY`.

This feature can only be enabled if the NANC 3.3 Feature Set has already been enabled.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal SPID_RECOVERY <new spid limit>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of SPID_RECOVERY will be updated in the database.
4. For changes to take effect, restart each running Npacagent if NANC_3_3_FEATURE_SET was changed. Restart just the Canada Npacagent if only CANADA_SPID_RECOVERY was changed.
5. If NANC_3_3_FEATURE_SET is enabled ("Y"), then Npacagents (other than Canada) will allow recovery of SPID values, but if disabled ("N"), they will not allow recovery of SPID values. For the Canada Npacagent, if the NANC_3_3_FEATURE_SET is enabled and the CANADA_SPID_RECOVERY is also enabled ("Y") then it will support recovery of SPID values, otherwise not.

LSMS Command Class Management Overview

LSMS supports configurable **GUI** permission groups *in addition to* the five non-configurable **GUI** permission groups (`lsmsadm`, `lsmsuser`, `lsmsview`, `lsmsall`, and `lsmsuext`).

The **LSMS** supports the creation of 128 additional, configurable **GUI** permission groups that can be used to ensure a specific and secure environment. After creating the new, configurable **GUI** permission groups, the system administrator can assign users to the appropriate group.

The configurable **GUI** permission groups control access to **GUI** commands, the **CLAA** (Command Line Administration Application) equivalent, or any Linux command equivalent of **GUI** functions.

A method to control access to a fixed set of Linux commands is provided. Existing Linux-level **LSMS** commands, executables, and scripts are classified as follows:

1. Linux command equivalents of **GUI** commands (Reports and functions of **CLAA**)

   These commands are controlled by the assignment of the corresponding **GUI** function.

2. Optional Linux command capability for Report Generator (**LQL**)

   This command may be assigned individually, similar to **GUI** commands, to one or more permission groups.

3. Root privilege-only commands

   These commands are root-only and are not assignable to any permission group.

4. Other commands owned by `lsmsadm`

   These commands include those used by the **LSMS** application, those used to control processes, and those for setup and configuration. Commands in this category are grouped as a single set of Linux level admin commands and defined as a Linux permission group. Users may or may not be granted access to this Linux group, in addition to being assigned to the appropriate **GUI** group.

   Some commands in this group, although owned by `lsmsadm`, are accessible to non-owners for limited operation, such as status. The incorporation of this feature will not have any impact on the current privileges of Linux commands for non-owners.

   Example:

   To set up a custom environment, system administrators should define the **GUI** permission groups and populate those groups with the appropriate commands (see Table 5-2):

Table 5-2 Define GUI Permission Groups and Assign Command Privileges

GUI Permission Group	Command Privileges
Custom **GUI CONFIG**	All Configuration Commands
Custom **GUI EMS**	All **EMS**-related Commands
Custom **GUI SUPER**	All **GUI** Commands

Optionally, assign users (for example, Mike, Sally, and Bill) to a specific Linux permission group (in this example, “lsmsadm”) or **GUI** permission group, as shown in Table 5-3.

Table 5-3 User Assignment Examples

User	Linux Permission Group	GUI Permission Group
Mike	`lsmsadm`	Custom **GUI CONFIG**
Joe	`lsmsall`	Custom **GUI EMS**
Sally	`lsmsadm`	lsmsadm
Bill	`lsmsadm`	Custom **GUI SUPER**

> **Note:**
>
> Secure activation is required because this is an optional feature.

After activating this feature, you can create permission groups and assign users to these new groups.

> **Note:**
>
> Changes in privileges do not automatically occur upon feature activation.

Permission Group Naming

- The **LSMS** supports the ability to uniquely name each configurable **GUI** permission group.
- A group name can consist of a minimum of one character to a maximum of 40 characters (alphanumeric characters only are permitted).

Permission Group Contents

- Each configurable **GUI** permission group supports any or all of the **LSMS GUI** commands.

> **Note:**
>
> The **GUI** command represents the function, via either the **GUI**, **CLAA**, or Linux command equivalent of **GUI** commands.

- Any **GUI** command may be associated with multiple **GUI** permission groups.
- The **LQL** optional Linux **LSMS** command for the Report Generator feature can be placed in **GUI** permission groups.
- The **LSMS** supports a Linux group containing the current Linux **LSMS** `lsmsadm` commands with the exception of Report, Audit, and **LQL**.

Permission Group Commands

The **LSMS** enables you to perform the following tasks:

- Create and modify **GUI** permission groups.
- Assign a user to a single **GUI** permission group.
- Assign a user access to the Linux group in addition to a **GUI** permission group.
- Retrieve the names of all permission groups, all the commands permitted within a permission group, and the names of all permission groups that contain a particular command.

Permission Group Processing

GUI Functions:

The **LSMS** allows a **GUI** user access to **GUI** commands, **CLAA** commands, or Linux command equivalents of **GUI** commands only if that user is an authorized user.

Linux-Level:

The **LSMS** allows a user access to Linux-level scripts and executables only if that user is an authorized user.

Enable Command Class Management

LSMS Command Class Management supports the creation of additional, configurable **GUI** permission groups. Also, a new report, the “Permission Group Data” report, provides a listing of all permission groups, commands authorized for each permission group, and users assigned to each permission group. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal COMMAND_CLASS <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of COMMAND_CLASS will be updated in the database.

The user is now capable of creating new groups and assigning users to the groups as described in this section.

> **Note:**
>
> No changes in privileges will happen automatically upon feature activation. Existing users will retain the same privileges upon initial activation of this feature. Existing permission groups (lsmsuser, lsmsadm, lsmsview, lsmsuext, and lsmsall) remain non-configurable.

If this feature is disabled, all configurable permission groups created and users' assignments to them are retained. The ability to create, modify and delete permission groups and user assignments will no longer be permitted.

Admin Menu Component Information

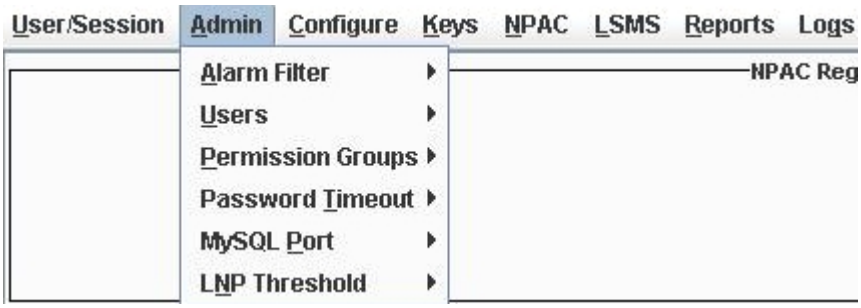
The Admin menu, which consists of the following submenu items:

- **Alarm Filter** - When activated, the Alarm Filter feature enables the system administrator to filter unwanted alarms from being sent to remote alarm surveillance management systems.
- **Users** - Enables the system administrator to modify or view existing users' permission group assignment.
- **Permission Groups** - Enables the system administrator to create, modify, view, or delete permission groups.
- **Inactivity Timeout** - When activated, the Automatic Inactivity Logout feature logs out **LSMSGUI** and Linux users after a preset period of inactivity occurs.
- **Password Timeout** - Enables the system administrator to modify password timeout intervals that are specific to individual users or user groups.

- **MySQL Port** - Enables the system administrator to configure the MySQL port to any port between 34000 and 34099.
- **LNP Threshold** - Enables the system administrator to configure the LNP quantity threshold.

> **Note:**
>
> To access the Admin menu functions, you must log in as lsmsadm or lsmsall group.

Figure 5-7 Admin Menu



The User dialog is used to modify and view permission group assignment for existing users.

When a user is initially created, the system administrator assigns that user to one of the non-configurable, default permission groups. After being initially assigned to a default permission group, the system administrator can assign a user to a different default permission group or to a configurable permission group. The permission group to which a user is assigned depends on the type of account it is and what it is to be used for. A user can only be assigned to a single permission group.

> **Note:**
>
> Default users of default permission groups cannot be re-assigned to another permission group. For example, an “lsmsadm” user assigned to the “lsmsadm” permission group cannot be re-assigned to the “lsmsview” permission group.

The permission group to which a user is assigned can be modified or viewed using the Modify (see Modify Users) or View User (see View Users) dialog, respectively.

Configurable permission groups can be created, modified, viewed, and deleted using the Permission Groups dialogs (see “Permission Groups Submenu”).

> **Note:**
>
> Permission group assignments will only effect new logins. Users that are currently logged in will retain their current group permissions until their next login.

> **Note:**
>
> Although the **LSMS** application does not impose a limit on the number of **LSMS** users that can be created on the system, a maximum of 128 users can be displayed in the Combo Box list of the **LSMSGUI** User Dialogs (when using **LSMS** local **GUI**). There is no limitation when running the **LSMSGUI** remotely on a Windows platform.

Alarm Filter Submenu

The Alarm Filter enables the system administrator to prevent certain alarms from being sent to remote alarm/surveillance management systems. For example, certain low priority alarms, certain alarms for known issues, or certain alarms the customer deems unnecessary, can be filtered out of notifications. Alarm filters can be created, modified, viewed, and deleted.

Enable Alarm Filtering Feature

To enable this feature, perform this procedure:

> **Note:**
>
> This feature can only be enabled if SNMP has already been enabled.

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal ALARM_FILTERING <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of ALARM_FILTERING will be updated in the database.

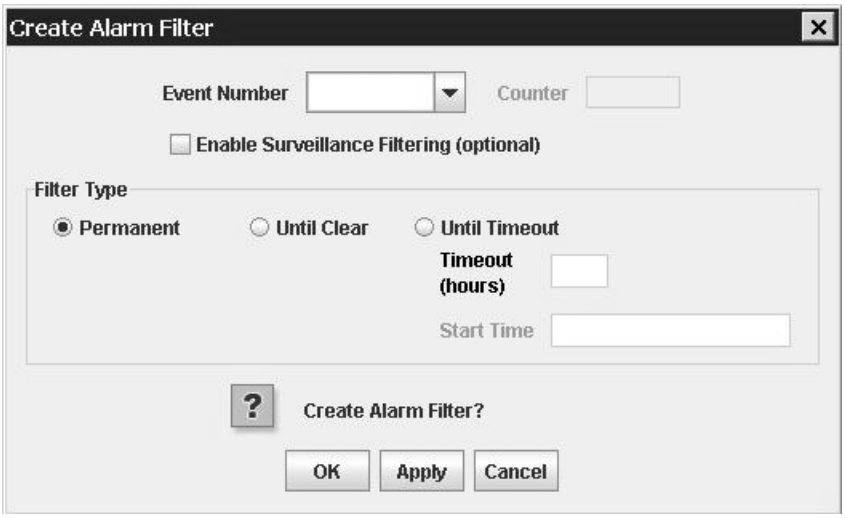
The user can now filter alarms from the LSMS GUI or Command Line.

Create Alarm Filter

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Alarm Filter** , and then **Create**.

   The Create Alarm Filter dialog appears.

Figure 5-8 Create Alarm Filter



3. Enter an **Event Number**.
4. Select **Enable Surveillance Filtering (optional)**. This step is optional
5. Select one of the **Filter Type** radio buttons.
6. Click **Apply** to save the changes and remain in the current window, or skip to 7

   When the Update Successful dialog appears, click **OK**.
7. Click **OK** to save the changes and return to the LSMS Console.

   When the Update Successful dialog appears, click **OK**.

Table 5-4 Create Alarm Filter Dialog - Field Constraints

Field	Type	Constraints
Event Number	Text field	Range: 1 to 4 numeric characters
Enable Surveillance Filtering (optional)	Checkbox	None
Filter Type	Radio buttons	None

Table 5-5 Create Alarm Filter Dialog - Field Descriptions

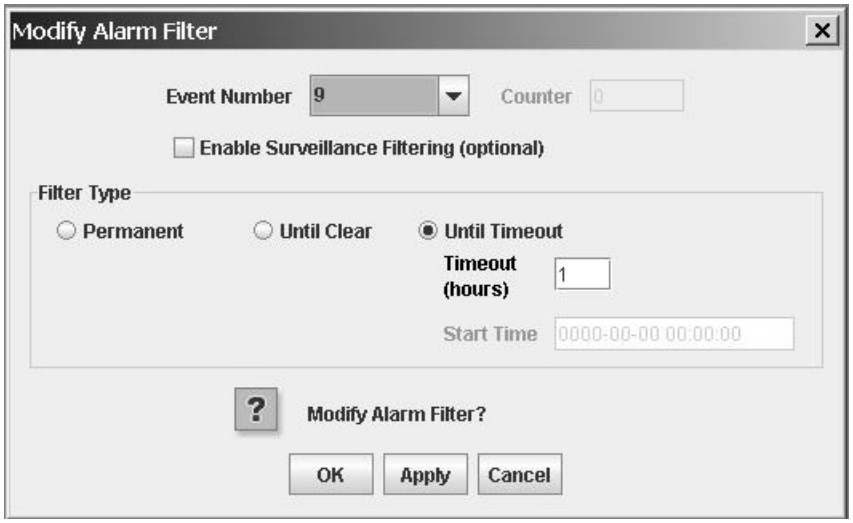
Field	Description
Event Number	The event number for which you want to create a filter.
Enable Surveillance Filtering (optional)	When selected, the alarm will not be sent to the console/serial port.
Filter Type	• Permanent - Filter the alarm permanently. • Until Clear - Filter alarm until it clears. • Until Timeout - Filter alarm until timeout.

Modify Alarm Filter

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Alarm Filter**, and then **Modify**.

   The Modify Alarm Filter dialog appears.

Figure 5-9 Modify Alarm Filter



3. Select an **Event Number** from the pulldown menu.
4. Select or deselect **Enable Surveillance Filtering (optional)**.
5. Make the necessary changes to the **Filter Type**.
6. Click **Apply** to save the changes and remain in the current window, or skip to 7.

   An Update Successful dialog appears. Click **OK**.
7. Click **OK** to save the changes and return to the LSMS Console.

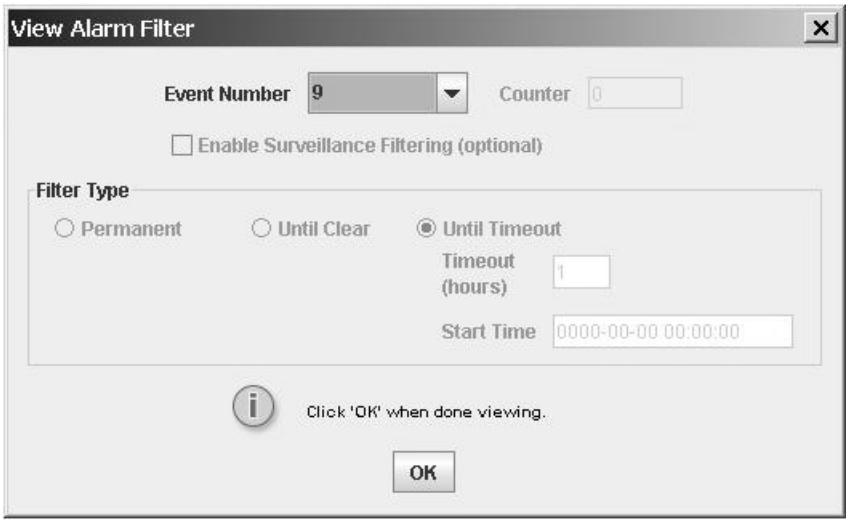
   An Update Successful dialog appears. Click **OK**.

View Alarm Filter

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Alarm Filter**, and then **View**.

   The View Alarm Filter dialog appears.

Figure 5-10 View Alarm Filter



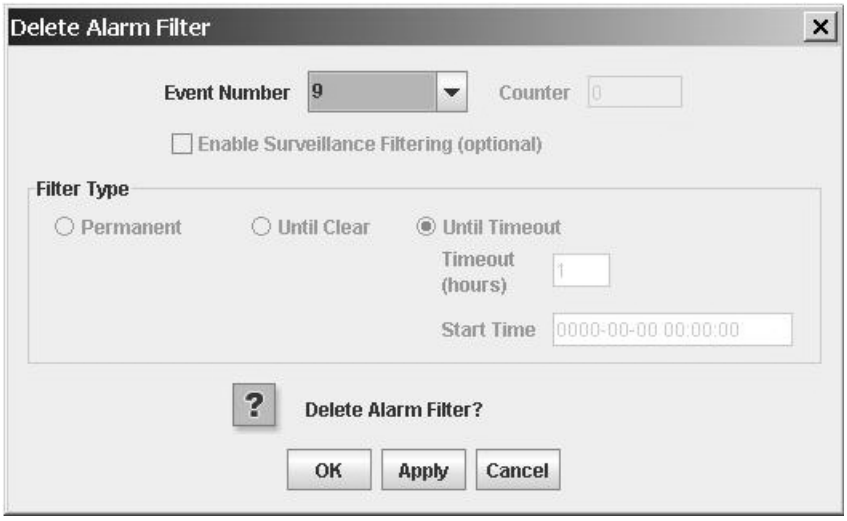
3. Select an **Event Number** from the pulldown menu to view its details.
4. Click **OK** to return to the LSMS Console.

Delete Alarm Filter

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Alarm Filter**, and then **Delete**.

   The Delete Alarm Filter dialog appears.

Figure 5-11 Delete Alarm Filter



3. Select an **Event Number** from the pulldown menu.
4. Click **Apply** to delete the **Event Number** and remain in the current window, or skip to 5.

   A Confirm Delete dialog appears.

   a. Click **Yes** to delete the **Event Number**.

An Update Successful dialog appears.

b. Click **OK**.

5. Click **OK** to delete the **Event Number** and return to the LSMS Console.

A Confirm Delete dialog appears.

a. Click **Yes** to delete the **Event Number**.

An Update Successful dialog appears.

b. Click **OK**.

Users Submenu

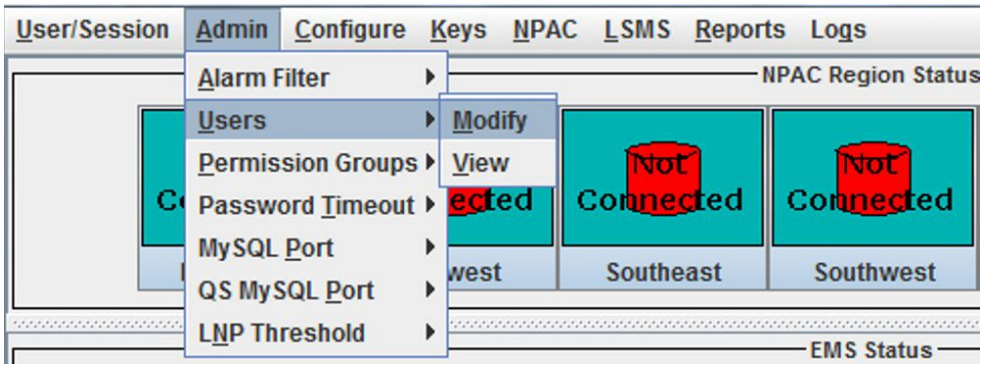
The **Users** submenu consists of a Modify and a View function.

Modify Users

The Modify User dialog is used to modify the group assignment for an existing user, as described in the following procedure.

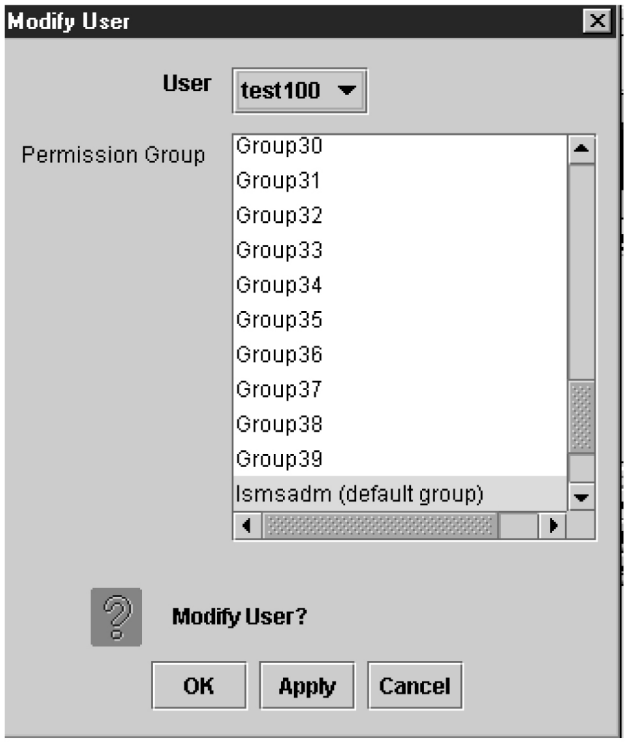
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Users**, and then **Modify**.

