LRS Reference Manual

For Lantronix Remote Access Servers

Contents

3 Basic Remote Networking

4 Additional Remote Networking

5 IP

6 IPX

8 PPP

9 Ports

10 Modems

11 Modem Sharing

12 Security

13 Command Reference

NOTE:*For the full command list, see the Command Reference Contents.*

1 Introduction

1 - Introduction

1.1 About the LRS

The Lantronix Remote Access Server (LRS) supports several ways to network remote users and remote locations. Using ordinary telephone lines, the LRS allows remote computers and remote networks to easily access a local Ethernet network. The LRS can be configured to initiate and drop connections to remote locations under certain conditions. For example, the LRS can automatically connect to a remote LRS, thereby joining two LANs.

In addition to remote networking capabilities, the LRS includes traditional terminal server functionality such as security features and modem control. The security features include dialback, passwords, database authentication, and menu mode. The LRS also allows automatic modem configuration and control.

1.1.1 Protocol Support

The LRS supports three industry-standard network protocols: IP, IPX, and AppleTalk.

1.1.1.1 IP

The LRS supports Telnet, Rlogin, and Domain Name Servers (DNS). The **Telnet** terminal protocol is supported on most UNIX systems. It is an easy to use interface that creates terminal connections to any networked host supporting Telnet. **Rlogin** enables you to initiate a TCP/IP login session. **DNS** enables a network name server to translate text node names into numeric IP addresses. The LRS also supports syslog functionality.

Windows 95 users can run NetBIOS over IP and use the DNS for name resolution, or a primary or secondary NetBIOS nameserver (NBNS). See the IP chapter for more information.

The LRS supports static and dynamic routing. Static routes can be entered when routing is needed but a dynamic route is not desirable. Dynamic routing information is obtained and transmitted through the receipt and generation of RIP (Routing Information Protocol) packets. The LRS also allows dymanic allocation of IP addresses.

1.1.1.2 IPX

The LRS supports the following frame types: **ETHERNET_II**, **SNAP**, **802.2**, and **802.3.** SPX connections are supported via EZCon, the point-and-click configuration software shipped with the unit. The LRS also supports NCP over IPX for NetWare printing and NetWare logging.

The LRS supports IPX RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) routing updates. The LRS also supports keepalive spoofing, which allows a connection between a workstation and file server (or between two LRS units) to remain idle when there is no interactive packet traffic.

1.1.1.3 AppleTalk

The LRS supports AppleTalk Phase 1 and AppleTalk Phase 2 networking. The LRS can function as an endnode for remote node connections, or as a router for LAN to LAN connections. The LRS can also be configured as a seed router for the AppleTalk network segment to which it is attached.

1.1.2 Link Layer Support

Two serial link-layer protocols are supported: PPP and SLIP.

1.1.2.1 PPP

The LRS supports the transfer of IP, IPX, and AppleTalk over PPP. Two PPP authentication protocols are supported: PAP and CHAP.

1.1.2.2 SLIP

The LRS supports SLIP and CSLIP (Compressed SLIP).

1.1.3 Remote Networking Support

The LRS supports the following remote networking features:

Remote node logins	A single remote node (such as a laptop) may log into the LRS, form a connection, and use a network's services as if it were directly connected to that network.
Incoming and outgoing LAN to LAN connections	The LRS can be used to connect two networks that don't always need to be connected; for example, a small remote office LAN and a central office LAN.
Packet filtering	Packet traffic can be restricted in a number of ways using packet filters. Filters may be used to restrict outgoing traffic, restrict incoming traffic, determine connection time-outs, or determine whether or not an outgoing connection should be initiated.
Chat scripts	The LRS supports the use of chat scripts to communicate with equipment at a remote location.
Bandwidth on demand (Multilink PPP)	The LRS may be configured to analyze current bandwidth utilization and add or subtract bandwidth when necessary.
Connection restrictions	Connections may be restricted to particular time periods and days of the week.
IP and IPX header compression	The LRS may be configured to compress IP / IPX packet headers, reducing the delay and bandwidth requirements.
IPX keepalive spoofing	The LRS may send keepalive packets to and from a Novell workstation and Novell fileserver, permitting a connection to remain idle until useful traffic is received.
Authentication	The LRS may be configured to require a dial-in user to authenticate itself. In addition, the LRS may authenticate itself to remote hosts when required.

1.1.4 Security Support

The LRS enables you to secure your network in a number of ways. Supported features include:

- Authentication of incoming connections in a variety of ways, including Kerberos, SecurID, RADIUS, and CHAP / PAP.
- Authentication of outgoing LAN to LAN connections
- Dialback during incoming connection attempts
- Restriction of user access to commands and functions
- Event logging

For more information on any of these features, see Chapter 12, *Security*.

1.2 Getting Started

To get started using the LRS, complete the following steps:

1. Install the unit. Refer to the included **Installation Guide** for instructions.
2. Give the LRS a network address. IP users must configure an IP address for their units (see the **Installation Guide**). LRS units on Novell networks will automatically learn an address.
3. Install EZCon, which is shipped with the LRS on CD-ROM and available via Lantronix's FTP server in the **/pub/ezcon** directory. EZCon is an easy-to-use, point-and-click configuration utility that will enable you to set up your LRS over the network.

NOTE: *To use the CD-ROM and navigate through its directories, see the instructions on the CD-ROM case.*

Macintosh users:

Mac TCP is required. Insert the distribution CD-ROM, locate the EZCon Installer for Macintosh, and double-click on the Installer icon.

Novell users:

Windows and the NetWare VLM client software are required.

UNIX users:

Instructions for running the EZCon install script are located in the README file located on the CD-ROM and on the Lantronix FTP server.

4. Run EZCon to configure your unit. Select the **Initial Setup** option that best suits your application. If additional configuration is required, complete your installation using the Maintenance option.

NOTE: *Macintosh users should select TCP/IP under the File:Protocol menu.*

If you choose to configure the LRS without EZCon, you'll need to determine the appropriate setup and enter a series of configuration commands. This manual covers all information necessary to configure your unit in this manner; see *Using This Manual* on page 1-4.

1.3 Using This Manual

While this reference manual primarily explains LRS setup from the command line interface, EZCon users should read the manual for conceptual information and cautionary material. The chapters should be read in the following order:

1. Read through the material and complete the steps in Chapter 2, *Getting Started*.

NOTE: *If at any point you need to look up a specific command, see Chapter 13, Command Reference. This chapter details the entire LRS command set.*

2. Set up LAN to LAN and Remote Node remote networking using Chapter 3, *Basic Remote Networking*.
3. To optimize remote networking, read through the conceptual information and complete the configuration instructions in Chapter 4, *Additional Remote Networking*.
4. Set up IP, IPX, and / or AppleTalk using the instructions in Chapter 5, *IP*, Chapter 6, *IPX*, and Chapter 7, *AppleTalk*.
5. For conceptual information about PPP, read Chapter 8, *PPP*.
6. Configure the LRS serial ports using Chapter 9, *Ports*.
7. If modems will be attached to the LRS, configure the modems using Chapter 10, *Modems*.
8. If modems attached to the LRS serial ports will be shared, see Chapter 11, *Modem Sharing*.
9. If security is required, complete the instructions in Chapter 12, *Security*. This chapter covers authentication, access restrictions, and logging.
10. For supplemental material, refer to the Appendices.

2 Getting Started

2 - Getting Started

2.1 Introduction

This chapter covers some background information to get you started using the LRS. Topics include methods for setting up the LRS, and ongoing maintenance issues such as restoring factory default settings.

This chapter assumes the following:

- The LRS is running operational code (in other words, the unit has successfully booted)
- The LRS is connected to an Ethernet
- If IP is being used, the LRS has been assigned an IP address

NOTE: *For details on booting, installation, or IP address assignment, refer to your Installation Guide.*

2.2 Methods of Configuration

The LRS may be configured using the EZCon configuration software or commands issued at the command line (Local>) prompt.

To configure the LRS when a problem has occurred (for example, the unit doesn't boot successfully and a Boot> prompt appears on the console port), refer to the Troubleshooting appendix of your Installation Guide.

2.2.1 EZCon

The EZCon software is the easiest way to configure the unit. EZCon guides you through configuration using a graphical interface.

TCP/IP, AppleTalk, and NetWare versions of EZCon are shipped with the LRS on a CD-ROM. To use the CD-ROM, refer to the instructions on the CD-ROM case. To install EZCon, refer to the appropriate EZCon README file.

All instructions for using EZCon are listed in each README file. For assistance once EZCon is running, refer to the EZCon online help.

2.2.2 Command Line Interface

To configure the LRS without EZCon, configuration commands must be entered at a command line. These commands are entered when a port is in **character mode**; in this mode, the Local> prompt will be displayed.

There are four ways to display the Local> prompt:

- Connect a terminal to the serial console port and press the Return key until the prompt is displayed.
- Establish a Telnet or Rlogin connection to the LRS from a TCP / IP host.
- In EZCon, click the Terminal icon. The Local> prompt will be displayed in a terminal emulation window.
- Establish a TCP / IP remote console connection. For a complete description, see Chapter 5, *IP*.

NOTE: *IPX users can use EZCon to log into the remote console port.*

NOTE: *The default serial port parameters are 9600 baud, 8 data bits, 1 stop bit, no parity, and XON/XOFF flow control.*

2.2.2.1 Entering and Editing Commands

In examples throughout the manual, LRS commands and keywords are displayed in upper case for clarity. They may be entered in upper, lower, or mixed case.

The Command Reference (Chapter 12) displays the syntax of each command, including any restrictions, known errors, and references to related commands. Optional parameters are enclosed in brackets **[ ]**. Required parameters are enclosed in curly braces **{ }**; one and only one of these parameters must be used. User-supplied parameters, such as a particular port ***number*** or host ***name***, are shown in italics.

When entering a string, such as a username or filename, it is important to remember to enclose the string in quotes; this will retain the case entered. If a string is not enclosed in quotes, it will be automatically changed to all uppercase characters.

NOTE: *The privileged and login passwords are case-independent, even when enclosed in quotes.*

The LRS **command completion** feature will complete partially-typed commands for you. This can save time and reduce errors if you're entering a number of commands. To use command completion, type part of a command, then press the space bar; the LRS will automatically "type" the remainder of the command.

NOTE: *Command completion is disabled by default. To enable command completion, refer to Set/Define Ports Command Completion on page 13-109.*

All keys used for entering and editing commands are listed in Table 2-1 on page 2-3.

Table 2-1: Command Editing Keys

Key	Purpose
Return	Executes the current command line
Delete	Deletes the character before the cursor
Ctrl-A	Toggles insert mode (insert or overstrike). Overstrike is on by default.
Ctrl-D	Logs out of the server
Ctrl-E	Moves the cursor to the end of the line
Ctrl-H or Backspace	Moves the cursor to the beginning of the line
Ctrl-R	Redisplays the current command
Ctrl-U	Deletes the entire current line
Ctrl-Z	Logs out of the server
Left Arrow	Moves the cursor left
Right Arrow	Moves the cursor right
Up Arrow or Ctrl-P	Recalls the previous command
Down Arrow or Ctrl-N	Recalls the next command
!*text*	Recalls the last command starting with *text*
!!	Recalls the last command

NOTE: *Line editing is disabled on hardcopy (printer) ports.*

2.2.2.2 Command Types

The following commands appear frequently throughout this manual. There are subtle differences between each group of commands, explained below:

2.2.2.2.1 Set and Define

Set Makes an immediate (but not permanent) change; the change will be lost when the LRS is rebooted. To make the change permanent, you must also enter the Save command.

Define Makes a permanent change, but the change doesn't take effect until the LRS is rebooted.