Figure 5-12 Select Admin, and then Users, and then Modify



3. Click **Modify**, and the Modify User dialog displays.

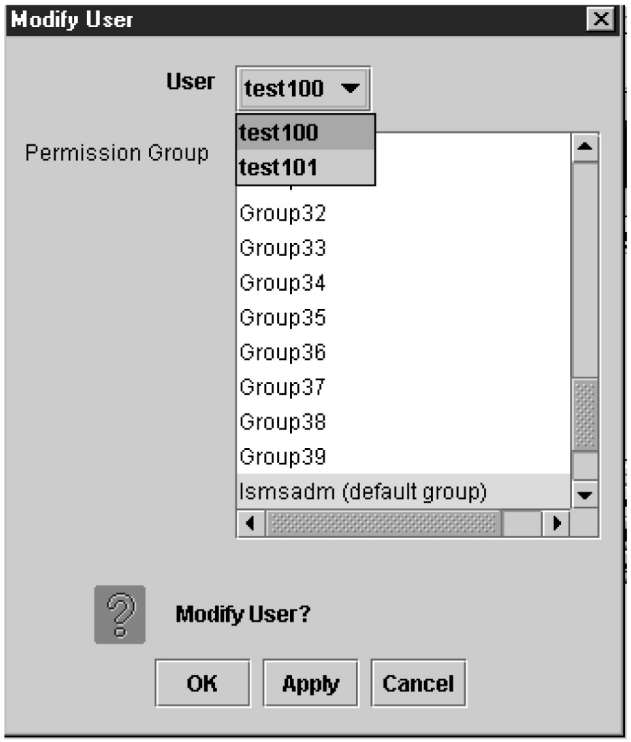
Figure 5-13 Modify User Dialog



4. Select a User, and the associated permission group is automatically selected in the Permission Group list.

> **Note:**
>
> See Table 5-6 and Table 5-7 for information about the Modify User dialog field constraints and descriptions, respectively.

Figure 5-14 Select a User



5. To modify the permission group assignment for another user, click **Apply**.

   If you try to modify permission group assignment for another user while there are unsaved changes for the current user, a confirmation dialog is displayed asking you to save the changes.

> **Note:**
>
> When you click **OK** or Apply to modify a user's permission group assignment, the permission group selection is checked to ensure that a permission group has been selected. If a permission group is not selected, an error dialog is displayed.

Figure 5-15 Confirmation Dialog

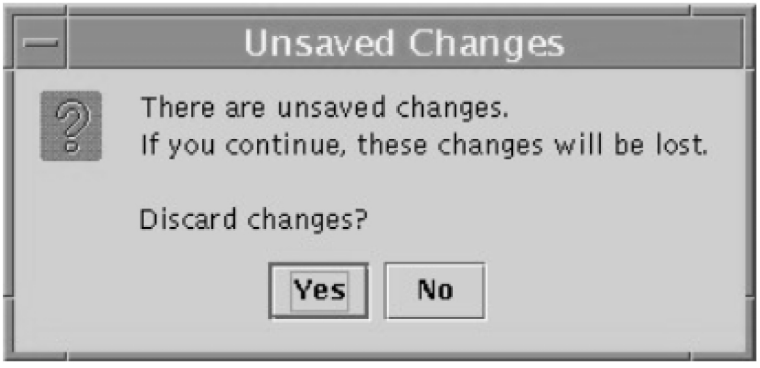


Table 5-6 Modify User Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
User	Combo Box	No	Single selection only
Permission Group	List	Yes	Single selection only

Table 5-7 Modify User Dialog - Field Description

Field	Description
User	Login name used to access the **LSMS**.
Permission Group	List of previously defined permission groups (see Permission Groups Submenu). The user is a member of the selected permissions group.

6. When you are done, click **OK** .

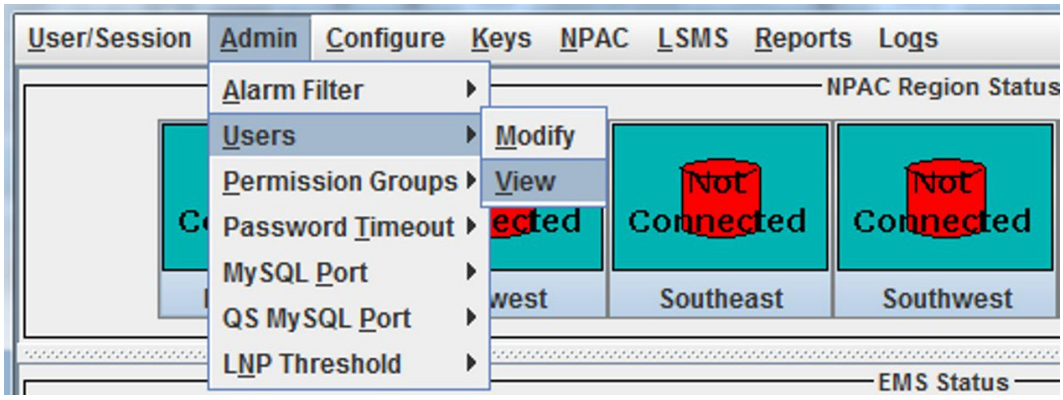
You have now completed this procedure.

View Users

The View User dialog is used to view the permission group assignment for existing users, as described in the following procedure.

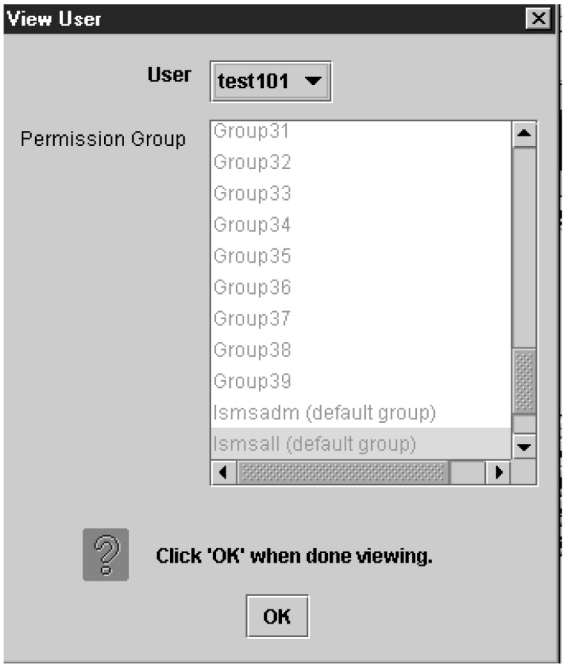
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Users**, and then **View**.

Figure 5-16 Select Admin, and then Users, and then View



3. Click **View**, and the View User dialog displays.

Figure 5-17 View User Dialog



4. Select a user, and the associated permission group is automatically selected in the Permission Group list.
5. When you are done, click **OK** .

Permission Groups Submenu

The Permission Groups dialog is used to manage configurable permission groups. A configurable permission group is a way for the system administrator to grant a group of users access privileges for a defined set of **LSMS GUI** and **CLAA** (Command Line Administration Application) equivalent functions.

> **Note:**
>
> The access privileges of the five default permission groups (`lsmsadm`, `lsmsuser`, `lsmsview`, `lsmsall`, and `lsmsuext`) are not configurable.

The system administrator users may grant or deny command access privileges to members of a configurable permission group by selecting or deselecting menus and functions in the permissions hierarchical list by clicking on the checkbox or on its corresponding descriptive text.

- A checked checkbox indicates that users assigned to that permission group will be granted access privileges for the corresponding **GUI** menus and/or functions and **CLAA** equivalent commands.
- An unchecked (empty) checkbox indicates that users assigned to that permission group will not be granted access privileges for the corresponding **GUI** menus and/or functions and **CLAA** equivalent commands.

- Sub-menus and functions are only available for selection when their higher-level menu's checkbox is checked.
- Access privileges can be granted or revoked for every **GUI** menu and/or functions and **CLAA** equivalent commands with the exception of the **User/Session** menu and menu items.

Individual users are assigned to permission groups using the User dialogs (as described in Users Submenu).

> **Note:**
>
> Modifications made to permission groups will only effect new logins. Users that are currently logged in will retain their current permissions until their next login.

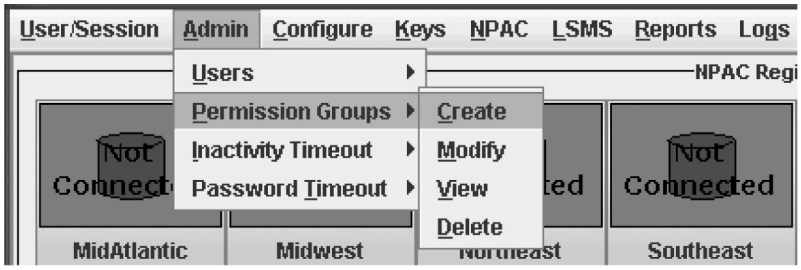
Create Permission Group

The Create Permission Group dialog is used to create a new configurable permission group. You must enter a unique name for the group and select the commands that users of the group will be authorized to access. The hierarchical list of **LSMS** menus and command permissions is initially unselected (no access privileges granted).

To create a permission group, use the following procedure.

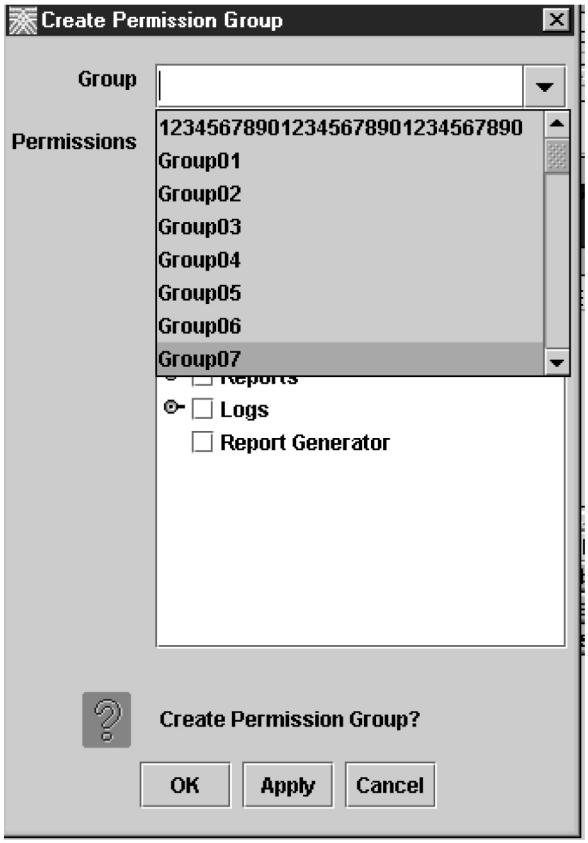
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Permission Groups** , and then **Create**.

Figure 5-18 Select Admin, and then Permission Groups , and then Create



3. Click **Create**, and the Create Permission Group dialog displays.

Figure 5-19 Create Permission Group Dialog



4. Type in a Group Name, and then select the items in the Permissions list that the users in that group will have access to.

> **Note:**
>
> See Table 5-8 and Table 5-9 for information about the Create Permission Group dialog field constraints and descriptions, respectively.

5. If you plan to create an additional permission group, click **Apply**.

   If not, click **OK** .

> **Note:**
>
> When you click **OK** or Apply to create a configurable permission group, the group name is checked to ensure that another group has not already been defined with the same name. If the group name has already been defined, the operation will fail, and an error dialog is displayed.

Table 5-8 Create Permission Group Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
Group	Text Field	Yes	• Must be a unique group name • Keyboard input enabled • Maximum of 40 alphanumeric characters
Permissions	Tree	Yes	None

Table 5-9 Create Permission Group Dialog - Field Description

Field	Description
Group	Create a Permission Group with this name.
Permissions	A hierarchical list of **LSMS GUI** menus and command privileges that can be assigned to the membership of the permissions group.

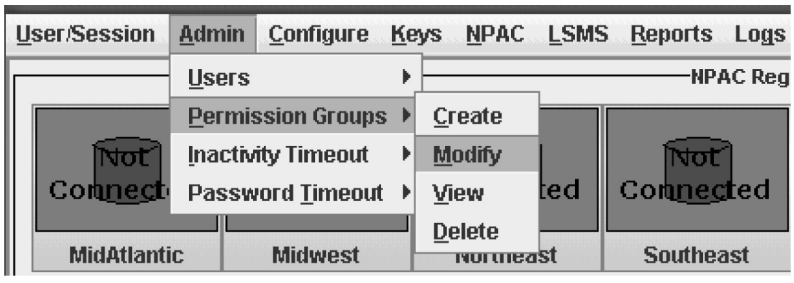
Modify Permission Group

The Modify Permission Group dialog is used to modify the access privileges for existing configurable permission groups. To modify the access privileges for an existing permission group, select the group name from the group list.

To modify a permission group, use the following procedure.

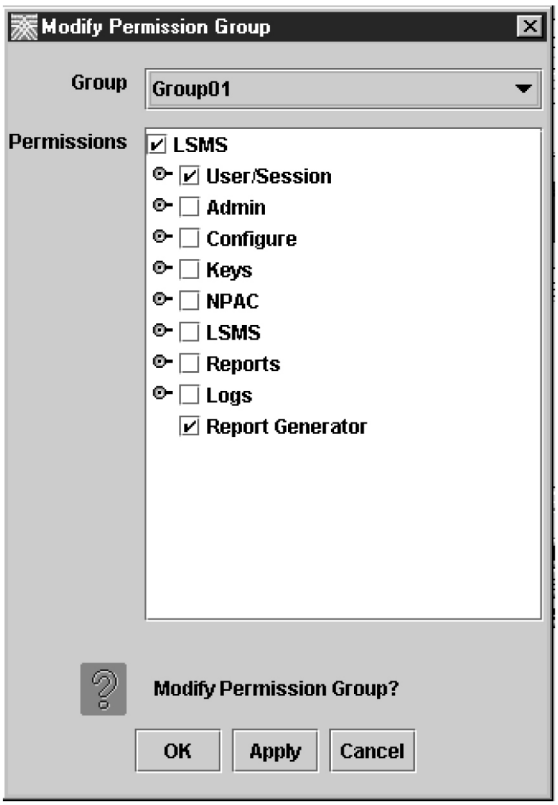
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Permission Groups**, and then **Modify**.

Figure 5-20 Select Admin, and then Permission Groups, and then Modify



3. Click **Modify** and the Modify Permission Group dialog displays.

Figure 5-21 Modify Permission Group Dialog



4. Select a Permission Group.

   The authorized permissions of the selected group are automatically checked in the Permissions area.

> **Note:**
>
> See Table 5-10 and Table 5-11 for information about the Modify Permission Group dialog field constraints and descriptions, respectively.

5. If you plan to modify the access privileges for an additional Permission Group, click **Apply**. If not, click **OK**.

   If you try to modify another Permission Group's access privileges while there are unsaved changes to the access privileges for the current group, a confirmation dialog is displayed asking you to save the changes.

> **Note:**
>
> The access privileges for default permission groups cannot be modified.

> **Note:**
>
> The name of an existing permission group cannot be modified (renamed) using the Modify User dialog. If the name of an existing permissions group needs to be modified, a new permissions group with the same permissions must be created and users re-assigned to it.

Table 5-10 Modify Permission Group Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
Group	Text Field	No	None
Permissions	Tree	Yes	None

Table 5-11 Modify Permission Group Dialog - Field Description

Field	Description
Group	Modify a Permission Group with this name.
Permissions	A hierarchical list of **LSMS GUI** menus and command privileges that can be assigned to the membership of the permissions group.

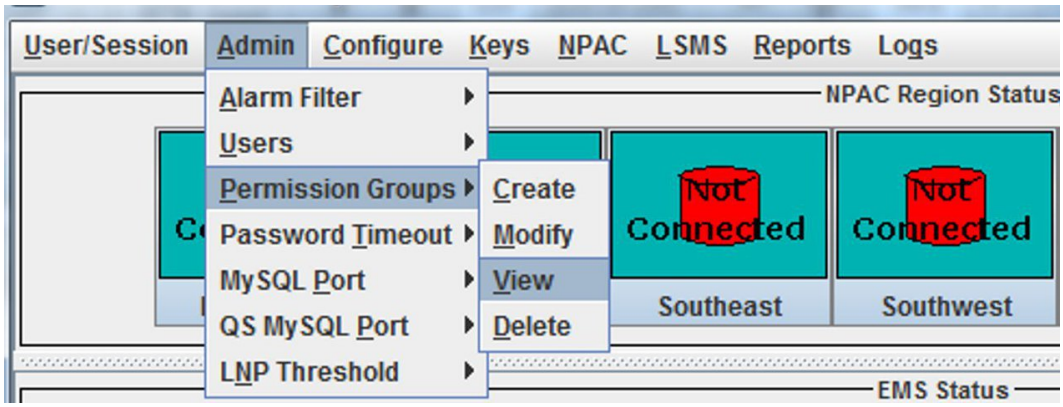
View Permission Group

The View Permission Group dialog is used to view access privileges for existing permission groups.

To view a permission group, use the following procedure.

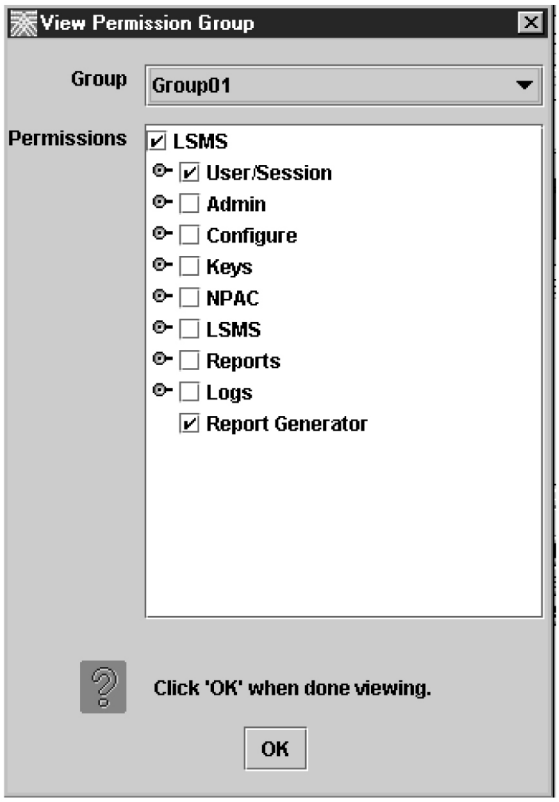
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Permission Groups**, and then **View**.

Figure 5-22 Select Admin, and then Permission Groups, and then View



3. Click **View**, and the View Permission Group dialog displays.

Figure 5-23 View Permission Group Dialog



4. Select a Permission Group.

   The access privileges of the selected group are automatically shown in the Permissions area.

> **Note:**
>
> See Table 5-12 and Table 5-13 for information about the View Permission Group dialog field constraints and descriptions, respectively.

5. If you plan to view the access privileges for an additional Permission Group, click **Apply**.

   If not, click **OK** .

Table 5-12 View Permission Group Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
Group	Text Field	No	None

Table 5-12 (Cont.) View Permission Group Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
Permissions	Tree	No	None

Table 5-13 View Permission Group Dialog - Field Description

Field	Description
Group	View a Permission Group with this name.
Permissions	A hierarchical list of **LSMS GUI** menus and command privileges that can be assigned to the membership of the permissions group.