NOTE:*Define Ports* *will take effect as soon as the port is logged out, and* ***Define Site*** *will take effect when a site starts.*

2.2.2.2.2 Show, Monitor, and List

Show Displays the current settings. Current settings include those made using the Set command but not saved as permanent changes.

Monitor Displays the current settings; information is updated every three seconds.

List Displays permanent settings.

2.2.2.2.3 Clear and Purge

Clear Removes a configured setting immediately, but does not make a permanent change.

Purge Removes a configured setting permanently, but does not take effect until the unit is rebooted.

NOTE: ***Purge Port*** *will take effect as soon as the port is logged out, and* ***Purge Site*** *will take effect when a site starts.*

2.2.2.3 Restricted Commands

Some commands require privileged (superuser) status. To obtain privileged status, you must enter the privileged password. See *Privileged Password* on page 2-8 for instructions.

The LRS prompt will change to reflect privileged user status if configured to do so. See *Changing the LRS Prompt* on page 2-4 and *Set/Define Server Prompt* on page 13-133 for more information.

2.3 Maintenance Issues

The following sections detail configuration that is required periodically or on an ongoing basis.

2.3.1 Changing the LRS Server Name

The LRS is initially configured with a server name. However, you can give the server a custom name of up to 16 alphanumeric characters using the following command:

Figure 2-1: Changing the Server Name

```
Local>> DEFINE SERVER NAME “CommServer”
```

NOTE: *The server name must be enclosed in quotes to preserve case.*

2.3.2 Changing the LRS Prompt

The prompt each user receives (usually the Local_x> prompt, where x is the port number) is configurable in a variety of ways. For a basic prompt, enter a string similar to the following:

Figure 2-2: Configuring the Server Prompt

```
Local> SET SERVER PROMPT “Server> ”
Server>
```

For a customized prompt, optional key combinations can be added to the prompt string. See **Set/Define Server Prompt** on page 13-133 for more information. Placing a space after the end of the prompt is recommended to improve readability.

NOTE: *The remote console port prompt cannot be changed.*

Figure 2-3 displays a few examples of commands used to change prompts. In the examples, the first command line results in the prompt used in the second command line, and so on.

Figure 2-3: Prompt Examples

```
Local> SET SERVER PROMPT “Port %n: “
Port 5: SET SERVER PROMPT “%D:%s! “
LRS:LabServ! SET SERVER PROMPT “%p%S_%n%P%% “
Port_5[NoSession]_5>%
```

2.3.3 Setting the Date and Time

The LRS can calculate and save the local time, coordinated Universal Time (UTC, also known as Greenwich Mean Time, or GMT), standard and Daylight Savings timezones, and the corresponding number of hours difference between UTC and the set timezone.

2.3.3.1 Setting the Clock

Use EZCon’s **Maintenance** feature to set the local date and time, or use the **Set/Define Server Clock** command at the Local> prompt. Time should be entered in hh:mm:ss “military format” as shown in the example below.

Figure 2-4: Setting the Clock

```
Local>> SET SERVER CLOCK 14:15:00 12/31/1995
```

2.3.3.2 Setting the Timezone

The LRS is configured to recognize a number of timezones. To display these timezones, use the **Show Timezone** command at the Local> prompt. Set the timezone by using EZCon’s **Maintenance** feature, or by using the **Set/Define Server Timezone** command at the Local> prompt:

Figure 2-5: Setting the Timezone

```
Local>> DEFINE SERVER TIMEZONE US/PACIFIC
```

If your timezone is not displayed, you will need to set it manually. Use the following information to set the timezone:

- A 3-letter timezone abbreviation; for example, PST
- The number of hours offset from UTC (Greenwich Mean Time); for example, -9:00
- The time, day, and amount of any time changes (for example, daylight savings time information)

NOTE: *Specifying time change information is optional.*

To manually set the timezone using EZCon, use the **Maintenance** option. To set the timezone using commands at the Local> prompt, refer to the following example:

Figure 2-6: Manual Timezone Configuration

```
Local>> DEFINE SERVER TIMEZONE EST -3:00 EST 1 Mar Sun>=1 3:00 Oct lastSun 2:00
```

In Figure 2-6, the first **EST** specifies that Eastern Standard Time will be used as the reference point. The second value, **-3:00**, indicates that this timezone is 3 hours behind Eastern Standard Time.

The third and fourth values, **EST** and **1**, specify that when a time change occurs the time will move forward one hour. The time change will occur in March, denoted by **Mar**. The date that the time change will occur will be the Sunday (**Sun**) greater than or equal to 1 (**>=1**), in other words, the first Sunday in the month. The **3:00** specifies that the time change will occur at 3 o'clock.

The final 3 values of the command string represent the day and time when the time will revert to the original time, in other words, when the time change will be reversed. The **Oct** and **lastSun** indicate that the time will revert on the last Sunday in October. The time change will occur at **2:00**.

2.3.3.3 Configuring a Timeserver

The LRS regularly verifies and updates its time setting with the designated timeserver. A timeserver is a host which provides time of day information for nodes on a network.

To specify a timeserver or backup timeserver, use either the **Set/Define IP Timeserver** command or the **Set/Define IPX Timeserver** command.

Figure 2-7: Defining Timeservers

```
Local>> DEFINE IP TIMESERVER 193.0.1.50
Local>> DEFINE IP SECONDARY TIMESERVER 193.0.1.51
```

2.3.4 Rebooting the LRS

There are two ways to reboot the LRS:

- At the Local> prompt, issue the **Initialize Server** command, discussed on page 13-50.
- Using EZCon, click Reset. You will be prompted with a dialog asking you to confirm the reboot.

Before rebooting the LRS, log out any current user sessions (if possible). Disconnecting sessions may prevent connection problems after the LRS is rebooted. It is courteous to warn users that the LRS will be "going down"; this can be done using the Broadcast feature.

2.3.5 Broadcast

Broadcast messages are sent to local users, but not remote networking users. Broadcasts can be sent with the following command.