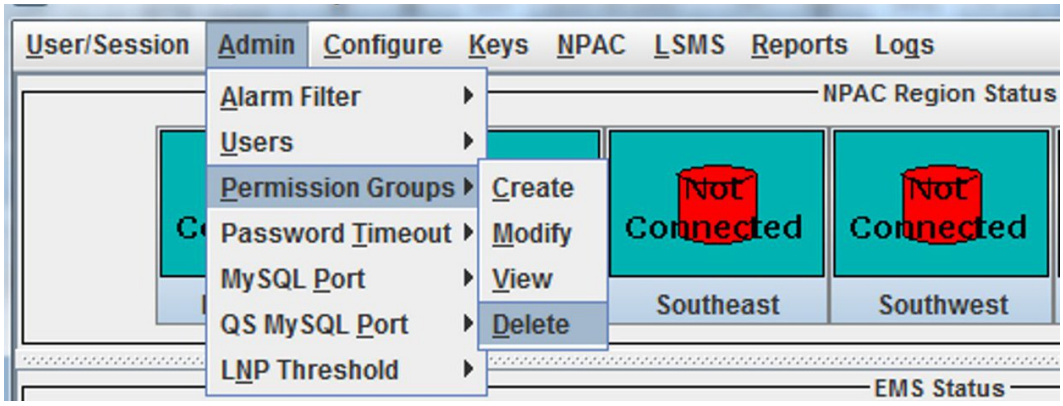
Delete Permission Group

The Delete Permission Group dialog is used to delete an existing configurable permission group.

To delete a configurable permission group, use the following procedure.

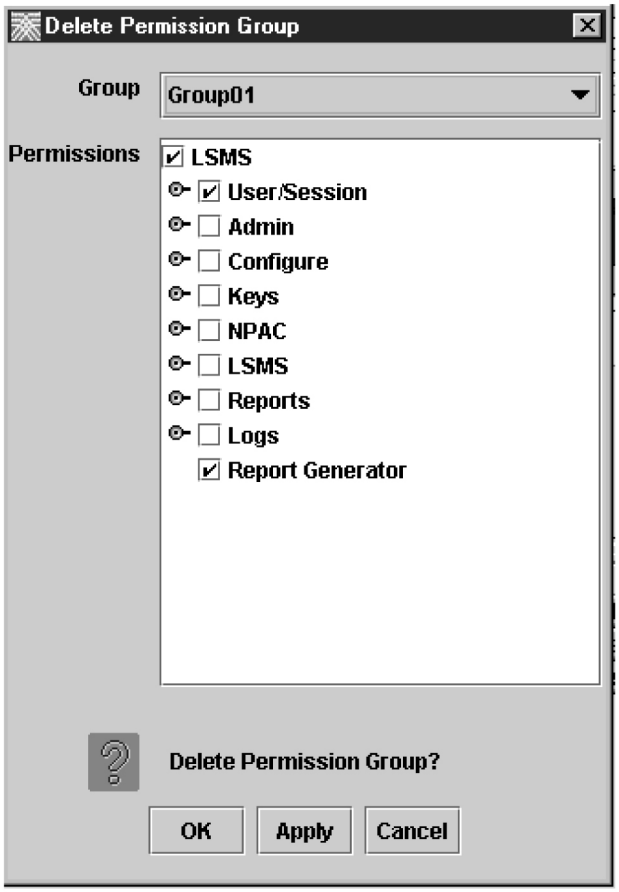
1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Permission Groups**, and then **Delete**.

Figure 5-24 Select Admin, and then Permission Groups, and then Delete



3. Click **Delete**, and the Delete Permission Group dialog displays.

Figure 5-25 Delete Permission Group Dialog



4. Select a Permission Group.

   The access privileges of the selected group are automatically shown in the Permissions area.

> **Note:**
>
> See Table 5-14 and Table 5-15 for information about the Delete Permission Group dialog field constraints and descriptions, respectively.

5. To delete an existing configurable permission group, select the name from the group list.

   If you plan to delete an additional Permission Group, click **Apply**. If not, click **OK** .

> **Note:**
>
> When you click **OK** or Apply to delete a configurable permission group, the users' data is checked to ensure that there are no users currently assigned to the group. If one or more users are currently assigned, the operation will fail, and an error dialog is displayed.

> **Note:**
>
> Default permission groups cannot be deleted.

Table 5-14 Delete Permission Group Dialog - Field Constraints

Field	Type	Modifiable?	Constraints
Group	Text Field	No	None
Permissions	Tree	No	None

Table 5-15 Delete Permission Group Dialog - Field Description

Field	Description
Group	Delete a Permission Group with this name.
Permissions	A hierarchical list of **LSMS GUI** menus and command privileges that can be assigned to the membership of the permissions group.

Inactivity Timeout Submenu

The Inactivity Timeout submenu is designed to manage the Inactivity Timeout feature, which will log out users from the **LSMS GUI** and Linux Shell after a specified period of inactivity. This is an optional feature and must be activated.

The Inactivity Timeout submenu includes two types of customizable timers—a system timer (see System Timer) and a user timer (see User Timer). The user timeout, if specified, will override the system timeout.

Inactivity Timeout Functionality for GUI Users

- For tasks of extended duration, such as audits, where the user initiates a task which continues without further user input, the task execution will not constitute user input. However, updates to the **GUI** from the process will continue as normal past the logout. At the completion of the process, if the timeout has expired, the log-in screen will pop up and block access to the **GUI**. If a user successfully logs in again, the results of the task will be available for review. Any time that user input is received during the process the timer would be reset.
- Any input by the user would constitute activity and reset the timer.
- Members of the `lsmsadm` or `lsmsall` default permission group (or members of any authorized configurable permission group) can modify the inactivity logout period. Values must be specified in whole minute intervals, and can range from 1 minute to a maximum value of 2147483647 minutes (which means, essentially, the logout period never expires). Specify this maximum value by using a zero (0).

Inactivity Timeout Functionality for Linux Users

- Any user input or task execution would constitute activity and reset the timer.

- For extended duration operations, where the user initiates a task which continues without additional user input, the operation will continue. The task execution is considered user activity in the Linux environment. The user will be logged off if the inactivity time expires.

Enable Inactivity Timeout Feature

Automatic Inactivity Logout automatically logs off **GUI** users and Linux users after the specified period of inactivity. This feature includes a configurable system timer and a configurable user timer. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`, or as a user of an authorized configurable permission group.
2. Issue the command `dbcfginternal INACTIVITY_TIMEOUT <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. Restart the LSMS GUI for the feature to take effect.

The user can now perform all of the functionality described in Inactivity Timeout Submenu.

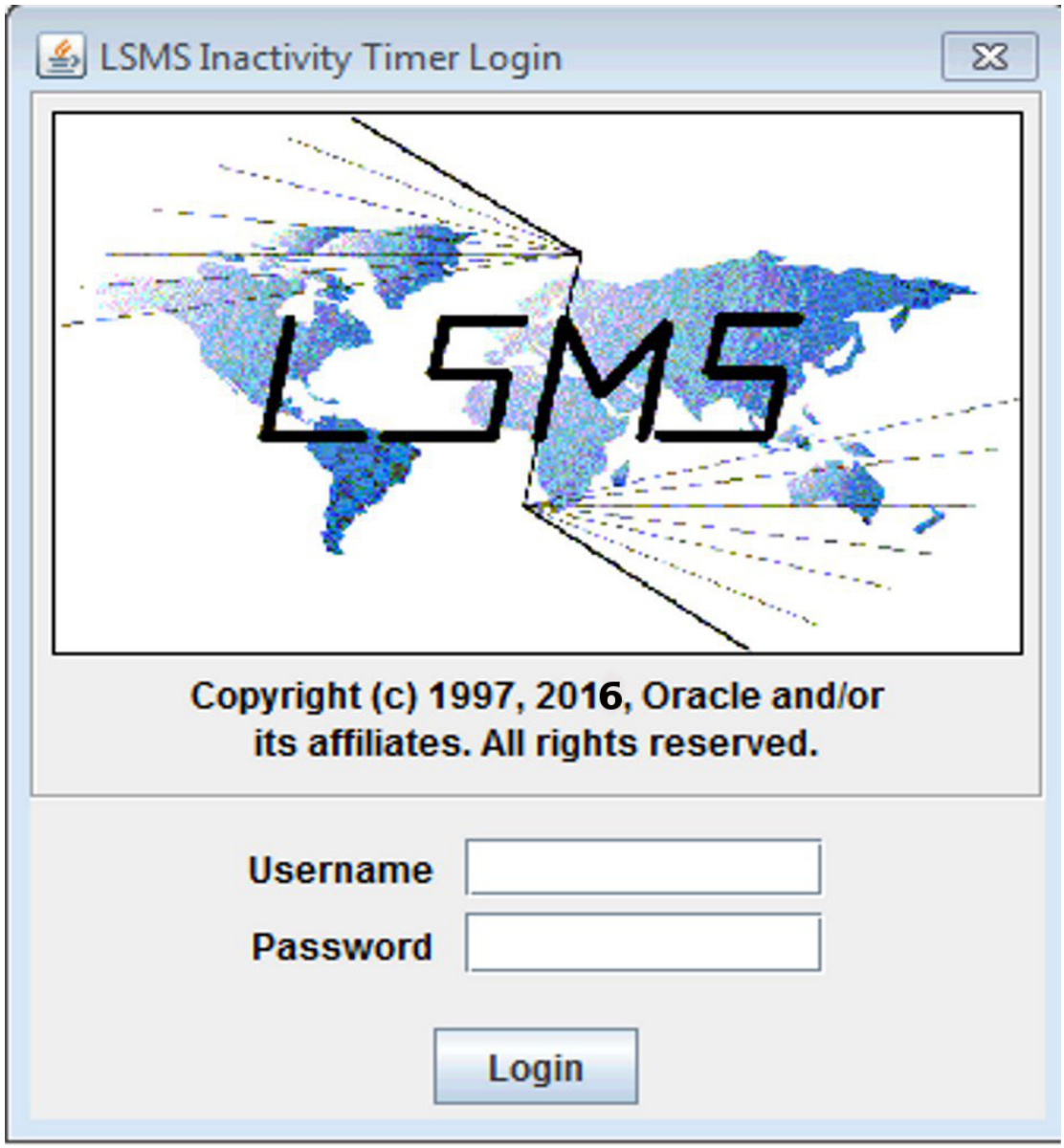
System Timer

The system timer provides an easy way to specify the same inactivity logout period, in minutes, for each **LSMS GUI** or Linux user. The default inactivity logout period is 15 minutes, but this logout period is configurable via the **GUI**.

> **Note:**
>
> The User Inactivity Timeout value, if set, will override the System Inactivity Timeout.

When the inactivity timer is activated, the **LSMS Inactivity Timer Login** window is displayed. It will accept only the username and password for the user that was last logged in.

Figure 5-26 LSMS Inactivity Timer Login Screen

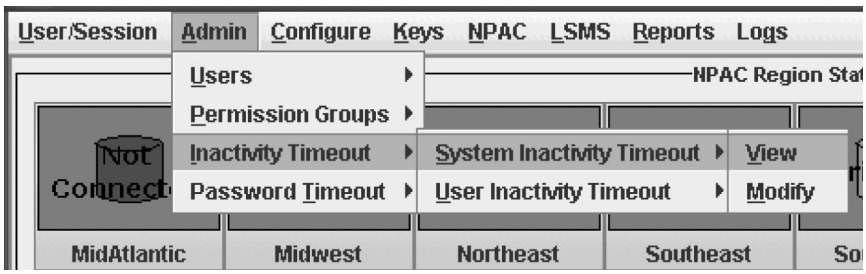


View System Inactivity Timeout

To access the **View System Inactivity Timeout** window, perform the following steps:

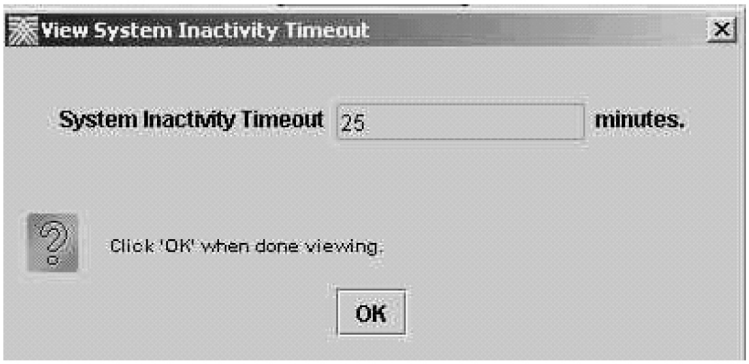
1. Log in as a user in the `lsmsadm` or `lsmsall` group, or as a user of an authorized configurable permission group.
2. From the **LSMS** Console window, select the **Admin** menu item.
3. Select **Inactivity Timeout**, and then **System Inactivity Timeout**, and then **View**.

Figure 5-27 Select Timeout, and then System Inactivity Timeout, and then View



4. Click **View**, and the **View System Inactivity Timeout** window displays.

Figure 5-28 View System Inactivity Timeout Window



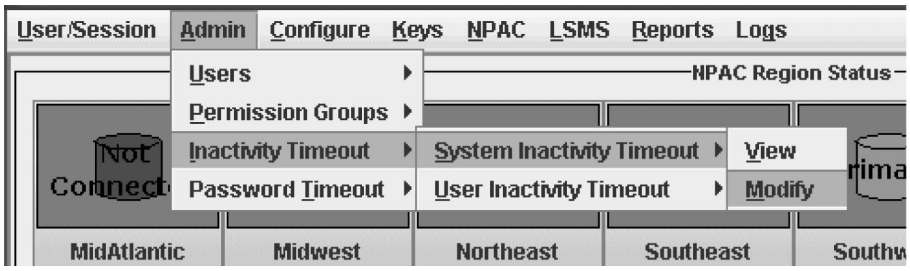
5. Click **OK** when you are done viewing.

Modify System Inactivity Timeout

To access the **Modify System Inactivity Timeout** window perform the following steps:

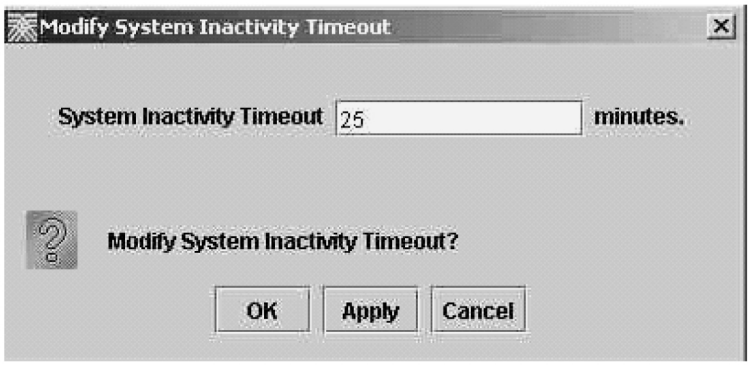
1. Log in as a user in the `lsmsadm` or `lsmsall` group, or as a user of an authorized configurable permission group.
2. From the **LSMS Console** window, select the**Admin** menu item.
3. Select **Inactivity Timeout**, and then **System Inactivity Timeout**, and then **Modify**.

Figure 5-29 Select Inactivity Timeout, and then System Inactivity Timeout, and then Modify



4. Click **Modify**, and the **Modify System Inactivity Timeout** window displays.

Figure 5-30 Modify System Inactivity Timeout Window



5. Specify the number of minutes.

> **Note:**
>
> A value of 0 (zero) means the timer will never expire and the user will never be logged out.

6. Click **Apply** then click **OK** when you are done, and a window similar to the one shown in Figure 5-31 displays.

   (Click **Cancel** if you do not want to make or accept any changes.)

Figure 5-31 Modify System Inactivity Timeout Change Notification Window

User Timer

The user timer provides an easy way to specify different inactivity logout periods, in minutes, for individual **LSMS GUI** and Linux users. The inactivity logout period is configurable via the **GUI**.

> **Note:**
>
> The User Inactivity Timeout value, if set, will override the System Inactivity Timeout.

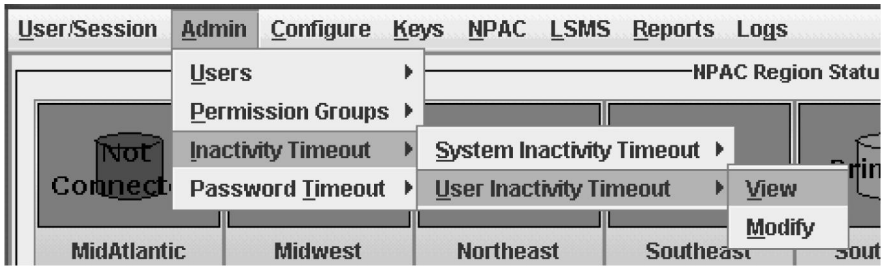
When the inactivity timer is activated, the **GUI** Inactivity Timer Login Screen is displayed. It will accept only the user name and password for the user that was last logged in.

View User Timer Inactivity Timeout

To access the **View User Inactivity Timeout** window, perform the following steps:

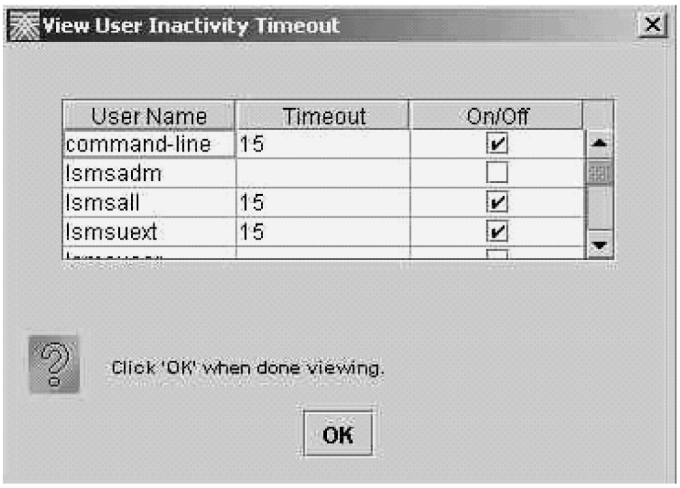
1. Log in as a user in the `lsmsadm` or `lsmsall` group, or as a user of an authorized configurable permission group.
2. From the **LSMS Console** window, select the **Admin** menu item.
3. Select **Inactivity Timeout**, and then **User Inactivity Timeout**, and then **View**.

Figure 5-32 Select Inactivity Timeout, and then User Inactivity Timeout, and then View



4. Click **View**, and the **View User Inactivity Timeout** window displays.

Figure 5-33 View User Inactivity Timeout Window



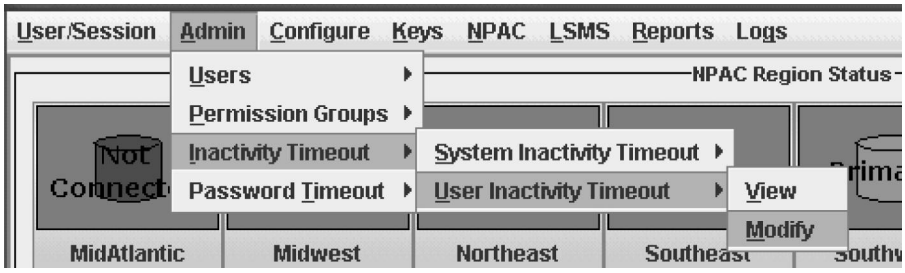
5. Click **OK** when you are done viewing.

Modify User Inactivity Timeout

To access the **Modify User Inactivity Timeout** window, perform the following steps:

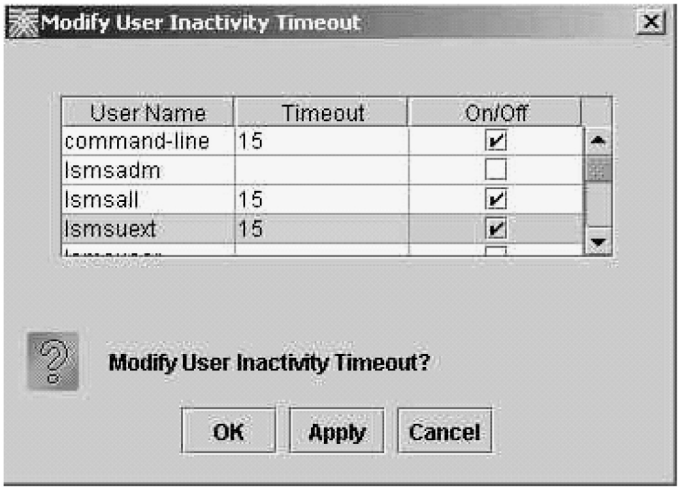
1. Log in as a user in the `lsmsadm` or `lsmsall` group, or as a user of an authorized configurable permission group.
2. From the **LSMS Console** window, select the **Admin** menu item.
3. Select **Inactivity Timeout**, and then **User Inactivity Timeout**, and then **Modify**.

Figure 5-34 Select Inactivity Timeout, and then User Inactivity Timeout, and then Modify



4. Click **Modify**, and the **Modify User Inactivity Timeout** window displays.

Figure 5-35 Modify User Inactivity Timeout Window



5. Do the following to make changes to the table:
   - To add a timeout entry for the first time, click the On-Off checkbox (a check appears).
     A default timeout value of 15 minutes is automatically entered in the **Timeout** field. To change this value, double-click the value, delete it, and type in the new value.
   - To change an existing timeout entry, double-click the timeout value, delete the existing value, and type in the new value.
   - To deactivate an existing entry, click the On/Off checkbox (the check disappears).

> **Note:**
>
> A value of 0 (zero) means the timer will never expire and the user will never be logged out.

6. Click **Apply** then click **OK** when you are done, and a window similar to the one shown below displays.

   (Click **Cancel** if you do not want to make or accept any changes.)

Figure 5-36 Modify User Inactivity Timeout Change Notification Window

Password Timeout Submenu

The Password Timeout dialog enables users in the permission groups lsmsadm and lsmsall to view and modify password timeout intervals at both the system and user levels. Access the Password Timeout feature by selecting **Admin**, and then **Password Timeout**.

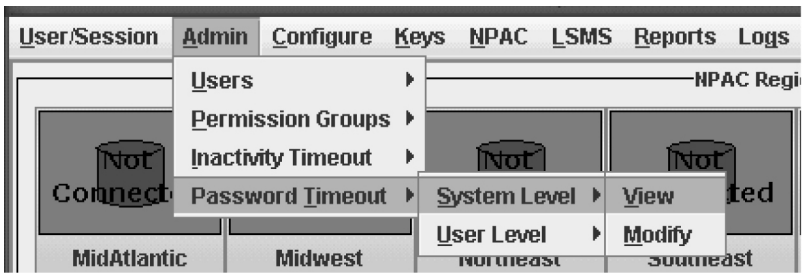
View System Level Password Timeout

The View System Level dialog is used to view the system level password timeout interval.

To view password timeout information at the system level, use the following procedure:

1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Password Timeout**, and then **System Level**, and then **View**.

Figure 5-37 Select Admin, and then Password Timeout, and then System Level, and then View



3. Click **View**, and the View System Level Password Timeout dialog displays.

Figure 5-38 View System Level Password Timeout

> **Note:**
>
> A password timeout value of 0 indicates the password is valid for an indefinite period of time. A password timeout value of -1 indicates the password timeout has not been configured.

4. Click **OK** when you are done viewing.

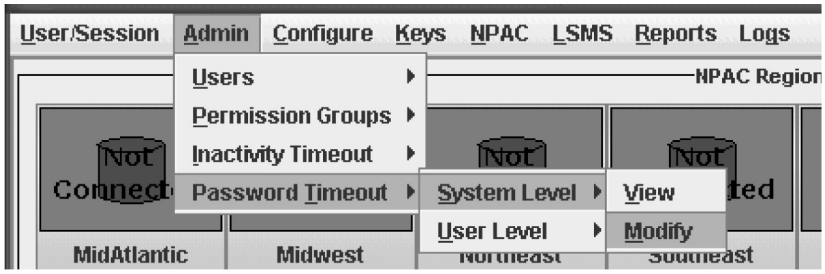
Modify System Level Password Timeout Interval

The Modify System Level dialog is used to modify the system level password timeout interval.

To modify the password timeout interval at the system level, use the following procedure:

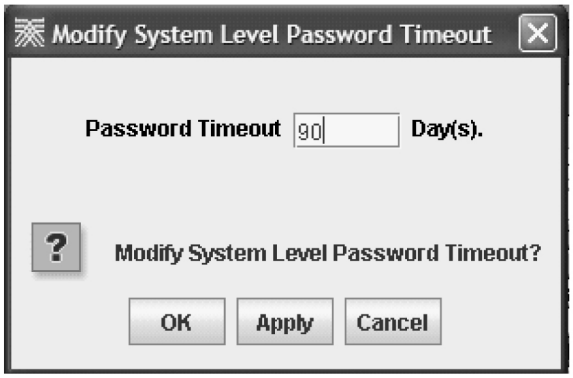
1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Password Timeout**, and then **System Level**, and then **Modify**.

Figure 5-39 Select Admin, and then Password Timeout, and then System Level, and then Modify



3. Click **Modify**, and the Modify System Level Password Timeout dialog displays.

Figure 5-40 Modify System Level Password Timeout



4. Type in the number of days for the password timeout interval, then click **OK** .

   If you have successfully modified the password timeout, then the Update Successful dialog displays.

Figure 5-41 Update Successful

5. Click **OK** .

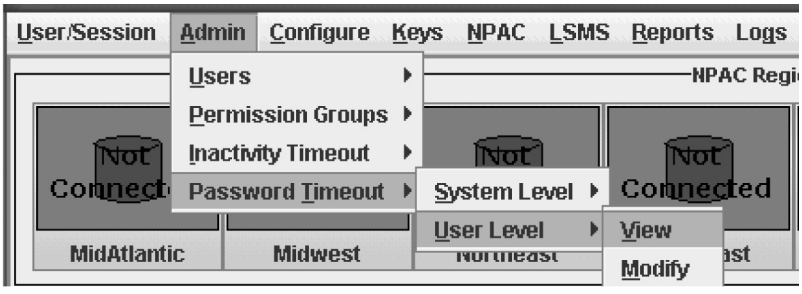
View User Level Password Timeout

The View User Level dialog is used to view the user level password timeout interval.

To view password timeout intervals at the user level, use the following procedure:

1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Password Timeout**, and then **User Level**, and then **View**.

Figure 5-42 Select Admin > Password Timeout > User Level > View



3. Click **View**, and the View User Level Password Timeout dialog displays..

Figure 5-43 View User Level Password Timeout

> **Note:**
>
> A password timeout value of 0 indicates the password is valid for an indefinite period of time. A password timeout value of -1 indicates the password timeout has not been configured.

4. Select a User, and the associated password timeout interval is automatically shown in the Password Timeout box.
5. Click **OK** when you are done viewing.

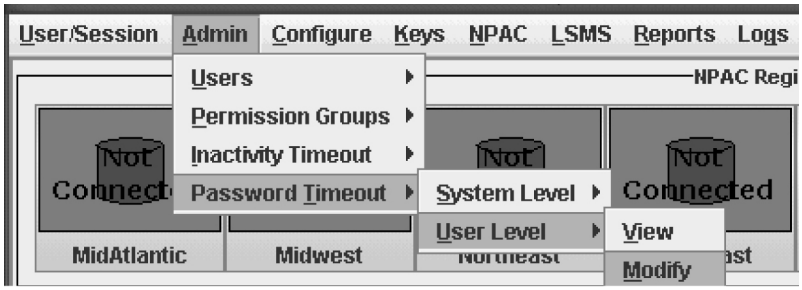
Modify User Level Password Timeout Interval

The Modify User Level dialog is used to modify the user level password timeout interval.

To modify password timeout intervals at the user level, use the following procedure:

1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **Password Timeout**, and then **User Level**, and then **Modify**.

Figure 5-44 Select Admin, and then Password Timeout, and then User Level, and then Modify



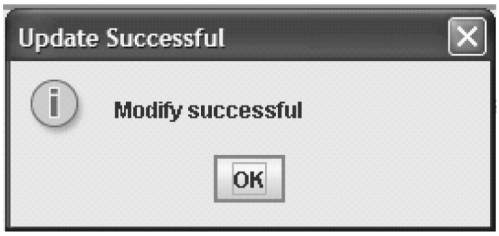
3. Click **Modify**, and the Modify User Level Password Timeout dialog displays.

Figure 5-45 Modify User Level Password Timeout

4. Select a User whose password timeout interval you want to modify.
5. Type in the number of days for the password timeout interval, then click **OK** .

   If you have successfully modified the password timeout, then the Update Successful dialog displays.

Figure 5-46 Update Successful



6. Click **OK** .

MySQL Port Submenu

This optional feature enhances the security of LSMS databases by enabling the system administrator to change the MySQL port.

Through the LSMS GUI, the MySQL port can be configured to ports 34000 through 34099. The port can be maintained through the GUI, and any changes to the port setting will raise an alarm on the LSMS. The MySQL port can also be changed back to the default port, 3306.

Enable Configurable MySQL Port Feature

To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal MYSQL_PORT <Y|N>`.

Use the value Y to enable the feature and N to disable the feature.

3. The value of MYSQL_PORT will be updated in the database.

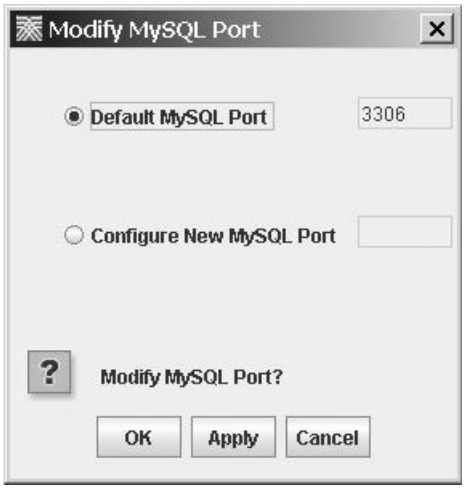
The user can now modify MySQL port for any valid value described in the next section.

Modify MySQL Port

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **MySQL Port**, and then **Modify**.

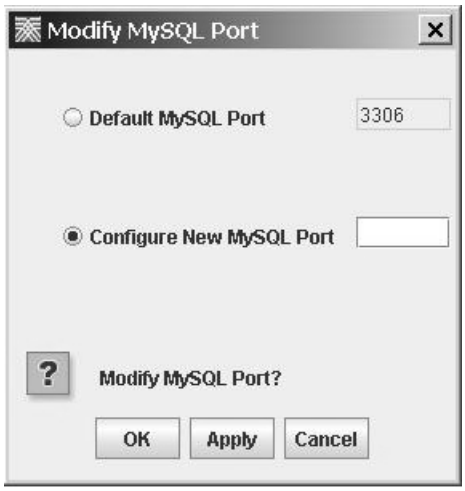
   The Modify MySQL Port dialog appears.

Figure 5-47 Modify MySQL Port



> **Note:**
>
> The default MySQL port is 3306. If the port has not been modified from the default setting, the **Default MySQL Port** radio button will be selected when the dialog appears.

3. Select the **Configure New MySQL Port** radio button to configure a new port.



4. Enter a new MySQL Port number.
5. Click **Apply** to save the changes and remain in the current window, or skip to 6.

   A Confirm Modify dialog appears.

   a. Click **Yes** to modify the MySQL port.

      A dialog box appears with the message: These changes will not be effective until the LSMS application has been stopped and restarted on both LSMS servers.
      See Stopping the Node, Starting the Node, and Updating MySQL Port on MySQL Server for more information.

   b. Click **Cancel** to close the dialogue box. Your changes have been saved.
6. Click **OK** to save the changes and return to the LSMS Console.

   A Confirm Modify dialog appears.

   a. Click **Yes** to modify the MySQL port.

      A dialog box appears with the message: These changes will not be effective until the LSMS application has been stopped and restarted on both LSMS servers.
      See Stopping the Node, Starting the Node, and Updating MySQL Port on MySQL Server for more information.

   b. Click **OK**.

Table 5-16 Modify MySQL Port Dialog - Field Constraints

Field	Type	Constraints
Default MySQL Port	Radio button	Default value: 3306
Configure New MySQL Port	Radio button	Range: 34000-34099

Stopping the Node

After you modify the MySQL port, you must stop and restart the LSMS application on both LSMS servers for the changes to take effect.

> **Note:**
>
> Perform this procedure on the ACTIVE LSMS server first, then on the STANDBY LSMS server.

1. Log in as `lsmsmgr` user. See Logging In to LSMS Server Command Line for more information.

   The `lsmsmgr` text interface appears.
2. Select **Maintenance** and press **Enter**.
3. Select **Stop Node** and press **Enter**.
4. Select **Yes** to confirm the node stop and press **Enter**.
5. Select **Exit** and press **Enter** to return to the Main Menu.
6. Select **Exit** and press **Enter** to exit the `lsmsmgr` text interface.

Starting the Node

After you modify the MySQL port, you must stop and restart the LSMS application on both LSMS servers for the changes to take effect.

> **Note:**
>
> Perform this procedure on the ACTIVE LSMS server first, then on the STANDBY LSMS server.

1. Log in as `lsmsmgr` user. See Logging In to LSMS Server Command Line for more information.

   The `lsmsmgr` text interface appears.
2. Select **Maintenance** and press **Enter**.
3. Select **Start Node** and press **Enter**.
4. Select **Yes** to confirm node startup and press **Enter**.
5. Select **Exit** and press **Enter** to return to the Main Menu.
6. Select **Exit** and press **Enter** to exit the `lsmsmgr` text interface.

Updating MySQL Port on MySQL Server

After you modify the MySQL port using the LSMS GUI, you must also update the MySQL server port number in the MySQL configuration file on the Query Server.

1. At the query server, log in as `root`.
2. Enter this command to verify the MySQL daemon is not running:

```
# ps -eaf |grep mysql
```

If the MySQL daemon is running, enter this command to shut down the MySQL server:

```
# cd /usr/mysql1/bin
# ./mysqladmin -u root -p shutdown
# Enter password:
<Query Server MySQL Root User Password>
```

3. Edit the `/usr/mysql1/my.cnf` file on the query server to reflect the new MySQL server port number:

```
master-port=<LSMS Server's MySQL Port Number>
```

4. Enter this command to start the MySQL daemon on the query server:

```
# ./mysqld_safe &
```

5. Enter this command to check the replication status:

```
# /usr/mysql1/bin/mysql -u root
mysql> show slave status \G
mysql> show processlist;
```

View MySQL Port

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **MySQL Port**, and then **View**.

   The View MySQL Port dialog appears.

Figure 5-48 View MySQL Port

3. Click **OK** to return to the LSMS Console.

LNP Threshold Submenu

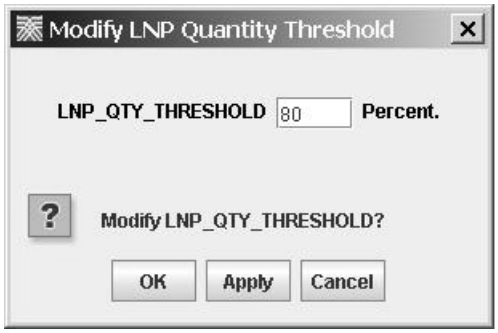
The LNP quantity threshold is an alarm that is raised when the database storage capacity has been reached. LNP quantity threshold can be modified or viewed through the LSMS GUI.

Modify LNP Threshold

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **LNP Threshold**, and then **Modify**.

   The Modify LNP Quantity Threshold dialog appears.

Figure 5-49 Modify LNP Threshold



3. Enter the **LNP_QTY_THRESHOLD** percentage.

   The LNP threshold is a configurable percentage of database storage capacity. An alarm is raised when the database storage capacity has been reached.
4. Click **Apply** to save the changes and remain in the current window, or skip to 5.

   When the Update Successful dialog appears, click **OK**.

   - Click **Cancel** to close the dialogue box. Your changes have been saved.
5. Click **OK** to save the changes and return to the LSMS Console.

   When the Update Successful dialog appears, click **OK**.

Table 5-17 Modify LNP Threshold - Field Constraints

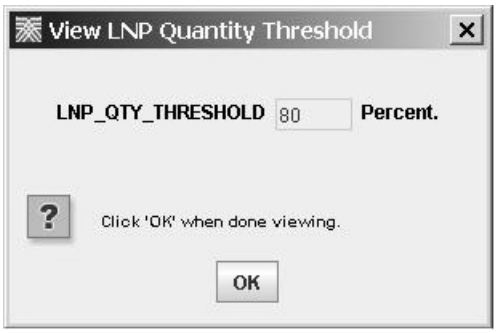
Field	Type	Constraints
LNP_QTY_THRESHOLD	Text field	Range: 1 to 99 percent

View LNP Threshold

1. Log in as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin**, and then **LNP Threshold**, and then **View**.

   The View LNP Quantity Threshold dialog appears.

Figure 5-50 View LNP Threshold



3. Click **OK** to return to the LSMS Console.

Switching NPAC Agent Versions

LSMS provides support for both the NPAC agent versions. The script to switch the NPAC agent versions `switch_NANC528` is available at the directory path: `/usr/TKLC/lsms/bin` in LSMS. This script serves the purpose of switching between the older NPAC agent and newer NPAC agent. The newer agent supports NANC 528 features.

If a user needs to switch back to the older NPAC agent for some reasons, the `switch_NANC528` script can be used for that purpose.

> **Note:**
>
> The NANC 528 interface is only used by iConectiv. It is not supported by Neustar for the Canada region.

The following sections describes the steps to switch across the NPAC agent versions:

Switching NPAC agent version - Newer to Older

Do the following steps to switch to the older npacagent version:

1. Login to LSMS CLI with user `lsmsadm`.
2. Shutdown both the LSMSPRI and LSMSSEC nodes.
   a. Login to LSMSMGR menu on LSMSPRI and go to **Maintenance Menu** and then **Stop Node**.

Figure 5-51 Main Menu

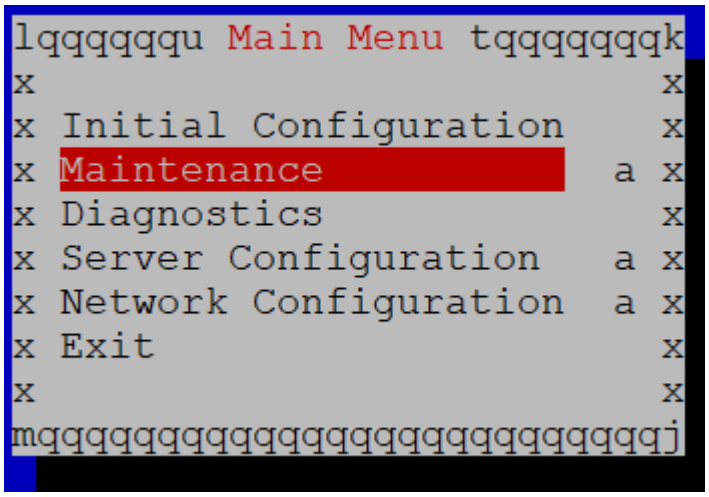
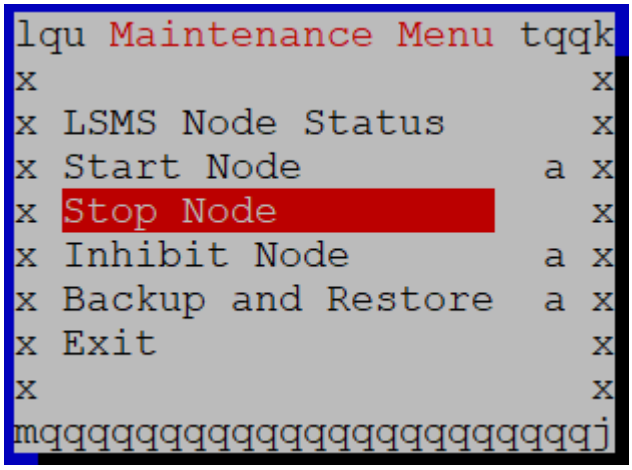


Figure 5-52 Stop Node



b. Repeat the same steps to stop the node on LSMSEC server. Login to LSMSMGR menu and then go to the **Maintenance Menu** and then **Stop Node**.