Figure 2-8: Broadcast Command

```
Local>> BROADCAST ALL “Server shutdown in 5 minutes.”
```

NOTE: *The complete syntax of Broadcast is listed on page 13-3.*

When the LRS is rebooted, any changes made using Set commands will be lost. To ensure that the changes will be saved, use Define commands, or use the Save command after the Set command.

2.3.6 Restoring Factory Defaults

Restoring factory default settings will erase all changes made since the LRS was shipped; the unit will function as if it just came out of the box. To restore factory defaults, use the **Initialize Server Factory** command at the Local> prompt.

NOTE: *The Initialize Server command is discussed on page 13-50.*

To perform a TFTP boot, the LRS IP and loadhost information will have to be re-entered. (If a BOOTP server will provide this information, this is not required.) Refer to your **Installation Guide** for instructions.

2.3.7 Reloading Operational Software

The LRS stores its software in Flash ROM. The software controls the initialization process, the operation of the LRS, and the processing of commands. The contents of Flash ROM can be updated by downloading a new version of the operational software.

For instructions on reloading Flash ROM, refer to your **Installation Guide**.

2.3.8 Editing Boot Parameters

If the information that the LRS uses at boot time changes, you will need to edit the LRS **boot parameters**. Boot parameters include the following:

- Loadhost (TCP / IP or NetWare)

  The **loadhost** is the host from which the LRS operational software is downloaded at boot time.

- Backup loadhost (optional)

  Software is downloaded from a backup loadhost when the primary loadhost is unavailable.

- Software filename
- RARP (may be enabled or disabled)
- BOOTP (may be enabled or disabled)

Boot parameters are edited using **Set/Define Server** commands, for example, Set / Define Server Loadhost.

Figure 2-9: Editing the Loadhost Address

```
Local>> DEFINE SERVER LOADHOST 192.0.1.8
```

NOTE: *Set/Define Server commands are listed beginning on page 13-125.*

2.3.9 System Passwords

There are two important passwords on the LRS: the privileged password and the login password. Both are discussed in the following sections.

2.3.9.1 Privileged Password

Changing any server, site, or port setting requires privileged user status. When using EZCon, you will be prompted for the privileged password when it is needed. If you are not using EZCon, you will need to use the **Set Privileged** command at the Local> prompt to become the privileged user. The default privileged password on the LRS is **system**.

Figure 2-10: Set Privileged Command

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>>
```

NOTE: *The complete command syntax for Set Privileged is available on page 13-124.*

If another user is currently logged into the LRS as the privileged user, use the **Set Privileged Override** command to forcibly become the privileged user.

To change the privileged password, the **Set/Define Server Privileged Password** command is required. Figure 2-11 displays an example of this command.

Figure 2-11: Changing Privileged Password

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> SET SERVER PRIVILEGED PASSWORD hippo
Local>> DEFINE SERVER PRIVILEGED PASSWORD hippo
```

NOTE: *The privileged password is case-insensitive, so it does not need to be enclosed in quotes.*

NOTE: *Set/Define Server Privileged Password is discussed in detail on page 13-132.*

2.3.9.2 Login Password

Each port can be configured to require a login password when in character mode. Users will be prompted for this password when attempting to log into the port; the Local> prompt will not be displayed until the correct password is entered. The default login password is **access**.

NOTE: *When a port is in character mode, PPP and SLIP are not running. See Port Modes on page 9-3 for a complete description.*

To change the login password, use the **Set/Define Server Login Password** command:

Figure 2-12: Defining Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
```

NOTE: *The login password is case-insensitive, so it does not need to be enclosed in quotes.*

The LRS uses the login password to log into NetWare file servers. If the login password is changed, NetWare print queue setups must also be changed to reflect the new password.

To enable the use of the login password on the appropriate port(s), use the following command:

Figure 2-13: Enabling Login Password

```
Local>> DEFINE PORT 3 PASSWORD ENABLED
```

NOTE: *To enable the password on virtual ports, use the Set/Define Server Incoming command instead.*

2.3.10 Configuration Files

A configuration file is a series of LRS commands used to automatically configure the server. A configuration file may be used by the system administrator when necessary or downloaded automatically each time the server boots.

Using a configuration file can reduce the time required to configure the LRS. Options that would need to be manually set using EZCon or using commands at the Local> prompt can be automatically executed.

2.3.10.1 Using EZCon

EZCon will examine the current configuration of your LRS, translate this information into a series of commands, and save the commands in a file. This file may then be downloaded to configure the server. Refer to EZCon's online help for more information.

2.3.10.2 Without EZCon

To create a configuration file without EZCon, each LRS command will need to be manually entered in the file. Complete the instructions in the following sections.

2.3.10.2.1 Creating the File

On your host, enter a series of LRS commands, one command per line. Privileged commands may be included; when the file is downloaded, the commands will be executed as if a privileged user was logged into the LRS.

Capitalization of commands is optional. If a string (such as a password) is entered, it must be enclosed in quotes in order to preserve the case. To include a comment in the file, preface the line with a pound (#) character. These lines will be ignored.

If Define Server commands are included in the file, they will not take effect until the LRS is rebooted. Define Port commands will not take effect until the specified ports are logged out. Define Site commands will take effect when the specified site is started.

The configuration file must not contain any initialization commands (for example, Initialize or Crash). Because the file is read when the LRS boots, a "reboot" command in the file would cause the LRS to boot perpetually. You would then have to flush the LRS' NVR to correct the error.

Testing the configuration file is strongly recommended. To test the file, use the **Source** command, discussed on page 13-164.

An example of a configuration file is displayed below:

Figure 2-14: Configuration File

```
DEFINE PORT 2 SPEED 9600
DEFINE PORT 2 PARTIY NONE
# The following commands set up the ports:
DEFINE PORT 2 ACCESS DYNAMIC
```

2.3.10.2.2 Host Configuration

A configuration file can be downloaded from a TCP/IP host (via TFTP) or from a NetWare fileserver.

If you're using a TCP/IP host, ensure that TFTP loading is enabled on your host and place the configuration file in a download directory. If you're using a NetWare host, place the configuration file in the fileserver's login directory.

2.3.10.2.3 LRS Configuration

To configure the LRS using the commands in the configuration file, use the **Source** command, discussed on page 13-164.

If the configuration file must be downloaded each time the LRS boots, the filename must be specified using the **Set/Define Server Startupfile** command. A TCP/IP filename must be specified in **host:filename** format, where **host** is an IP address. To download the configuration file from a NetWare fileserver, use the **node\sys:\login\filename** format.

NOTE: *If lower-case or non-alphabetical characters are used, the filename must be enclosed in quotes.*

For example, to download the file **config.sys** from TCP/IP host 192.0.1.110, the following command would be used:

Figure 2-15: Downloading From TCP/IP Host

```
Local>> DEFINE SERVER STARTUP "192.0.1.110:config.sys"
```

If the LRS has a nameserver defined, a text name may be specified as a TCP/IP host name. The LRS will attempt to resolve the name at boot time; if it cannot resolve the name, the download will fail. To designate a nameserver, see **Set/Define Server Nameserver** on page 13-130.

Figure 2-16 displays an example of a NetWare download configuration:

Figure 2-16: Downloading From NetWare Fileserver

```
Local>> DEFINE SERVER STARTUP “TROUT\SYS:\LOGIN\config.sys”
```

NOTE: *The LRS is not usable during download attempts.*

2.3.10.3 Download Sequence

During its boot sequence, the LRS will load its operational code first, then attempt to download the configuration file. If the attempt to download the configuration file is unsuccessful, the LRS may re-attempt the download. By default, the LRS will make a total of six attempts to download the file (one initial attempt, and five re-attempts). To change this setting, use the **Set/Define Server Startupfile Retry** command:

Figure 2-17: Setting Number of Download Attempts

```
Local>> DEFINE SERVER STARTUPFILE “TROUT\SYS:\LOGIN\config.sys” RETRY 10
```

If Retry is set to zero, the LRS can no longer be used; it will wait indefinitely for the configuration file to download.

3 Basic Remote Networking

3 - Basic Remote Networking

The LRS connects to remote nodes or networks using serial network links, which allow network traffic to flow through ordinary modems. This chapter discusses initiation, maintenance, and disconnection of these remote connections.

This chapter is intended to get users started remote networking. After completing this chapter, you should be able to configure the LRS to support the following:

- Incoming remote node
- Incoming character, PPP, and SLIP modes in a secure manner
- Basic outgoing LAN to LAN using PPP

The functionality described in this chapter may not meet all of your performance needs; in addition, it will not ensure complete network security. If your network requires more complex configuration, or if you are not using modems, refer to Chapter 4, *Additional Remote Networking*, for additional configuration instructions.

3.1 Connection Types

The LRS enables two types of remote networking connections: LAN to LAN and remote node.

In **LAN to LAN** connections, the LRS provides a link between two networks. The LRS will communicate with a remote **router**, which may be another remote access server, a UNIX machine capable of PPP routing, or another LRS. The LRS may be connected to the remote router with temporary “dial on demand” connections such as ordinary dialup modems. The LRS may also be permanently connected to the remote router with leased lines, a statistical multiplexor, or a direct serial connection.

LAN to LAN connections are often used to connect two locations that don’t always need to be connected. For example, a small remote office with only a few nodes and a central office might need to be connected occasionally, however, the amount of traffic wouldn’t warrant using a leased line for the connection. Using an LRS and dialup modems, the connection could come up and go down when required, simulating a permanent connection between the two locations.

A **remote node** connection enables a single remote node (such as a PC) to use a network’s services. For example, a laptop user on a business trip may wish to access files from a network’s file server. Using a modem, the laptop could dial the LRS, form a connection, and download the files as if the laptop were directly connected to that network.

The LRS cannot initiate connections to remote nodes. Remote nodes must call the LRS when they wish to communicate with the network.

3.2 Managing Connections With Sites

A **site** represents a remote physical location, for example, a remote router or a remote node. Sites are referenced by a name, such as **seattle**. The site's name should indicate the physical location of the remote device, a group of remote node users, or a particular remote node user.

NOTE: *Using sites for connections enables each connection to have different characteristics; connections aren't limited solely to the characteristics of the port used.*

Sites serve four purposes:

- To configure the LRS and the remote router appropriately for a connection. For example, particular LRS ports may be assigned for use with the connection.
- To enforce specific network requirements. For example, compression may be required for all connections.
- To manage a connection once it is in place. For example, it may be desirable to control the amount of bandwidth used for a connection.
- To enable a system administrator to monitor a single connection. For example, a system administrator may wish to restrict remote node users to a particular range of IP addresses.

Every incoming and outgoing remote networking connection, whether LAN to LAN or remote node, has a site associated with it. To create and edit sites, see *Setting Up Sites* on page 3-3.

The type of authentication used determines which site will be used. For more information, see *Incoming LAN to LAN and Remote Node* on page 3-9 and *Outgoing LAN to LAN Connections* on page 3-13.

3.2.1 Incoming Connections (Remote Node or LAN to LAN)

Incoming connections can use either custom sites, or temporary sites which use the **default** site's configuration.

Custom sites allow the most flexibility in the control and configuration of incoming connections. They are used when a specific configuration is required for the incoming router or remote node, and should be named for the location or user that is calling the LRS. Custom sites are required for Dialback and recommended for incoming LAN to LAN connections.

If a group of incoming connections can use the same configuration, they can be allocated temporary sites used only for that session to save time and system resources. Each temporary site takes its configuration from the LRS **default site**. The default site may be customized in the same manner as custom (named) sites; this customized configuration can then be shared with many remote routers and remote nodes.

NOTE: *The default site configuration is listed in Table 3-1 on page 3-4.*

When an incoming caller is allocated a temporary site, the name of the site is based on the port receiving the call. For example, an incoming call to port 3 may be allocated a temporary site named **Port3**.

3.2.2 Outgoing LAN to LAN Connections

A site must be configured for each outgoing LAN to LAN connection. This site controls when and how the LRS will call the remote location, what protocols to use, and when to terminate the connection.

Outgoing sites are typically named for the remote router that the LRS will call; for example, if a site is used for outgoing connections to a remote router in Dallas, the site used for the connection might be named **dallas**. This site could also be used for incoming calls; if the router in Dallas needed to call the first LRS, it could use dallas to make the connection.

3.2.3 Setting Up Sites

The **Define Site** commands are used to create new sites and edit existing sites. The **Show/Monitor/List Sites** commands are used to get information about existing sites.

These commands require privileged access, and each example in this section denotes privileged status with the **Local>>** prompt. For information on obtaining privileged access, see **Set Privileged/Noprivileged** on page 13-124.

3.2.3.1 Creating a New Site

To create a new site, assign a name using the following command:

Figure 3-1: Creating New Site