3. Run the script with the following command on CLI:
`/usr/TKLC/lsms/bin/switch_NANC528`

4. User is prompted to enter YES/NO depending upon the requirement of switching to the older npacagent version as follows:

```
[lsmsadm@lsmspri ~]$ /usr/TKLC/lsms/bin/switch_NANC528
INFO: This script is used for switching between older and newer
npacagent. LSMS should be stopped for this process to continue.
Checking whether LSMS is stopped...

INFO: No active node found, We can proceed...

INFO: You are going to switch to older version of npacagent that
```

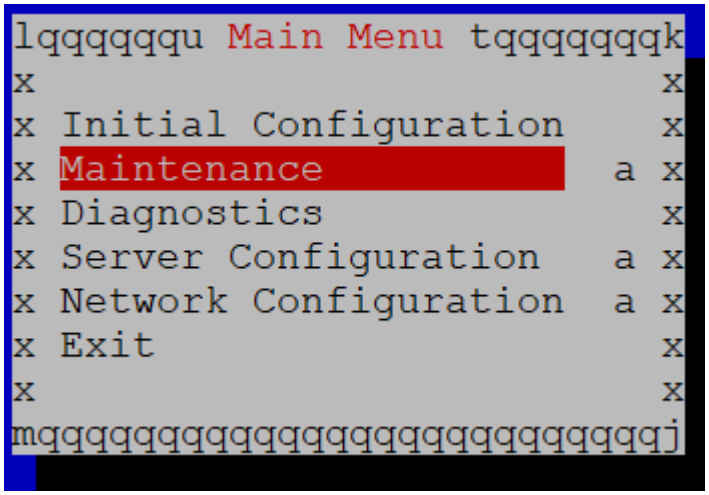
```
will not have NANC 528 updates.
Are you sure you want to continue? (y/n)
```

5. Enter **Y** to switch to the older npacagent version.
   Once the user enters **Y** to the above prompt, npacagent will move to the older version. Below mentioned output will be observed on entering **Y** or **YES**:

```
INFO: Binary replaced successfully on local server, Replacing it on mate
now.
FIPS integrity verification test failed.
INFO: Binary replaced on mate successfully
```

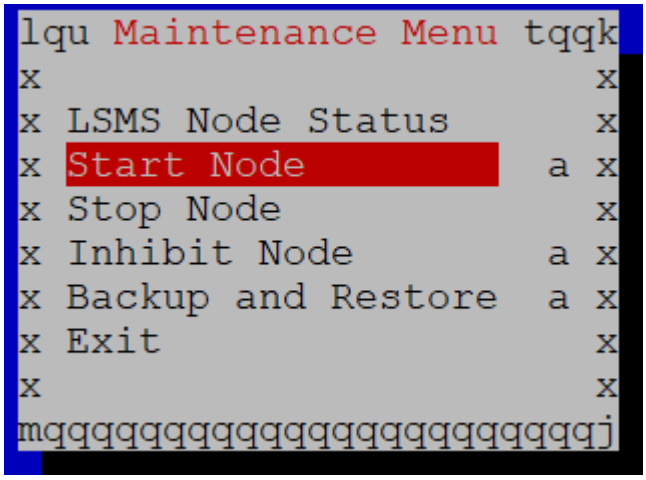
6. Start both LSMSPRI and LSMSSEC nodes.
   a. Login to LSMSMGR menu on LSMSPRI and go to **Maintenance Menu** and then **Start Node**.

Figure 5-53 Maintenance



   b. Select **Start Node** from the menu.

Figure 5-54 Start Node



c. Repeat step 6 to start node on the LSMSSEC server.

Switching NPAC agent version - Older to Newer

Do the following steps to switch to the newer npacagent version:

1. Login to LSMS CLI with user `lsmsadm`.
2. Shutdown both the LSMSPRI and LSMSSEC nodes.
   a. Login to LSMSMGR menu on LSMSPRI and go to **Maintenance Menu** and then **Stop Node**.

Figure 5-55 Main Menu

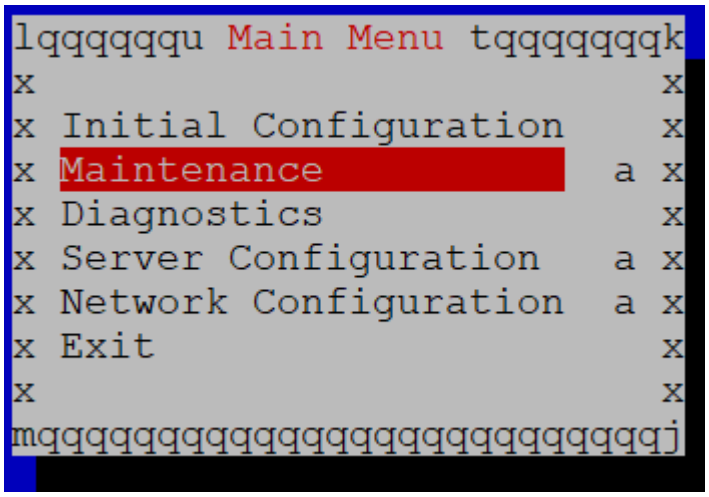
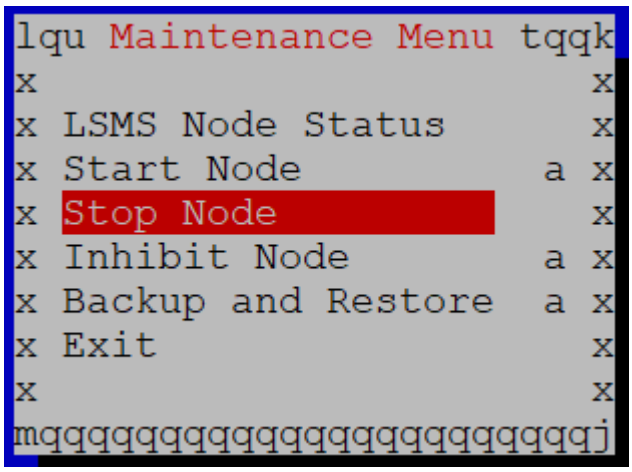


Figure 5-56 Stop Node



   b. Repeat the same steps to stop the node on LSMSEC server. Login to LSMSMGR menu and then go to the **Maintenance Menu** and then **Stop Node**.
3. Run the script with the following command on CLI:
   `/usr/TKLC/lsms/bin/switch_NANC528`

4. User is prompted to enter YES/NO depending upon the requirement of switching to the newer npacagent version as follows:

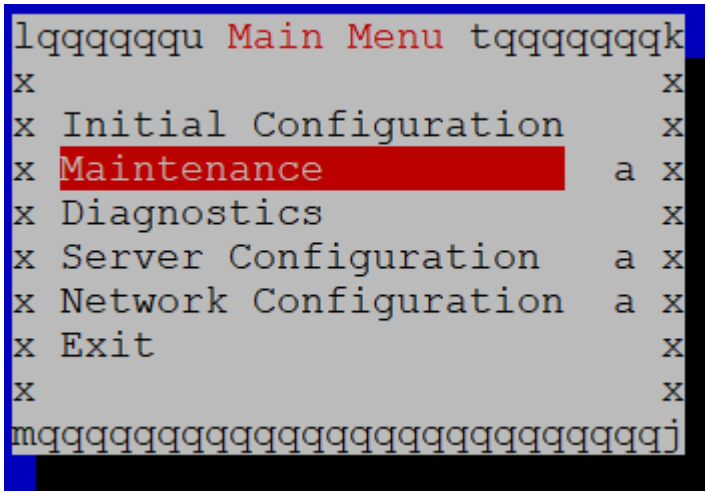
```
[lsmsadm@lsmspri ~]$ /usr/TKLC/lsms/bin/switch_NANC528
INFO: This script is used for switching between older and newer
npacagent. LSMS should be stopped for this process to continue.
Checking whether LSMS is stopped...

INFO: No active node found, We can proceed...

INFO: You are going to switch to newer version of npacagent that will
have NANC 528 updates.
Are you sure you want to continue? (y/n)
```

5. Enter **Y** to switch to the newer npacagent version.
Once the user enters **Y** to the above prompt, npacagent will move to the newer version. Below mentioned output will be observed on entering **Y** or **YES**:

```
INFO: Binary replaced successfully on local server, Replacing it on mate
now.
FIPS integrity verification test failed.
INFO: Binary replaced on mate successfully
```

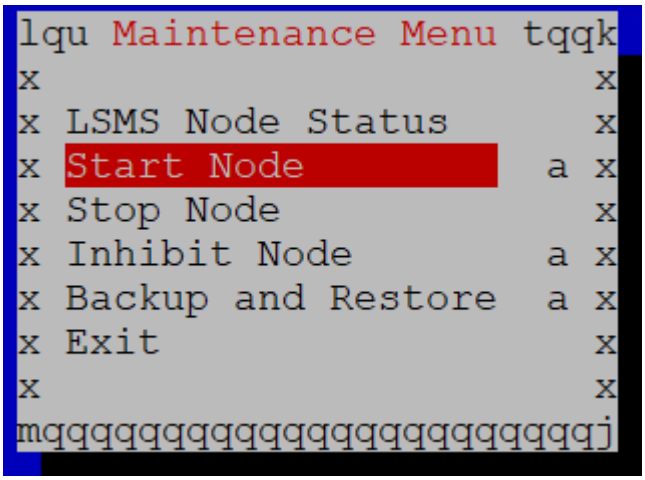
6. Start both LSMSPRI and LSMSSEC nodes.
   a. Login to LSMSMGR menu on LSMSPRI and go to **Maintenance Menu** and then **Start Node**.

Figure 5-57 Maintenance



   b. Select **Start Node** from the menu.

Figure 5-58 Start Node



c. Repeat step 6 to start node on the LSMSSEC server.

A

Configuring the Query Server

This appendix provides overview information as well as detailed, step-by-step configuration procedures to get the query server up-and-running.

Overview of the Query Server Package

The optional **LSMS** Query Server Package enables customers to access real time **LNP** data —automatically—using a standard **API**. Customers can perform customized, high volume automated data queries for use by internal office and support systems such as systems for service assurance, testing, service fulfillment, and customer care.

The Query Server Package provides a query server database which consists of replicated copies of the **LSMS LNP** databases, as shown in Table A-1 through Table A-2. The provision of this database enables customers to write applications, using **SQL**, **ODBC**, or **JDBC** interfaces, to access the data in the database. The query server supports direct query of objects and attributes in the database. The user has the flexibility to customize **SQL** queries in order to create new queries. No predefined queries are provided with this feature.

The query server resides on a separate platform from the **LSMS**, and maintains a separate and distinct copy of the **LNP** data. Customers must provide their own hardware system that is consistent with the platform specifications provided by Oracle Communications. Hosting a copy of the **LSMS** database on this separate platform provides the following benefits:

- High volumes of customized queries can be performed without processing impact on the **LSMS**. These queries are standard, non-updating **SQL** queries.
- Live backups of the database can be accomplished by performing a backup on the query server.

> **Note:**
>
> For purposes of quantifying the number of **EAGLE** nodes supported by the **LSMS** (so that the maximum number of supported **EAGLE** nodes is not exceeded), each query server supported must be counted as one **EAGLE** node. For example, if the **LSMS** is configured to support 8 pairs of **EAGLE**, each query server constitutes one **EAGLE** node (half of a pair).

If additional query servers are desired after the maximum number of supported **EAGLE** is reached, customers can daisy-chain additional query servers from a query server that is directly-connected to the **LSMS**. However, the **LSMS** cannot monitor connectivity to, or status of, daisy-chained query servers.

This feature includes the complete software package as well as information about notifications, the automated system check feature, configuration, maintenance, platform requirements and recommendations, the **LSMS** command line utility and command summary, and the query server error log.

> **Note:**
>
> Installation and configuration of software at the query server and the **LSMS** are supported. The feature provides for the replication of the data to the query server. Applications, network configuration to the query server, and development of interfaces to the query server database are the responsibility of the customer. For information about the database structure to be used to develop customer-provided applications, refer to the *Alarms and Maintenance Guide*.

Enable Query Server Feature

To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal QUERY_SERVER <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.

The Query Server can now be configured according to procedures contained in this Appendix.

Enable ResyncDB Query Server Feature

The ResyncDB Query Server feature enables the LSMS to directly host the ResyncDB Query Server. To enable this feature, perform this procedure:

1. Login to the LSMS as `lsmsadm`.
2. Issue the command `dbcfginternal RESYNCDB_QUERY_SERVER <Y|N>`.

   Use the value Y to enable the feature and N to disable the feature.
3. The value of RESYNCDB_QUERY_SERVER will be updated in the database.

After setting the values to "Y," the ResyncDB Query Server can now be configured according to procedures contained in the Query Server Feature Technical Reference, TR005579.

Overview of Database Replication

The query server system is provisioned from the Oracle Communications **LSMS** using database replication techniques provided by MySQL, as illustrated in Figure A-1. The one-way replication functionality is based on a master-slave relationship between two or more servers, with one (the **LSMS**) acting as the master, and others (query servers) acting as slaves. The **LSMS** keeps a binary log of updates (creates, modifies, deletes, etc.) that is made available to one or more query servers.

The query servers run on separate hardware, connected by the network. Each query server, upon connecting to the **LSMS**, informs the **LSMS** where it left off since the last successfully propagated update, synchronizes itself by reading the **LSMS**'s binary log file and executing the same actions on its copy of the data, then blocks and waits for new updates to be processed.

The slave servers mirror these changes a short time after they occur on the **LSMS**. Other than the brief periods when query servers are synchronizing, each query server mirrors the **LSMS**. If the **LSMS** becomes unavailable or the query server loses connectivity with the master, the query server tries to reconnect every 60 seconds until it is able to reconnect and resume listening for updates. The amount of time a query server can be disconnected (not replicating) from the **LSMS** before it can no longer reconnect and resume replication and must be completely reloaded is dependent only on the availability of the binary log files on the **LSMS**. The **LSMS** application actively manages the number of binary logs available on the server, always keeping the ten most recent binary log files (up to 10 **GB** worth of updates).

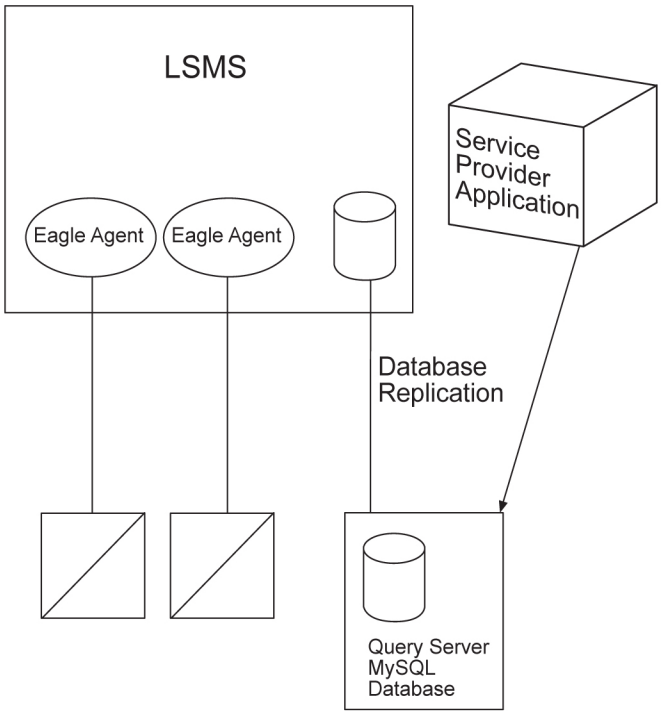
The purging of binary logs may occur. If there is some connectivity issue between the Query Server and the LSMS, the binary logs will not be removed. In this case, logs are forcefully removed if BIN_LOG_THRESHOLD parameter is set.

If the query server database becomes corrupted or back-level such that it cannot be automatically resynchronized, you can reload it from either the **LSMS** or from another query server (for more information, refer to the *Alarms and Maintenance Guide*).

Query servers connect to the **LSMS** application using a **VIP** (virtual **IP**) address on the application network. The **VIP** address ensures that query servers are constantly connected to the active server. In the event of an application switch over in which the active **LSMS** server changes (for instance, from server A to server B), the query servers follow the active server and reconnect automatically to the new active **LSMS** server.

To enable this capability, the **LSMS** application actively manages the binary logs on both servers to ensure they remain synchronized. It is important that the binary logs on the **LSMS** servers are not removed or reset except by the **LSMS** application, because this change could negatively impact the database replication occurring between the two **LSMS** servers as well as the query servers.

Figure A-1 LSMS Query Server Overview



LNP Data Replicated on the Query Server

The **LSMS** supports replication of the following **LNP** data to a local or remote query server:

- Telephone Number (Subscription Version) (**NPAC** data)
  - Version **ID**
  - **TN**
  - **LRN**
  - Service Provider
  - **CLASSDPC**, **SSN**
  - **CNAMDPC**, **SSN**
  - **ISVMDPC**, **SSN**
  - **LIDBDPC**, **SSN**
  - **WSMSCDPC**, **SSN** (if optional feature is provisioned)
  - **LNP** type
  - Billing **ID**
  - End User Location
  - End User Value
  - Activation Timestamp
  - Download reason
  - SV Type
  - Alternative SPID
- Number Pool Block (**NPAC** data)
  - Block **ID**
  - **NPA**-**NXX**-X
  - **LRN**
  - Service Provider
  - **CLASSDPC**, **SSN**
  - **CNAMDPC**, **SSN**
  - **ISVMDPC**, **SSN**
  - **LIDBDPC**, **SSN**
  - **WSMSCDPC**, **SSN** (if optional feature is provisioned)
  - Activation Timestamp
  - Download reason
  - SV Type
  - Alternative SPID
- **NPAC** network data (for example, **LRN**, **NPA**-**NXX**) (**NPAC** data)

- Default **GTT** (locally provisioned data)
- Override **GTT** (locally provisioned data)
- **NPA** Split information (locally provisioned data)
- **TN** filters (locally provisioned data)

The Query Server database consists of replicated copies of the **LSMS LNP** database tables as shown below.

> **Note:**
>
> In the table below, names of regional LNP database tables and fields may be split between lines. This does not imply a space in the name of the table or field.

Table A-1 Regional Database Tables and Fields

Regional (<Region>) DB) LNP Database Tables	Fields			
SubscriptionVersion	versionID	tn	lrn	newCurrentSp
	classDPC	classSSN	lidbDPC	lidbSSN
	isvmDPC	isvmSSN	cnamDPC	cnamSSN
	wsmscDPC	wsmscSSN	LnpType	billingId
	endUserLocation Value	endUserLocation Type	activation Timestamp	downloadReason
	SVType	alternativeSPID		
NumberPoolBlock	blockId	npanxx_x	lrn	newCurrentSP
	classDPC	classSSN	lidbDPC	lidbSSN
	isvmDPC	isvmSSN	cnamDPC	cnamSSN
	wsmscDPC	wsmscSSN	activation Timestamp	downloadReason
	SVType	alternativeSPID		
ServiceProvLRN	serviceProviderId	id	lrn	creationTimeStamp
	downloadReason			
ServiceProv NPA_NXX	serviceProviderId	id	npanxx	creationTimeStamp
	effective TimeStamp	downloadReason		
ServiceProv NPA_NXX_X	serviceProviderId	id	npanxx_x	creationTimeStamp
	effective TimeStamp	modified TimeStamp	downloadReason	
ServiceProv Network	serviceProvId	serviceProvName	serviceProvType	
Where <Region> is one of the following:	Canada	MidAtlantic	Midwest	Northeast
	Southeast	Southwest	WestCoast	Western

Below is detailed information about the Regional Database table and fields.