```
Local>> DEFINE SITE IRVINE
```

When a site is defined, it uses a “factory default” configuration (see Table 3-1, *Default Site Configuration*). The site’s settings may then be modified at will.

3.2.3.2 Displaying Existing Sites

To display currently active sites, use the **Show Site** command. To display all defined sites, use the **List Site** command.

To display specific information about sites, the following parameters may be used in conjunction with Show Site and List Site: IP, IPX, Ports, Counters, and Status. For example, to display the IP configuration of site **irvine**, use the following command:

Figure 3-2: Displaying a Site’s IP Configuration

```
Local>> LIST SITE IRVINE IP
```

NOTE: *The List Site command is used in Figure 3-2 because site irvine isn’t currently running.*

3.2.3.3 Default Site Configuration

The default site configuration is used for all temporary sites. To display this configuration, use the following command:

Figure 3-3: Displaying Default Site

```
Local>> LIST SITE DEFAULT
```

The following table lists the default site configuration.

Table 3-1: Default Site Configuration

Characteristic	Configuration in Default Site
CHAP authentication on outgoing calls	Disabled
PAP authentication on outgoing calls	Disabled
Remote password	None configured
Local password	None configured
Username	None configured
Chat script entries	None
IP / IPX compression	Enabled
IP / IPX packet forwarding	Enabled
Maximum idle time	10:00 (10 minutes)
Remote host's IP configuration	Undefined
IP compression slots	16
IPX compression slots	16
IPX keepalive spoofing	Enabled
Maximum packet size (MTU): PPP	1522
Ports defined	None
PPP	Enabled
SLIP	Disabled
Telephone number of remote site	None defined
Outgoing packet filter	None defined
Incoming packet filter	None defined
Idle time filter	None defined
Startup filter	None defined
Maximum packet size (MTU): SLIP	1500
Maximum Session Time	Disabled

3.2.4 Editing Sites

All site characteristics can be edited with the **Define Site** commands. For example, a site's authentication can be edited with the command below:

Figure 3-4: Editing Site Characteristic

```
Local>> DEFINE SITE irvine AUTHENTICATION PAP DISABLED
```

NOTE: *All Define Site commands are described beginning on page 13-31.*

Currently active sites can be edited, but changes will not take effect until the site is logged out.

3.2.5 Testing Sites

The **Test Site** command causes a site to start as if outgoing traffic for the site had come into the LRS. It allows users to test sites without having to generate packet traffic. To test a site, enter a command similar to the following.

Figure 3-5: Testing a Site

```
Local>> TEST SITE irvine
```

The terminal will display a message that the specified site has started. To stop the test, enter the Logout Site command followed by the site name.

In the event that there is a problem with the site, or the Test Site command does not work, the LRS site logging feature may be useful. See Set / Define Logging Site on page 13-96 and Show / Monitor / List Logging Site on page 13-152 for more information.

3.2.6 Deleting Sites

To delete a site, use the **Purge Site** command.

Figure 3-6: Deleting a Site

```
Local>> PURGE SITE irvine
```

When the Purge command is used with the default site, the site's default configuration will be restored. Any editing changes you've made to the default site will be removed.

Figure 3-7: Restoring Default Site Configuration

```
Local>> PURGE SITE DEFAULT
```

3.3 IP, IPX, and AppleTalk Addressing

3.3.1 IP Address Assignment

By default, sites use “unnumbered” interfaces for IP. The IP address of the Ethernet connected to the LRS will be used as the IP address on all LRS serial ports. This reduces the amount of required configuration and eliminates the need to allocate a separate IP network for each port.

When the LRS receives an incoming connection request (remote node or LAN to LAN), an IP address is negotiated for the caller. The address agreed upon depends on the caller’s requirements; some don’t have a specific address requirement, while others must use the same IP address each time they log into the LRS.

NOTE: *PPP negotiation is covered in Chapter 8, PPP.*

For a complete discussion of IP address assignment (including configuration instructions), see *Remote Networking IP Address Assignment* on page 5-15.

3.3.2 IPX Address Assignment

Every IPX network (including all serial links to remote sites) must be assigned a unique IPX network number. When the LRS is initially configured, a range of IPX network numbers (a **netrange**) must be defined. The LRS will use the netrange to allocate a network number to each port.

To specify the base number of the range, use the **Set/Define IPX Netrange** command. Each serial port is assigned a network number equalling the sum of the base number and its port number.

Figure 3-8: Defining IPX Netrange

```
Local>> DEFINE IPX NETRANGE 0x100
```

NOTE: *The complete syntax of Set/Define IPX Netrange is listed on page 13-92.*

3.3.3 AppleTalk Address Assignment

The LRS comes pre-configured with a server name which will be used to identify it on the AppleTalk network. In addition to a name, the LRS will need a valid network number. It can obtain a startup network number when it is first attached to the AppleTalk network, and use the startup number until it can obtain a valid network number from an AppleTalk router on the network.The LRS will also need to be assigned to an AppleTalk zone. Initially, it will appear in the default zone.

NOTE: *To change any of these parameters, see Chapter 7, AppleTalk.*

3.4 IP and IPX Routing

The following sections discuss IP and IPX routing issues as they pertain to remote networking. For a complete discussion of IP Routing, refer to Chapter 5, *IP*. For coverage of IPX routing, see Chapter 6, *IPX*.

When a packet is received from or generated for a remote network, the LRS will check its routing table to determine the most efficient route to the destination. If the LRS does not have a route to a remote network, it cannot send the packet to the destination.

The entries in the routing table are one of three types:

Local routes	The network that is directly attached. This route is automatically determined from the LRS IP address and network mask, and is never deleted.
Static routes	Routes that were manually entered in the routing table by a system administrator. These routes are used when dynamic routes cannot be.
Dynamic routes	Routes learned through the receipt of RIP (Routing Information Protocol) packets.

Each routing entry can point to another router on the Ethernet or to a site configured for LAN to LAN connections.

3.4.1 Outgoing LAN to LAN

Generally, the LRS has static routes configured for each remote LAN that it will connect to. These routes point to sites that are configured for outgoing LAN to LAN connections. The first time that the LRS needs to send a packet destined for a network on a remote LAN, the site will be activated and the LRS will attempt to call the remote router. Once the connection has been formed, subsequent packets for the remote LAN will be forwarded over that link.

While the LRS is connected to the remote router, it may learn additional dynamic routes from that remote router. Once these additional routes are entered into the routing table, packets may be routed to these new networks as well. Once the connection is dropped, the LRS can be configured to maintain these routes. Subsequent traffic to these dynamically learned networks or to the pre-existing static route networks will cause the site to form a new connection.

If the LRS is a **stub router** (or you're using the LRS to connect to the Internet), default routes can be used to reduce configuration time. A stub router connects a LAN without any other routers to a larger LAN. For example, in a remote office with no other outside connections, an LRS that connects to exactly one other (larger) location is a stub router. All traffic generated on the remote office's LAN that is destined for the remote location must pass through the LRS. A default route pointing to the larger site may be entered on the LRS.

NOTE: *Default routes should be used with caution. See Chapter 5, IP, or Chapter 6, IPX, for complete details.*

3.4.2 Incoming LAN to LAN

If RIP is being used, no static routing entries need to be configured on the LRS. Routes to networks on the remote LAN will be learned automatically.

NOTE: *RIP is enabled by default.*

If RIP is not being used, the LRS must have a specific site configured for this incoming connection. The remote router must use this site when it connects to the LRS. The site may be started in one of two ways: through the authentication sequence (which requires that authentication be appropriately configured), or with the **Set PPP <sitename>** command. Static routes pointing to the site must be configured for each of the incoming caller's IP or IPX networks.

NOTE: *To configure authentication, see Setting up Incoming LAN to LAN and Remote Node on page 3-12, or Chapter 12, Security.*

3.4.3 Remote Node

The LRS automatically generates routes for remote nodes when the node connects. These routes are deleted when the connection is terminated.

If the remote node receives a dynamic address from the LRS IP address pool, a **host route** is entered for that address. If proxy ARPing is enabled (see *Proxy ARP* on page 5-14), the LRS will proxy-ARP for the address. See *Host Routes* on page 5-12 for more information.

If a remote node uses an IP address that is not on the Ethernet's IP network, then the LRS will enter a **network route** for that node. For example, if the LRS's Ethernet IP address is 192.0.1.4, and a node selects the address 192.0.2.6, the LRS will enter a route to 192.0.2.0 in its routing table.

IPX remote nodes are always on the IPX network assigned to the port that the call was received on. The LRS will add a route to that port's network number.

Remote nodes do not have to make routing decisions, as they can only send network packets to the LRS. Therefore, most remote nodes do not need to receive RIP packets. Sites that only support remote nodes may turn off RIP to reduce traffic on the connection.

Figure 3-9: Disabling RIP Packets

```
Local>> DEFINE SITE IP RIP DISABLED
Local>> DEFINE SITE IPX RIP DISABLED
```

NOTE: *For more information about disabling RIP, see Define Site IP on page 13-39 or Define Site IPX on page 13-41.*

3.5 PPP and SLIP

The LRS uses asynchronous serial lines to connect remote locations. A protocol is then run on this serial connection to allow network packets to be sent.

The LRS supports the use of PPP and SLIP to send network packets.

PPP PPP is the Point to Point protocol. Its use is recommended wherever possible. PPP enables devices to simultaneously transport IP and IPX packets, negotiate certain options, authenticate users, and use checksums with virtually no performance loss.

SLIP SLIP is the Serial Line Internet Protocol. It is supported primarily for backwards compatibility with equipment that doesn't support PPP. SLIP can only transport IP packets—it does not support negotiation of IP addresses or other options, nor does it provide any diagnostic facilities.

To enable PPP and/or SLIP (they are both disabled by default), use the **Define Ports PPP** and **Define Ports SLIP** commands. For more information on these commands, see *Port Modes* on page 9-3.

Figure 3-10: Enabling PPP and SLIP on a Port