> **Note:**
>
> The following information was taken from actual source code. It may contain irrelevant data, such as comments.

```
--
-- Create SubscriptionVersion table
--
-- The Fields are defined in the order and format that are defined by
the
-- NPAC bulk data file. This allows the SQL LOAD DATA command to be
used
-- to load tables which is extremely fast.
--
-- Revision History
-- 15-may-07  ARICENT  Feature 110663: NANC 399
--
CREATE TABLE  SubscriptionVersion
(
    -- Required field (Primary key)
    versionId            INT             NOT NULL,

    -- Required field (10 numeric character unique key)
    tn                   CHAR(10)        NOT NULL,

    -- Optional field (10 numeric characters, Empty string means not
present)
    lrn                  CHAR(10)        NOT NULL DEFAULT "",

    -- Required field (1-4 characters)
    newCurrentSp         CHAR(4)         NOT NULL DEFAULT "0000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    activationTimestamp  CHAR(14)        NOT NULL DEFAULT
"00000000000000",

    -- Optional field (9 characters, Empty string means not present)
    classDPC             CHAR(9)         NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    classSSN             CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    lidbDPC              CHAR(9)         NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    lidbSSN              CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    isvmDPC              CHAR(9)         NOT NULL DEFAULT "",
```

```
    -- Optional field (1-3 characters, Empty string means not present)
    isvmSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    cnamDPC              CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    cnamSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (1-12 numeric characters, Empty string means not
present)
    endUserLocationValue CHAR(12)         NOT NULL DEFAULT "",

    -- Optional field (2 numeric characters, Empty string means not present)
    endUserLocationType  CHAR(2)          NOT NULL DEFAULT "",

    -- Required field (1-4 characters, Empty string means not present)
    billingId            CHAR(4)          NOT NULL DEFAULT "",

    -- Required field (lspp(0), lisp(1), pool(2))
    lnpType              TINYINT UNSIGNED NOT NULL DEFAULT 0,

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason       TINYINT UNSIGNED NOT NULL DEFAULT 0,

    -- Optional field (9 characters, Empty string means not present)
    wsmscDPC             CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    wsmscSSN             CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field  (wireline(0), wireless(1), voIP(2), voWiFi(3),
sv_type_4(4), sv_type_5(5), sv_type_6(6) )
    svType TINYINT NOT NULL DEFAULT -1,

    -- Optional field (1-4 CHARACTERS)
    alternativeSPIDCHAR(4)         NOT NULL DEFAULT "",

    -- Primay key is the Npac SubscriptionVersion id
    PRIMARY KEY (versionId),

    -- TN must be indexed and unique
    UNIQUE KEY tn (tn),

    -- Index lrn, for LSMS Subscription Version by LRN reports
    INDEX (lrn),

    -- Index lrn, for LSMS Subscription Version by SPID reports
    INDEX (newCurrentSp)

)
TYPE = MyIsam;

--
-- Create NumberPoolBlock table
```

```
--
-- The Fields are defined in the order and format that are defined by
the
-- NPAC bulk data file. This allows the SQL LOAD DATA command to be
used
-- to load tables which is extremely fast.
--
CREATE TABLE  NumberPoolBlock
(
    -- Required field (Primary key)
    blockId              INT             NOT NULL,

    -- Required field (7 numeric characters, Unique key)
    npanxx_x             CHAR(7)         NOT NULL,

    -- Optional field (10 numeric characters, Empty string means not
present)
    lrn                  CHAR(10)        NOT NULL DEFAULT "",

    -- Required field (1-4 characters)
    newCurrentSp         CHAR(4)         NOT NULL DEFAULT "0000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    activationTimestamp  CHAR(14)        NOT NULL DEFAULT
"00000000000000",

    -- Optional field (9 characters, Empty string means not present)
    classDPC             CHAR(9)         NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    classSSN             CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    lidbDPC              CHAR(9)         NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    lidbSSN              CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    isvmDPC              CHAR(9)         NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    isvmSSN              CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    cnamDPC              CHAR(9)         NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    cnamSSN              CHAR(3)         NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    wsmscDPC             CHAR(9)         NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    wsmscSSN             CHAR(3)         NOT NULL DEFAULT "",

    -- Required field (new(0), delete(1), modified(2), audit-
descrepancy(3)

    downloadReason       TINYINT UNSIGNED NOT NULL DEFAULT 0,
```

```
    -- Optional field  (wireline(0), wireless(1), voIP(2), voWiFi(3),
sv_type_4(4), sv_type_5(5), sv_type_6(6) )
    svType TINYINT NOT NULL DEFAULT -1,

    -- Optional field (1-4 CHARACTERS)
    alternativeSPID     CHAR(4)         NOT NULL DEFAULT "",

    -- Primay key is the Npac NumberPoolBlock id
    PRIMARY KEY (blockId),

    -- TN must be indexed and unique
    UNIQUE KEY npanxx_x (npanxx_x),

    -- Index lrn, for LSMS Number Pool Block by LRN reports
    INDEX (lrn),

    -- Index lrn, for LSMS Number Pool Block by SPID reports
    INDEX (newCurrentSp)
)
TYPE = MyIsam;

--
-- Create ServiceProvNetwork table
--
-- The Fields are defined in the order and format that are defined by the
-- NPAC bulk data file
--
CREATE TABLE ServiceProvNetwork
(
    -- Required field (Primary key)
    serviceProvId    CHAR(4)       NOT NULL,

    -- Required field (1 - 40 characters)
    serviceProvName  CHAR(40)      NOT NULL DEFAULT "",

     -- Service Provider type
    serviceProvType  ENUM("wireline", "wireless", "non_carrier",
"sp_type_3",
"sp_type_4", "sp_type_5") NULL DEFAULT NULL,

    -- Prmary key is the Service Provider ID
    PRIMARY KEY (serviceProvId)
)
TYPE = MyIsam;

--
-- Create ServiceProvLRN table
--
-- The Fields are defined in the order that are defined by the
-- NPAC bulk data file
--
CREATE TABLE ServiceProvLRN
(
    -- Foreign key -> ServiceProvNetwork
```

```
    serviceProvId     CHAR(4)   NOT NULL,

    -- Required field (Primary key within each ServiceProvNetwork)
    id                INT       NOT NULL,

    -- Required field (10 numeric characters)
    lrn               CHAR(10)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp CHAR(14)  NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-
descrepancy(3)
    downloadReason    TINYINT   NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- Lrn is unique key within each ServiceProvNetwork
    UNIQUE KEY lrn (serviceProvId, lrn),

    -- Index lrn
    INDEX (lrn),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES
ServiceProvNetwork(serviceProvId)
)
TYPE = MyIsam;

--
-- Create ServiceProvNPA_NXX table
--
-- The Fields are defined in the order defined by the NPAC bulk data
file
-- but the npac file formats the npanxx as 'npa-nxx'.
--
CREATE TABLE ServiceProvNPA_NXX
(
    -- Foreign key -> ServiceProvNetwork
    serviceProvId      CHAR(4)  NOT NULL,

    -- Required field (Primary Unique Key)
    id                 INT      NOT NULL,

    -- Required field (6 numeric characters)
    npanxx             CHAR(6)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    effectiveTimeStamp CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-
```

```
descrepancy(3)
    downloadReason     TINYINT  NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- NpaNxx is unique key within each ServiceProvNetwork
    UNIQUE KEY npanxx (serviceProvId, npanxx),

    -- Index npanxx
    INDEX (npanxx),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES ServiceProvNetwork(serviceProvId)

)
TYPE = MyIsam;

--
-- Create ServiceProvNPA_NXX_X table
--
-- The Fields are defined in the order defined by the NPAC bulk data file
-- but the npac file formats the npanxx as 'npa-nxx-x'.
--
CREATE TABLE ServiceProvNPA_NXX_X
(
    -- Foreign key -> ServiceProvNetwork
    serviceProvId      CHAR(4)  NOT NULL,

    -- Required field (Primary Unique Key)
    id                 INT      NOT NULL,

    -- Required field (7 numeric characters)
    npanxx_x           CHAR(7)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    effectiveTimeStamp CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    modifiedTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason     TINYINT  NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- NpaNxx is unique key within each ServiceProvNetwork
    UNIQUE KEY npanxx_x (serviceProvId, npanxx_x),

    -- Index npanxx_x
    INDEX (npanxx_x),
```

```
    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES
ServiceProvNetwork(serviceProvId)
)
TYPE = MyIsam;
```

> **Note:**
>
> In the table below, names of regional LNP database tables and fields may be split between lines. This does not imply a space in the name of the table or field.

Table A-2 Supplemental Database Tables and Fields

Supplemental (supDB) LNP Database Tables	Fields			
AlarmFilter	eventNumber	activateSurvFilteri ng	filterType	timeStamp
	timeout	counter		
DefaultGtt	groupName	npanxx	spid	
	ain_set	ain_tt	ain_dpc	ain_ssn
	ain_xlat	ain_ri	ain_ngt	ain_rgta
	in_set	in_tt	in_dpc	in_ssn
	in_xlat	in_ri	in_ngt	in_rgta
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta
OverrideGtt	groupName	lrn	spid	
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn

Table A-2 (Cont.) Supplemental Database Tables and Fields

Supplemental (supDB) LNP Database Tables	Fields			
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta
NpaSplit	oldNpa	newNpa	nxx	startPDP
	endPDP	region	status	
LsmsService Provider	spid	description	contactInfo	
GttGroup	name	description		
	ain_set	ain_tt	ain_dpc	ain_ssn
	ain_xlat	ain_ri	ain_ngt	ain_rgta
	in_set	in_tt	in_dpc	in_ssn
	in_xlat	in_ri	in_ngt	in_rgta
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta
EmsInterface	clli	emsType	primaryAddress	secondaryAddress
	mateClii	pointCode	matePointCode	capabilityPointCode
	gttGroup	tnFilter	ownerSpid	componentInfo
	contactInfo	dcmAddress	retryinterval	retryCount
	pingMethod			
TnFilter	spid	name	description	filterType
	regions	npanxxType	npanxxs	
NpacRegion	region	npacSmsName	lsmsPsel	lsmsSsel
	lsmsTsel	lsmsNsap	primaryNpacPsel	primaryNpacSsel
	primaryNpacTsel	primaryNpacNsap	primaryNpacFtpAddress	secondaryNpacPsel
	secondaryNpacSsel	secondaryNpacTsel	secondaryNpacNsap	secondaryNpacFtpAddress
	active	componentInfo	contactInfo	lastChangedTimestamp
	currentNpac			
<Region>Npac Measurements	yyyydddhh	Binds	SuccessOps	FailedOps
<Clii>Eagle Measurements	yyyydddhh			
	updTnSuccess	updTnFail	DelTnSuccess	DelTnFail
	updDGttSuccess	updDGttFail	DelDGttSuccess	DelDGttFail

Table A-2 (Cont.) Supplemental Database Tables and Fields

Supplemental (supDB) LNP Database Tables	Fields			
	updOGttSuccess	updOGttFail	DelOGttSuccess	DelOGttFail
	updSplitSuccess	updSplitFail	DelSplitSuccess	DelSplitFail
	Binds	LsmsRetries	NERetries	
<Region>PublicKey	id	listId	keyId	status
	exponent	modulus		
<Region>PrivateKey	id	listId	keyId	status
	keyval			
LsmsUser	name	golden	groupName	inactivityTimeout
LsmsUserSpid	lsmsUser	spid		
Where <Region> is one of the following:	Canada	MidAtlantic	Midwest	Northeast
	Southeast	Southwest	WestCoast	Western
Where <Clii> is the Common Language Location Indicator of the EMS/EAGLE to which that LSMS is connected.				

Note:

By default, the following Supplemental (SupDB) **LNPDatabase** Tables are not replicated:

- <Region>PublicKey
- <Region>PrivateKey
- LsmsUser
- LsmsUserSpid

To replicate these tables, see the Notes in #unique_170/unique_170_Connect_42_V998816 of the topic #unique_170.

Below is detailed information about the Supplemental Database tables and fields.

Note:

The following information was taken from actual source code. It may contain irrelevant data, such as comments.

```
--
-- Create NpacRegion table
--
-- One NpacRegion defines the configuration of the primary and
secondary NPAC.
```

```
--
-- Revision History
--
-- 19-Dec-03  Groff  Feature 53384: Customizable Login Message.
-- 14-Jul-06  FSS    Feature 103276: Password Expiration.
-- 14-may-07  ARICENT  Feature 110663: NANC 399
--
CREATE TABLE  NpacRegion
(
    -- Region name
    region               VARCHAR(40)  NOT NULL,

    -- SMS Name defined by NPAC
    npacSmsName          TINYBLOB,

    -- OSI address of LSMS
    lsmsPsel              TINYBLOB,
    lsmsSsel              TINYBLOB,
    lsmsTsel              TINYBLOB,
    lsmsNsap              TINYBLOB,

    -- OSI address of primary NPAC
    primaryNpacPsel       TINYBLOB,
    primaryNpacSsel       TINYBLOB,
    primaryNpacTsel       TINYBLOB,
    primaryNpacNsap       TINYBLOB,

    primaryNpacFtpAddress TINYBLOB,

    -- OSI address of secondary NPAC
    secondaryNpacPsel     TINYBLOB,
    secondaryNpacSsel     TINYBLOB,
    secondaryNpacTsel     TINYBLOB,
    secondaryNpacNsap     TINYBLOB,

    secondaryNpacFtpAddress TINYBLOB,

    -- Region is active
    active               BOOL        NOT NULL DEFAULT 0,

    -- Component Info (stored as CSV string)
    componentInfo        BLOB        NOT NULL,
    -- Contact Info (stored as CSV string)
    contactInfo        BLOB          NOT NULL,

    -- Last changed timestamp set by npacagent
    lastChangedTimestamp CHAR(14)    NOT NULL, -- Default now

    -- Current npac in use set by npacagent
    currentNpac          ENUM("Primary", "Secondary") DEFAULT "Primary",

    -- Region name is primary key
    PRIMARY KEY (region)
)
TYPE = MyIsam;
```

```
INSERT INTO NpacRegion
    (region, npacSmsName,
     lsmsPsel, lsmsSsel, lsmsTsel, lsmsNsap,
     primaryNpacPsel, primaryNpacSsel, primaryNpacTsel,
primaryNpacNsap, primaryNpacFtpAddress,
     secondaryNpacPsel, secondaryNpacSsel, secondaryNpacTsel,
secondaryNpacNsap, secondaryNpacFtpAddress,
     componentInfo, contactInfo, lastChangedTimestamp)
    VALUES ("Canada", "Region8 NPAC Canada",
            "psel", "ssel", "", "000000000000",
            "cw7", "cw7", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234",
"1234","9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("MidAtlantic", "Mid-Atlantic Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw1", "cw1", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234",
"1234","9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("Midwest", "Midwest Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw0", "cw0", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234",
"1234","9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("Northeast", "Northeast Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw2", "cw2", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234",
"1234","9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("Southeast", "Southeast Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
```

```
            "cw3", "cw3", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1234"
,"9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("Southwest", "Southwest Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw4", "cw4", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1234"
,"9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("WestCoast", "West Coast Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw6", "cw6", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1234"
,"9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("Western", "Western Regional NPAC SMS",
            "psel", "ssel", "", "000000000000",
            "cw5", "cw5", "", "000000000000",
            "0.0.0.0",
            "", "", "", "000000000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1234"
,"9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s"));

--
-- Create  LsmsServiceProvider table
--
CREATE TABLE  LsmsServiceProvider
(
    -- The service provider id (Primary Key)
    spid        CHAR(4)   NOT NULL,

    -- Description of the service provider
    description CHAR(80)  NOT NULL,

    -- Contact Info (stored as comma separated value string)
```

```
    contactInfo BLOB NOT NULL,

    -- Primary key is the spid
    PRIMARY KEY (spid)
)
TYPE = MyIsam;

--
-- Create  LsmsUser table
--
CREATE TABLE  LsmsUser
(
    -- The user name (Primary Key)
    name    CHAR(64) NOT NULL,

    -- Description of the service provider
    golden  BOOL     NOT NULL DEFAULT 0,

    -- The assigned permission group
    groupName    CHAR(64) NOT NULL,

    -- The assigned inactivity timeout
    inactivityTimeout    CHAR(11) NOT NULL DEFAULT '-1',

    -- The user level password timeout
    UsrPwdExpInterval SMALLINT NOT NULL DEFAULT -1,

    -- The first logon flag
    FirstLogonFlag    BIT NOT NULL DEFAULT 0,

    -- The password changed date
    LastUpdDate       DATE NOT NULL DEFAULT '1970-01-01',

    -- Primary key is the user name
    PRIMARY KEY (name)
)
TYPE = MyIsam;
-- Create default 'golden' users
INSERT INTO LsmsUser (name, golden, groupName)
            VALUES('lsmsadm',1,'lsmsadm'),
                  ('lsmsuser',1,'lsmsuser'),
                  ('lsmsview',1,'lsmsview'),
                  ('lsmsall',1,'lsmsall'),
                  ('lsmsuext',1,'lsmsuext'),
                  ('command-line',1,'lsmsadm');
--
-- Create  GttGroup table
--
CREATE TABLE  GttGroup
(
    -- The group name (Primary Key)
    name        CHAR(64)   NOT NULL,

    -- Description of the GttGroup
    description CHAR(80)  NOT NULL,
```

```
-- Services in GttGroup are for storing default TT/SSN values
-- AIN Service
ain_set  BOOL    NOT NULL DEFAULT 0,
ain_tt   TINYINT UNSIGNED NOT NULL,
ain_dpc  CHAR(9) NOT NULL,
ain_ssn  CHAR(3) NOT NULL,
ain_xlat TINYINT UNSIGNED NOT NULL,
ain_ri   TINYINT UNSIGNED NOT NULL,
ain_ngt  TINYINT UNSIGNED NOT NULL,
ain_rgta BOOL    NOT NULL,
-- IN Service
in_set  BOOL    NOT NULL DEFAULT 0,
in_tt   TINYINT UNSIGNED NOT NULL,
in_dpc  CHAR(9) NOT NULL,
in_ssn  CHAR(3) NOT NULL,
in_xlat TINYINT UNSIGNED NOT NULL,
in_ri   TINYINT UNSIGNED NOT NULL,
in_ngt  TINYINT UNSIGNED NOT NULL,
in_rgta BOOL    NOT NULL,
-- CLASS Service
class_set  BOOL    NOT NULL DEFAULT 0,
class_tt   TINYINT UNSIGNED NOT NULL,
class_dpc  CHAR(9) NOT NULL,
class_ssn  CHAR(3) NOT NULL,
class_xlat TINYINT UNSIGNED NOT NULL,
class_ri   TINYINT UNSIGNED NOT NULL,
class_ngt  TINYINT UNSIGNED NOT NULL,
class_rgta BOOL    NOT NULL,
-- LIDB Service
lidb_set  BOOL    NOT NULL DEFAULT 0,
lidb_tt   TINYINT UNSIGNED NOT NULL,
lidb_dpc  CHAR(9) NOT NULL,
lidb_ssn  CHAR(3) NOT NULL,
lidb_xlat TINYINT UNSIGNED NOT NULL,
lidb_ri   TINYINT UNSIGNED NOT NULL,
lidb_ngt  TINYINT UNSIGNED NOT NULL,
lidb_rgta BOOL    NOT NULL,
-- ISVM Service
isvm_set  BOOL    NOT NULL DEFAULT 0,
isvm_tt   TINYINT UNSIGNED NOT NULL,
isvm_dpc  CHAR(9) NOT NULL,
isvm_ssn  CHAR(3) NOT NULL,
isvm_xlat TINYINT UNSIGNED NOT NULL,
isvm_ri   TINYINT UNSIGNED NOT NULL,
isvm_ngt  TINYINT UNSIGNED NOT NULL,
isvm_rgta BOOL    NOT NULL,
-- CNAM Service
cnam_set  BOOL    NOT NULL DEFAULT 0,
cnam_tt   TINYINT UNSIGNED NOT NULL,
cnam_dpc  CHAR(9) NOT NULL,
cnam_ssn  CHAR(3) NOT NULL,
cnam_xlat TINYINT UNSIGNED NOT NULL,
cnam_ri   TINYINT UNSIGNED NOT NULL,
cnam_ngt  TINYINT UNSIGNED NOT NULL,
```

```
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- Primary key is the group name
    PRIMARY KEY (name)
)
TYPE = MyIsam;

--
-- Create GttGroupSpid table
--
-- This table is used to associate a GttGroup to an authorized
-- LsmsServiceProvider. The many-many relationship between the two
-- is stored by this table a group-spid combinations.
--
CREATE TABLE  GttGroupSpid
(
    -- Group name
    gttGroup    CHAR(64) NOT NULL,

    -- Spid
    spid        char(4) NOT NULL,

    -- Force GttGroup,LsmsServiceProvider combinations to be unique
    PRIMARY KEY (gttGroup, spid),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (gttGroup) REFERENCES GttGroup(groupName),
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)
)
TYPE = MyIsam;

--
-- Create LsmsUserSpid table
--
-- This table is used to associate a LsmsUser to an authorized
-- LsmsServiceProvider. The many-many relationship between the two
-- is stored by this table a group-spid combinations.
--
CREATE TABLE  LsmsUserSpid
(
    -- User name
    lsmsUser    CHAR(64) NOT NULL,

    -- Spid
    spid        CHAR(4) NOT NULL,
```

```
    -- Force LsmsUser,LsmsServiceProvider combinations to be unique
    PRIMARY KEY (lsmsUser, spid),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (lsmsUser) REFERENCES LsmsUser(name),
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)
)
TYPE = MyIsam;

--
-- Create DefaultGTT Table
--
CREATE TABLE  DefaultGtt
(
    -- The group this DefaultGtt belongs to
    groupName  CHAR(64) NOT NULL, -- Foreign key

    -- NPA-NXX of the DefaultGtt
    npanxx     CHAR(6) NOT NULL,

    -- The SPID that created the DefaultGtt
    spid       CHAR(4) NOT NULL,

    -- AIN Service
    ain_set  BOOL    NOT NULL DEFAULT 0,
    ain_tt   TINYINT UNSIGNED NOT NULL,
    ain_dpc  CHAR(9) NOT NULL,
    ain_ssn  CHAR(3) NOT NULL,
    ain_xlat TINYINT UNSIGNED NOT NULL,
    ain_ri   TINYINT UNSIGNED NOT NULL,
    ain_ngt  TINYINT UNSIGNED NOT NULL,
    ain_rgta BOOL    NOT NULL,
    -- IN Service
    in_set  BOOL    NOT NULL DEFAULT 0,
    in_tt   TINYINT UNSIGNED NOT NULL,
    in_dpc  CHAR(9) NOT NULL,
    in_ssn  CHAR(3) NOT NULL,
    in_xlat TINYINT UNSIGNED NOT NULL,
    in_ri   TINYINT UNSIGNED NOT NULL,
    in_ngt  TINYINT UNSIGNED NOT NULL,
    in_rgta BOOL    NOT NULL,
    -- CLASS Service
    class_set  BOOL    NOT NULL DEFAULT 0,
    class_tt   TINYINT UNSIGNED NOT NULL,
    class_dpc  CHAR(9) NOT NULL,
    class_ssn  CHAR(3) NOT NULL,
    class_xlat TINYINT UNSIGNED NOT NULL,
    class_ri   TINYINT UNSIGNED NOT NULL,
    class_ngt  TINYINT UNSIGNED NOT NULL,
    class_rgta BOOL    NOT NULL,
    -- LIDB Service
    lidb_set  BOOL    NOT NULL DEFAULT 0,
    lidb_tt   TINYINT UNSIGNED NOT NULL,
    lidb_dpc  CHAR(9) NOT NULL,
    lidb_ssn  CHAR(3) NOT NULL,
```

```
    lidb_xlat TINYINT UNSIGNED NOT NULL,
    lidb_ri   TINYINT UNSIGNED NOT NULL,
    lidb_ngt  TINYINT UNSIGNED NOT NULL,
    lidb_rgta BOOL    NOT NULL,
    -- ISVM Service
    isvm_set  BOOL    NOT NULL DEFAULT 0,
    isvm_tt   TINYINT UNSIGNED NOT NULL,
    isvm_dpc  CHAR(9) NOT NULL,
    isvm_ssn  CHAR(3) NOT NULL,
    isvm_xlat TINYINT UNSIGNED NOT NULL,
    isvm_ri   TINYINT UNSIGNED NOT NULL,
    isvm_ngt  TINYINT UNSIGNED NOT NULL,
    isvm_rgta BOOL    NOT NULL,
    -- CNAM Service
    cnam_set  BOOL    NOT NULL DEFAULT 0,
    cnam_tt   TINYINT UNSIGNED NOT NULL,
    cnam_dpc  CHAR(9) NOT NULL,
    cnam_ssn  CHAR(3) NOT NULL,
    cnam_xlat TINYINT UNSIGNED NOT NULL,
    cnam_ri   TINYINT UNSIGNED NOT NULL,
    cnam_ngt  TINYINT UNSIGNED NOT NULL,
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- DefaultGtt npanxx's are unique within each group
    PRIMARY KEY (groupName, npanxx),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (groupName) REFERENCES GttGroup(name)
)
TYPE = MyIsam;

--
-- Create OverrideGtt Table
--
CREATE TABLE  OverrideGtt
(
    -- The group this OverrideGtt belongs to
    groupName  CHAR(64) NOT NULL, -- Foreign key

    -- LRN of the OverrideGtt
    lrn        CHAR(10) NOT NULL,

    -- The SPID that created the OverrideGtt
    spid       CHAR(4)  NOT NULL,

    -- CLASS Service
```

```
    class_set  BOOL    NOT NULL DEFAULT 0,
    class_tt   TINYINT UNSIGNED NOT NULL,
    class_dpc  CHAR(9) NOT NULL,
    class_ssn  CHAR(3) NOT NULL,
    class_xlat TINYINT UNSIGNED NOT NULL,
    class_ri   TINYINT UNSIGNED NOT NULL,
    class_ngt  TINYINT UNSIGNED NOT NULL,
    class_rgta BOOL    NOT NULL,
    -- LIDB Service
    lidb_set  BOOL    NOT NULL DEFAULT 0,
    lidb_tt   TINYINT UNSIGNED NOT NULL,
    lidb_dpc  CHAR(9) NOT NULL,
    lidb_ssn  CHAR(3) NOT NULL,
    lidb_xlat TINYINT UNSIGNED NOT NULL,
    lidb_ri   TINYINT UNSIGNED NOT NULL,
    lidb_ngt  TINYINT UNSIGNED NOT NULL,
    lidb_rgta BOOL    NOT NULL,
    -- ISVM Service
    isvm_set  BOOL    NOT NULL DEFAULT 0,
    isvm_tt   TINYINT UNSIGNED NOT NULL,
    isvm_dpc  CHAR(9) NOT NULL,
    isvm_ssn  CHAR(3) NOT NULL,
    isvm_xlat TINYINT UNSIGNED NOT NULL,
    isvm_ri   TINYINT UNSIGNED NOT NULL,
    isvm_ngt  TINYINT UNSIGNED NOT NULL,
    isvm_rgta BOOL    NOT NULL,
    -- CNAM Service
    cnam_set  BOOL    NOT NULL DEFAULT 0,
    cnam_tt   TINYINT UNSIGNED NOT NULL,
    cnam_dpc  CHAR(9) NOT NULL,
    cnam_ssn  CHAR(3) NOT NULL,
    cnam_xlat TINYINT UNSIGNED NOT NULL,
    cnam_ri   TINYINT UNSIGNED NOT NULL,
    cnam_ngt  TINYINT UNSIGNED NOT NULL,
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- OverrideGtt lrns are unique within each group
    PRIMARY KEY (groupName, lrn),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (groupName) REFERENCES GttGroup(name)
)
TYPE = MyIsam;

--
-- Create EmsInterface table. A row in the EmsInterface table can represent
```

```
-- either a MpsInterface or a OapInterface object
--
CREATE TABLE  EmsInterface
(
    -- The CLLI (Primary Key)
    clli                CHAR(11)    NOT NULL,

    emsType             ENUM("OAP", "MPS", "TEKPATH") NOT NULL,

    -- The IP address of the primary interface
    primaryAddress      TINYBLOB    NOT NULL,

    -- The IP address of the secondary interface
    secondaryAddress    TINYBLOB    NOT NULL,

    -- The method to use to verify the presence of the MPS
    pingMethod          ENUM("PING", "SSH", "NONE") NOT NULL,

    -- The mate CLLI
    mateClli            CHAR(11)    NOT NULL,

    -- Point code
    pointCode           CHAR(9)     NOT NULL,

    -- Point code of the mate
    matePointCode       CHAR(9)     NOT NULL,

    -- Capability point code
    capabilityPointCode CHAR(9)     NOT NULL,

    -- GttGroup assigned to the EmsInteraface
    gttGroup            CHAR(64)    NOT NULL DEFAULT ""
        REFERENCES GttGroup(name),

    -- TnFilter assigned to the EmsInteraface
    tnFilter            CHAR(64)    NOT NULL DEFAULT ""
        REFERENCES TnFilter, -- via FOREIGN KEY (ownerSpid, tnfilter)

    -- ServiceProvider to which this EmsInterface is assigned
    ownerSpid           CHAR(4)     NOT NULL DEFAULT ""
        REFERENCES LsmsServiceProvider(spid),

    -- Component Info (stored as CSV string)
    componentInfo        BLOB        NOT NULL,
    -- Contact Info (stored as CSV string)
    contactInfo        BLOB          NOT NULL,

    -- The last fields are only used when the row represents a
    -- OAP interface. The row is used to construct both OapInterface
    -- objects and MpsInterface objects which are subclasses of
EmsInterface

    -- OAP dcmAddress
    dcmAddress        TINYBLOB NULL DEFAULT NULL,
```

```
    -- OAP retry interval
    retryInterval     INTEGER  NULL DEFAULT NULL,

    -- OAP retry count
    retryCount        INTEGER  NULL DEFAULT NULL,

    -- Primary key is the CLLI name
    PRIMARY KEY (clli),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (ownerSpid, tnFilter) REFERENCES TnFilter
)
TYPE = MyIsam;

--
-- Create TnFilter table. A row in the EmsInterface table can represent
-- either a RegionTnFilter or a NpaNxxTnFilter object
--
CREATE TABLE  TnFilter
(
    -- The LsmsServiceProvider this TnFilter belongs to
    spid           char(4)    NOT NULL,   -- Foreign key

    -- The name of the TnFilter
    name           CHAR(64)   NOT NULL,

    -- Description of the TnFilter
    description CHAR(80)  NOT NULL,

    -- The filter type (NpaNxxTnFilter or RegionalTnFilter)
    filterType     ENUM("Regional", "NpaNxx") NOT NULL,

    -- If RegionalTnFilter, the region to send
    regions        SET("Not Used", "Canada", "MidAtlantic", "Midwest",
"Northeast",
                       "Southeast", "Southwest", "WestCoast", "Western") NOT
NULL,

    -- If NpaNxxTnFilter, the filter type
    npanxxType     ENUM("Include", "Exclude") NOT NULL,

    -- If NpaNxxTnFilter, the npa-nxxs to send
    npanxxs        LONGBLOB NOT NULL,

    -- TnFilter names are unique within LsmsServiceProvider
    PRIMARY KEY (spid, name),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)

)
TYPE = MyIsam;

--
--  Create private and public key tables
```

```
--
--  The first four fields define a base class Key in the object
interface
--
--         +--- PrivateKey
--  Key <--|
--         +--- PublicKey
--
-- Each subclass and table has the key values for the key type.
--

--
-- Create "Model" PrivateKey table
--
CREATE TABLE IF NOT EXISTS PrivateKeyModel
(
    listId      INT UNSIGNED,
    keyId       INT UNSIGNED,
    status      ENUM("Expired", "Valid", "InUse"),
    keyval      BLOB -- Max length 1024
)
TYPE = MyIsam;

-- Create CanadaPrivateKey table
CREATE TABLE  CanadaPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create NortheastPrivateKey table
CREATE TABLE  NortheastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create MidAtlanticPrivateKey table
CREATE TABLE  MidAtlanticPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create MidwestPrivateKey table
CREATE TABLE  MidwestPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create SoutheastPrivateKey table
CREATE TABLE  SoutheastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
```

```
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create SouthwestPrivateKey table
CREATE TABLE  SouthwestPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create WestCoastPrivateKey table
CREATE TABLE  WestCoastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

-- Create WesternPrivateKey table
CREATE TABLE  WesternPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PrivateKeyModel;

--
-- Create "Model" PublicKey table
--
CREATE TABLE IF NOT EXISTS PublicKeyModel
(
    listId      INT UNSIGNED,
    keyId       INT UNSIGNED,
    status      ENUM("Expired", "Valid", "InUse"),
    exponent    TINYBLOB, -- Max length 3
    modulus     TINYBLOB  -- Max length 256
)
TYPE = MyIsam;

-- Create CanadaPublicKey table
CREATE TABLE  CanadaPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create NortheastPublicKey table
CREATE TABLE  NortheastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create MidAtlanticPublicKey table
CREATE TABLE  MidAtlanticPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
```

```
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create MidwestPublicKey table
CREATE TABLE  MidwestPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create SoutheastPublicKey table
CREATE TABLE  SoutheastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create SouthwestPublicKey table
CREATE TABLE  SouthwestPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create WestCoastPublicKey table
CREATE TABLE  WestCoastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

-- Create WesternPublicKey table
CREATE TABLE  WesternPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM PublicKeyModel;

--
-- Create one measurements table for each region
--
-- Create "Model" NpacMeasurements table
CREATE TABLE IF NOT EXISTS NpacMeasurementsModel
(
    yyyydddhh   INT UNSIGNED NOT NULL,
    Binds       INT UNSIGNED NOT NULL DEFAULT 0,
    SuccessOps  INT UNSIGNED NOT NULL DEFAULT 0,
    FailedOps   INT UNSIGNED NOT NULL DEFAULT 0,

    PRIMARY KEY (yyyydddhh)
)
TYPE = MyIsam;

-- Create CanadaNpacMeasurements table
CREATE TABLE  CanadaNpacMeasurements
```

```
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create NortheastNpacMeasurements table
CREATE TABLE  NortheastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create MidAtlanticNpacMeasurements table
CREATE TABLE  MidAtlanticNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create MidwestNpacMeasurements table
CREATE TABLE  MidwestNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create SoutheastNpacMeasurements table
CREATE TABLE  SoutheastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create SouthwestNpacMeasurements table
CREATE TABLE  SouthwestNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create WestCoastNpacMeasurements table
CREATE TABLE  WestCoastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

-- Create WesternNpacMeasurements table
CREATE TABLE  WesternNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM NpacMeasurementsModel;

--
-- Create DbConfig table
--
CREATE TABLE  DbConfig
(
    keyType     ENUM("Canada", "MidAtlantic", "Midwest", "Northeast",
                     "Southeast", "Southwest", "WestCoast", "Western",
                     "R9", "R10", "R11", "R12", "R13", "R14",
                     "R15", "R16", "R17", "R18", "R19", "R20", -- Future
```

```
Regions
                    "Internal", "Ebda", "Lsms") NOT NULL,
    keyName     TINYBLOB NOT NULL,            -- Max length 256
    description TINYBLOB NOT NULL DEFAULT "", -- Max length 256
    value           BLOB NOT NULL DEFAULT "", -- Max length 64K

    -- keyName is unique within keyType
    PRIMARY KEY (keyType, keyName(255))
)
TYPE = MyIsam;

INSERT INTO DbConfig (keyType, keyName, description, value)
    VALUES
    ("Canada",      "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Canada",      "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Canada",      "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),
    ("Canada",      "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Canada",      "NPAC_BIND_TIMEOUT",      "Bind Timeout with
NPAC", "15"),
    ("Canada",      "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("MidAtlantic", "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("MidAtlantic", "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("MidAtlantic", "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),
    ("MidAtlantic", "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("MidAtlantic", "NPAC_BIND_TIMEOUT",      "Bind Timeout with
NPAC", "15"),
    ("MidAtlantic", "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("Midwest",     "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Midwest",     "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Midwest",     "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),
    ("Midwest",     "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Midwest",     "NPAC_BIND_TIMEOUT",      "Bind Timeout with
NPAC", "15"),
    ("Midwest",     "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("Northeast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Northeast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Northeast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),
```

```
    ("Northeast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Northeast",   "NPAC_BIND_TIMEOUT",      "Bind Timeout with NPAC",
"15"),
    ("Northeast",   "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("Southeast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Southeast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Southeast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC recovery
requests",   "3"),
    ("Southeast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Southeast",   "NPAC_BIND_TIMEOUT",      "Bind Timeout with NPAC",
"15"),
    ("Southeast",   "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("Southwest",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Southwest",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Southwest",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC recovery
requests",   "3"),
    ("Southwest",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Southwest",   "NPAC_BIND_TIMEOUT",      "Bind Timeout with NPAC",
"15"),
    ("Southwest",   "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("WestCoast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("WestCoast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("WestCoast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC recovery
requests",   "3"),
    ("WestCoast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("WestCoast",   "NPAC_BIND_TIMEOUT",      "Bind Timeout with NPAC",
"15"),
    ("WestCoast",   "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
    ("Western",     "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
    ("Western",     "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),
    ("Western",     "RECOV_RETRY_NUMBER",     "Retry times for NPAC recovery
requests",   "3"),
    ("Western",     "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),
    ("Western",     "NPAC_BIND_TIMEOUT",      "Bind Timeout with NPAC",
"15"),
    ("Western",     "BIND_RETRY_INTERVAL",    "Retry seconds for Bind
requests", "120"),
```

```
    ("Internal", "MAX_SPIDS",     "Maximum Service Providers
allowed.",             "32"),
    ("Internal", "EDR",           "Enable Efficient Data
Reperesentation (EDR).",   "N" ),
    ("Internal", "SNMP",          "Enable SNMP
Agent.",                           "N" ),
    ("Internal", "AFT",           "Enable Automatic File
Transfer.",               "N" ),
    ("Internal", "WSMSC",         "Enable wireless service
feature.",              "N" ),
    ("Internal", "WSMSC_TO_EAGLE","Enable sending of WSMSA service to
Eagle.",      "N" ),
    ("Internal", "IP_GUI",        "Enable Web based ip
gui.",                       "N" ),
    ("Internal", "SPID_SECURITY", "Enable SPID based
security.",                    "N" ),
    ("Internal", "MAX_USERS",     "Maximum Number of
Users",                        "8" ),
    ("Internal", "ENHANCED_FILTERS","Enable Group and Regional filter
creation.",   "N" ),
    ("Internal", "MAX_EAGLES",    "Maximum number of
eagles.",                      "16"),
    ("Internal", "REPORT_GEN",    "Enable report
generator.",                    "N" ),
    ("Internal", "REPORT_GEN_QUERY_ACTIVE","Report generator pid
field",            "0" ),
    ("Internal", "QUERY_SERVER",  "Enable Query Server
feature",                   "N" ),
    ("Internal", "COMMAND_CLASS", "Enable Command Class Managment
feature",         "N" ),
    ("Internal", "NANC_3_2_ENHANCEMENTS",  "Enable NANC 3.2
enhancements feature",  "N" ),
    ("Internal", "NPAC_RECOVERY_PERIOD", "NPAC Download Request Time
Period",       "60" ),
    ("Internal", "LOGIN_MSG",     "Enable Customizable Login
Message",              "N" ),
    ("Internal", "INACTIVITY_TIMEOUT", "Gui and Shell inactivity
timeout feature",  "N" ),
    ("Internal", "SYSTEM_INACTIVITY_TIMEOUT", "System wide GUI and
Shell inactivity timeout value", "15" ),
    ("Internal", "LOG_EAGLE_SUCCESS_RESP", "Log time for successful
Eagle response", "N" ),
    ("Internal", "RESYNCDB_QUERY_SERVER", "Enable ResyncDB Query
Server feature",    "N" ),
    ("Internal", "HSOP_BUNDLING", " Enable HSOP bundling
feature",                  "Y" ),
    ("Internal", "NPAC_HEARTBEAT_TIMEOUT", "Timeout seconds for NPAC
heartbeat","60" ),
    ("Internal", "NPAC_HEARTBEAT_RETRY_NUMBER", "Retry times for NPAC
heartbeat","3" ),
    ("Internal", "NPAC_HEARTBEAT_QUIET_PERIOD_TIMEOUT", "Timeout
seconds for NPAC heartbeat quiet period","900" ),
    ("Internal", "NPAC_HEARTBEAT_QUIET_PERIOD_TIMEOUT_CANADA",
"Timeout seconds for NPAC heartbeat quiet period (Canada)","100000" ),
    ("Internal", "DEFAULT_PASSWORD_TIMEOUT", "System wide GUI and
```

```
Shell password timeout", "0" ),
    ("Internal", "NANC_3_3_FEATURE_SET", " Enable the support of NANC 3.3
Feature Set","N" ),
    ("Internal", "SERVICE_PROV_TYPE", " Enable the support of Service
Provider Type","N" ),
    ("Internal", "SWIM_RECOVERY", " Enable the support of SWIM Recovery
Feature","N" ),
    ("Internal", "CANADA_SPID_RECOVERY", " Enable the support of Canada SPID
Recovery","N" ),
    ("Internal", "ERROR_CODES_FOR_ACTIONS", " Enable the support of Action
Error Codes","N" ),
    ("Internal", "ERROR_CODES_FOR_NON_ACTIONS", " Enable the support of Non-
Action Error Codes","N" ),
    ("Internal", "SV_TYPE", " Enable SV Type feature","N" ),
    ("Internal", "ALT_SPID", " Enable Alternative SPID feature","N" ),
    ("Internal", "SURV_OK_TRAP", "Send SNMP trap every 5 minutes that
Surveillance is running","N" ), ("Internal", "SERVDI_ENABLED", "Enable
SERVDI feature","N" ), ("Internal", "ALARM_FILTERING", " Enable LSMS Alarm
Filtering Feature","N" ), ("Internal", "MYSQL_PORT", " Enable LSMS
Configurable MySQL Port Feature","N" ), ("Lsms", "LNP_QTY_THRESHOLD",
"Configurable percent","80" ), ("Internal", "BINLOGS_THRESHOLD", "Threshold
for forceful purging","98" ),
    ("Ebda", "CMD_ARGS", "EBDA command line arguments", ""),

    ("Lsms", "NPAC_SPID", "Spid used to connect to NPAC", ""),
    ("Lsms", "CONTACT_INFO", "Spid used to connect to NPAC", '"Lsms
Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1234"
,"9195551234"'),
    ("Lsms", "COMPONENT_INFO", "Spid used to connect to NPAC",
'"LSMS","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"');

--
-- Create NpaSplit table
--
CREATE TABLE  NpaSplit
(
    -- The old npa
    oldNpa         char(3)    NOT NULL,

    -- The new npa
    newNpa         CHAR(3)    NOT NULL,

    -- The nxx
    nxx            CHAR(3)    NOT NULL,

    -- The start of the permissive dialing period
    startPDP       CHAR(8)    NOT NULL,

    -- The end of the permissive dialing period
    endPDP         CHAR(8)    NOT NULL,

    -- The region the split belongs to
    region      ENUM("Canada", "MidAtlantic", "Midwest", "Northeast",
                     "Southeast", "Southwest", "WestCoast", "Western",
```

```
                    "R9", "R10", "R11", "R12", "R13", "R14",
                    "R15", "R16", "R17", "R18", "R19", "R20"), --
Future Regions

    -- The status of the npa split
    status      ENUM("NotSet", "Pending", "Active", "Error"),

    -- Old npa, new npa and nxx form primary unique key
    PRIMARY KEY (oldnpa, newnpa, nxx)
)
TYPE = MyIsam;

--
-- Create Authorization table
--
CREATE TABLE Authorization
(
    -- The group (Primary Key)
    groupName  CHAR(64) NOT NULL,

    -- The function (Primary Key)
    function   CHAR(64) NOT NULL,

    -- Whether this function may be performed by members of this group.
    authorized  BOOL     NOT NULL DEFAULT 0,

    -- Force the group plus the name to be unique
    PRIMARY KEY (groupName, function)
)
TYPE = MyIsam;

--
-- Create default non-configurable user authorizations
--
-- Insert lsmsadm default data for table `Authorization`
```

Query Server Maintenance

Following is a list of ways to monitor and determine the status of the query server:

- The **LSMS** monitors the connectivity with each directly-connected query server. **GUI** messages, surveillance messages, and **SNMP** traps are generated at the **LSMS** for failure and recovery of the connection to the query server.
- The **LSMS** enables customers to check the connection status of directly-connected query servers.
- Instructions are provided to enable customers to determine the status of the replication of **LNP** data at the query server (refer to “Check MySQL Replication Status on Query Servers” in the *Alarms and Maintenance Guide*).

Additionally, detailed instructions and procedures are provided to enable customers to perform initialization and recovery procedures in the event of a failure.

For more information, refer to *Alarms and Maintenance Guide*.

Query Server Requirements

The platform that is used to host a query server must meet the minimum requirements shown in the following tables in order to meet performance requirements.

Table A-3 Query Server Platform Requirements for Solaris 10

Component	Minimum Requirement
Operating System	N/A
Processor	333 Mhz
Memory	256 Megabytes
Minimum Disk Space (in partition containing `/usr/mysql1`) See Note 1.	10 **GB** (for up to 48 million **TNs**) 20 **GB** (for up to 96 million **TNs**) 25 **GB** (for up to 120 million **TNs**) 40 **GB** (for up to 192 million **TNs**) 48 **GB** (for up to 228 million **TNs**) 80 **GB** (for up to 384 million **TNs**) 95 **GBs** (for up to 504 million TNs) 480 **GBs** E5-APPB-02 cards (for up to 756 million TNs)

Note:

- The partitioning and setting up of the `/usr/mysql1` file system with the minimum required disk space are the responsibility of the customer.
- The /opt/ file system on the Query Server must contain enough free space to store the MySQL binary executables (325 MB for MySQL 5.6).
- The executable gzip version 1.2.24 cannot decompress files larger than 2 **GB**. **NPAC** regions with databases greater than 59 million records require a version of gzip capable of supporting compressed files larger than 2 **GB**. For this reason, Oracle Communications recommends using gzip version 1.3 or greater.

Table A-4 Query Server Platform Requirements for Linux

Component	Minimum Requirement
Operating System	Oracle Linux Server
Release	7.2
Architecture	X86_64
Processor	Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz
Memory	4 Gigabytes
Minimum Disk Space	250 Gigabytes

Interface Support

The Query Server supports automated database access using standard interfaces described in this section.

MySQL provides support for various Application Programming Interfaces (**API**s) that can be used to create clients to directly query objects and attributes in the **LSMS LNP** database replica on the query server.

> **Note:**
>
> Because customers have the flexibility to customize **SQL** queries in order to create new queries, Oracle Communications does not provide “canned queries” with this platform.

ANSI SQL Standard Support

MySQL provides support for the **ANSI** (**American National Standards Institute**) **SQL** Standard (Entry-level **SQL92**). The MySQL server includes a command-line option for turning on **ANSI** mode. This mode changes some of MySQL's behavior to better accept **SQL** statements that are valid according to the **SQL**-92 standard.

For more information, refer to the section “Running MySQL in **ANSI** Mode” in the *MySQL Reference Manual*, available at www.mysql.com.

ODBC Support

MySQL provides support for **ODBC** (Open Data Base Connectivity) by means of the MyODBC program. MyODBC is a 32-bit **ODBC** (2.50) level 0 (with level 1 and level 2 features) driver for connecting an **ODBC**-aware application (such as Microsoft Access, Microsoft Excel, and Crystal Reports) to MySQL.

For more information about how to install and use MyODBC, refer to the section “MySQL **ODBC** Support” in the *MySQL Reference Manual*, available at www.mysql.com.

JDBC Support

MySQL supports the following **JDBC** (Java Data Base Connectivity) driver:

- The MySQL Connector/J driver. You can find a copy of the MySQL Connector/J driver at http://dev.mysql.com/downloads/connector/j/5.6.html

For more information, consult any **JDBC** documentation and the driver's own documentation for MySQL-specific features.

C, C++, Eiffel, Java, Perl, PHP, Python, and Tcl Support

MySQL provides **APIs** for C, C++, Eiffel, Java, Perl, **PHP**, Python, and Tcl. Reference “MySQL **APIs**” section in [3] for all the **APIs** available for MySQL, where to get and how to use them.

For more information about where to get one of these **API**s and how to use it, refer to the section “MySQL **APIs**” in the *MySQL Reference* manual, available at www.mysql.com.

LSMS Query Server Configuration Scenario

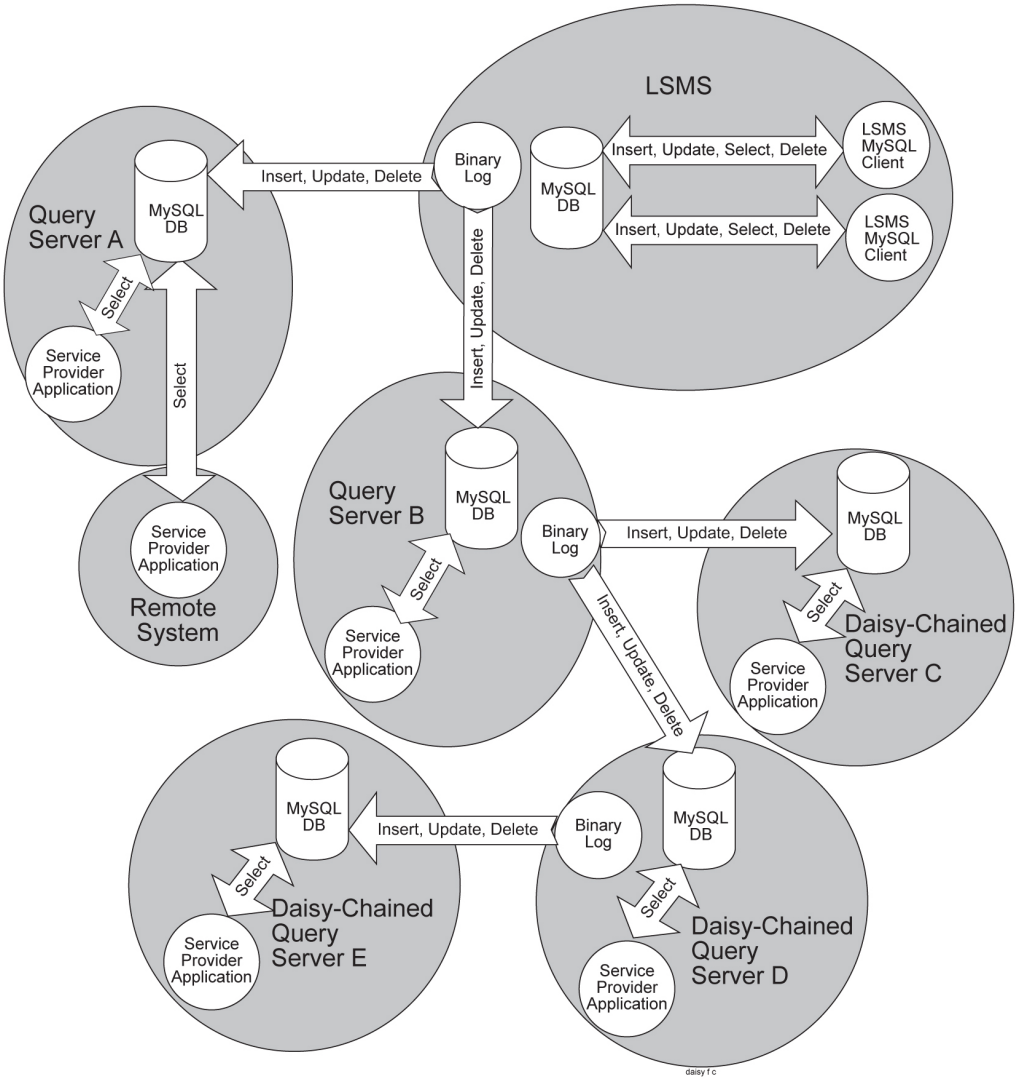
Figure A-2 illustrates a query server configuration scenario depicting how the **LSMS** might be directly-connected to a query server, or indirectly-connected to daisy-chained query servers. This scenario includes the following:

- One master (**LSMS**)
- One remote system
- Five query servers:
  - One directly-connected slave (Query Server A)
  - One directly-connected master/slave (Query Server B)
  - Two daisy-chained slaves (Daisy-chained Query Servers C and E)
  - One daisy-chained master/slave (Daisy-chained Query Server D)

Client applications on each query server represent a non-Oracle Communications provided Service Provider application that queries the replicated **LSMS LNP** databases using supported MySQL database **API**s.

> **Note:**
>
> Process all updates to the query server database through the master.

Figure A-2 LSMS Query Server Configuration Scenario



Query Server Installation and Configuration

Before you use the query server feature, you must perform the following procedures:

1. MySQL Replication Configuration for LSMS
2. MySQL Installation/Upgrade for Query Server Platform
3. MySQL Replication Configuration for Daisy-Chained LSMS Query Servers

MySQL Replication Configuration for LSMS

Use the following procedure to configure the **LSMS** to support one or more directly-connected query servers.

> **Note:**
>
> Perform all the steps in the following procedure the first time you configure the **LSMS** system and Linux platform to support the Query Server Package, or to verify that you previously performed all configuration correctly.

> **Caution:**
>
> The following procedure may briefly interrupt traffic being sent to **EAGLE** from the **NPAC** and from local **LSMS** provisioning. The time required to accomplish this procedure depends on the bandwidth of the customer's network and the amount of data to be reloaded. It is recommended that this procedure be performed during a scheduled maintenance window.

1. Activate the **LSMS** Query Server Package:

   The Query Server Package is an optional feature that must be activated at the **LSMS**. To activate the Query Server Package, contact the Customer Care Center.
2. Log into the active server as `root`, and continue with the following steps.
3. Associate the names of the query server hosts with their **Internet Protocol** (**IP**) addresses:

   To do this, add an **IP** address and hostname pair for each query server to the `/etc/hosts` file on both the primary and secondary **LSMS** servers. The hostname of the query server will be used to identify each query server when reporting on its status.
4. Setup a special replication user (for each query server) on the **LSMS** with privileges and permissions that a query server can use to access the **LSMS** to perform database replication:

   ```
   # lsmsdb -c addrepluser -h <hostname> -p <password>
   ```

   > **Note:**
   >
   > The combination of username and password is unique to replication use and provides read access only to the binary log on the **LSMS** system. Additionally, access to this user account is restricted to the hostname specified.
5. Remove all (if any) existing snapshots to ensure that a sufficient amount of disk space is available for creating new snapshots of the **LSMS** data.

   If an alternative location is specified to store the snapshot files, remove all snapshot files from that directory (instead of the default, /`var/TKLC/lsms/free`):

   ```
   # rm /var/TKLC/lsms/free/mysql-snapshot*
   ```

   ```
   # rm /var/TKLC/lsms/free/snapinfo.sql
   ```
6. Create a compressed snapshot of all the **LSMS** data.

> **Caution:**
>
> Do not create a snapshot while a database backup is occurring. To ensure that a database backup is not occurring, perform the procedure described in “Check for Running Backups” in Appendix E of the *Alarms and Maintenance Guide*.

> **Note:**
>
> GNU tar (gtar) must be installed on the Query Server prior to any single region exceeding 60 million TNs.

```
lsmsdb -c snapshot
```

During the creation of the **LSMS** data, the following occurs:

- A read lock is obtained
- Table information is flushed
- A snapshot is created
- The read lock is released

If you successfully create the snapshot, the **LSMS** data is captured and stored in the following files in `/var/TKLC/lsms/free`:

- `mysql-snapshot-supDB.tar.gz`
- `mysql-snapshot-<regionalDB>.tar.gz`(one file for each region present)
- `snapinfo.sql`

You have now completed this procedure.

MySQL Installation/Upgrade for Query Server Platform

For details related to MySQL installation and upgrade for query server platform, refer to *LSMS Query Server on Linux Installation and Upgrade Guide*.

MySQL Replication Configuration for Daisy-Chained LSMS Query Servers

Use this procedure to configure each query server platform that will have one or more directly-connected daisy-chained query servers. (Perform this procedure on Query Servers B and D, as shown in Figure A-2).

1. Start the MySQL command-line utility on the query server that is directly-connected to the **LSMS**:

```
# cd /usr/mysql1/bin
# mysql -u root -p

Enter password:

<Query Server’s MySql root user password>
```

2. Set up a special replication user on the slave query server with the **FILE** privilege and permission that all slaves can use to access the query server from any host:

   ```
   mysql> GRANT REPLICATION SLAVE, FILE ON *.* TO '<username>'@"%"
   IDENTIFIED BY '<password>';
   ```
   where `<username>` and `<password>` are the replication user's name and password (optional).

   Confirm the slave settings are correct:

   ```
   mysql> show GRANTS for 'username' ;
   ```

3. Stop MySQL replication:

   (When replication is off, the slave server data is not updated and is not kept in synchronization with the master server).
   ```
   mysql> STOP SLAVE;
   ```

4. Obtain a read lock and flush table cache information:

   The flush writes changes to indexes to the table. The read lock does not allow changes to be made to tables but continues to allow other threads to read from them.
   ```
   mysql> FLUSH TABLES WITH READ LOCK;
   ```

5. Exit the MySQL command-line utility:

   ```
   mysql> exit
   ```

6. Shutdown the MySQL server:

   ```
   #./mysqladmin -u root -p shutdown
   Enter password: <Query Server's MySql root user password>
   ```

7. Create a snapshot of all the **LSMS** data.

   Remove all existing compressed snapshot files (if any):
   ```
   rm /usr/mysql1/mysql-snapshot*
   ```

   Create a compressed snapshot file for the **LSMS** Supplemental database:
   ```
   # tar -cvf - /usr/mysql1/supDB/* | gzip >

   /usr/mysql1/mysql-snapshot-supDB.tar.gz
   ```

   Create compressed snapshot files for each of the **LSMS** regional databases. Replace <regionDB> with the regional database name (for example, CanadaDB, MidwestDB, and so forth).

   > **Note:**
   >
   > GNU tar (gtar) must be installed on the Query Server prior to any single region exceeding 60 million TNs.

   ```
   # tar -cvf - /usr/mysql1/<regionDB>/* | gzip >

   /usr/mysql1/mysql-snapshot-<regionDB>.tar.gz
   ```

8. Add the `log-bin`, `log-slave-updates`, and `binlog-format=ROW` options to the `[mysqld]` section of the `my.cnf` option file on the query servers if you plan to daisy-chain one or more query servers from the directly-connected query server.

   This option tells the query server to log the updates from the slave thread to the binary log that daisy-chained query servers use to synchronize their data.

```
log-bin=mysql-bin

log-slave-updates

binlog-format=ROW
```

9. Restart the MySQL **daemon** on the query server that is directly-connected to the **LSMS**:

```
# cd /usr/mysql1/bin
# ./mysqld_safe &
```

You have now completed this procedure.