```
Local>> DEFINE PORT 2 PPP ENABLED
Local>> DEFINE PORT 2 SLIP ENABLED
```

3.6 Incoming LAN to LAN and Remote Node

When an incoming LAN to LAN or remote node connection is initiated, there are a number of ways that PPP or SLIP may be started:

- The caller may be presented with a Local> prompt (the port will be in character mode), requiring him to enter commands in order to run PPP or SLIP.

NOTE: *For a description of the port modes, see Port Modes on page 9-3.*

- The port may detect when a PPP or SLIP packet is received and automatically run the appropriate protocol.
- The port may be dedicated to PPP or SLIP; the protocol will automatically run when any character is received.

A port may be configured to offer a combination of these methods; giving the incoming remote node or router flexibility in how the connection is started.

To configure the LRS for incoming LAN to LAN and remote node connections, see *Setting up Incoming LAN to LAN and Remote Node* on page 3-12.

3.6.1 Starting PPP or SLIP from the Local> Prompt

The Set PPP and Set SLIP commands may be entered from the Local> prompt. The remote router or node must pass through the authentication procedures, if enabled, on the port in character mode. The remote device must support chat scripts or must rely on a user to enter the required information and type Set PPP or Set SLIP at the Local> prompt.

NOTE: *For a complete description of authentication, refer to Chapter 12, Security. For information on chat scripts, see Chat Scripts on page 4-7.*

If no site name is given in the Set PPP or Set SLIP command, a temporary copy of the default site will be started. If a custom site is to be started, it can be specified as a string: **Set PPP <sitename>**.

NOTE: *To prevent users from starting inappropriate sites, users can be prompted for the site's local password.*

To use the Set PPP / Set SLIP commands, PPP and / or SLIP must be enabled on the port used for the connection. See *PPP and SLIP* on page 3-8.

3.6.2 Starting PPP or SLIP Using Automatic Protocol Detection

Automatic Protocol Detection allows the LRS to determine what type of connection the remote device is attempting to establish. By detecting which protocol is to be run on each connection, a port can support character mode (Local> prompt) connections, PPP connections, and SLIP connections without reconfiguration. One modem pool can support all incoming connections; there is no need to dedicate ports to remote networking.

NOTE: *To configure autodetection, see Chapter 9, Ports.*

By default, the LRS detects character mode by looking for the return character.

If PPPdetect is enabled on the port, and a PPP packet is detected, PPP will be started with a temporary copy of the default site.

A custom site can also be run by enabling PPP authentication on the port. If the remote device sends a valid username and password and the username matches a site name, that site will start running on the port. All further configuration of the connection will be from this new site.

If PPP authentication is not enabled on this port, there is a security risk. Unauthorized users may gain access to your network. Use dedicated PPP mode with PPP authentication (CHAP or PAP) wherever possible. If PPP authentication is not possible, use port authentication and the Set PPP command to authenticate incoming calls.

NOTE: *To configure PPP authentication, see Chapter 12, Security.*

If SLIPdetect is enabled on the port, and a SLIP packet is detected, SLIP will be started. SLIP does not support authentication. Incoming connections to a port in dedicated SLIP mode cannot be authenticated. **This is a security risk in most situations. Unauthorized users may gain access to your network. Use this mode with caution.**

Custom sites cannot be run when using dedicated SLIP as there is no method to switch sites once the temporary site is running. Start SLIP with the **Set SLIP** command to allow custom sites and to authenticate incoming calls.

3.6.3 Starting PPP or SLIP on a Dedicated Port

A port may be dedicated to PPP or SLIP mode. Whenever the port receives a character, it starts up a temporary copy of the default site using the appropriate link layer. The port cannot be used for character mode connections and the Local> prompt cannot be reached.

To dedicate a port, see *Preferred/Dedicated Services and Protocols* on page 9-7.

Once PPP or SLIP is running, the behavior of a dedicated port is the same as a port with automatic protocol detection enabled. See *Starting PPP or SLIP Using Automatic Protocol Detection* on page 3-9 for information about security issues.

3.6.4 Incoming Connection Sequence

The following steps detail the events that occur when the LRS receives an incoming call.

3.6.4.1 Port Automatically Runs PPP or SLIP

If the port receiving the call is using automatic protocol detection, or is dedicated to SLIP or PPP, the following sequence of events will take place:

1. If automatic protocol detection (for PPP, SLIP, or both) is enabled, the link layer will start up automatically when a PPP or SLIP character is received from the incoming call. If the port is dedicated, the link layer will start upon the receipt of any character.
2. The caller will be attached to a temporary site. The name of this site will be based on the port number used. For example, an incoming call to port number 6 will generate a temporary site named **Port6**.
   A. If using SLIP, callers will continue to use the temporary site for the remainder of the connection.

B. If using PPP, the following steps will occur:

1. If the LRS port receiving the call has been configured to authenticate remote hosts using CHAP or PAP, CHAP / PAP will request a username and password from the remote host. If the remote host has been configured to send a username and password, it will send the pair to the LRS.

2. The username and password will be compared to existing site names. One of the following will occur:

a. If the username matches the name of a site, the site will be checked to see if it has a local password. If it does, this will be compared to the password entered by the caller. If the passwords match, the user will begin using the custom site; the temporary site will stop running.

b. If the site isn't configured with a password, or the password entered by the caller doesn't match the site password, the username / password pair will be compared to any authentication databases. One of two outcomes is possible:

If a match is found, the connection will be successfully authenticated, and the caller will continue using the temporary site for the remainder of the connection.

If a match is not found, the connection attempt will fail.

3.6.4.2 Port Doesn't Automatically Run PPP or SLIP

If an incoming call is received on an LRS port that's not configured to automatically run PPP or SLIP, the following login sequence will occur:

1. The caller sends a carriage return.

2. If the port is configured to prompt for a login password, the caller must enter the correct login password to continue. If the port is configured to prompt for a username, the caller must then enter a username. If the port is configured for authentication, the caller will need to enter a valid password for the username.

3. To start the link layer, the user will need to enter commands to start PPP or SLIP. One of two scenarios will occur:

A. If the caller specifies a particular site to be started when PPP or SLIP is started, the user will be attached to this site. If the site has been configured to prompt for its local password, the user will have to enter the site's local password. At this point, the caller will be unable to run another site.

B. If a site isn't specified, the user will be attached to a temporary site. The name of this site will be based on the port number used. For example, an incoming call to port number 6 will generate a temporary site named **Port6**. This site will be used for the remainder of the call.

NOTE: *Incoming LAN to LAN connections will need to enter commands via a chat script.* *See Chat Scripts on page 4-7.*

3.6.5 Setting up Incoming LAN to LAN and Remote Node

Configuring the LRS for LAN to LAN and remote node networking involves the following steps.

1. Configure the Ports

   Port configuration for incoming connections involves a number of factors: whether PPP or SLIP will be used, whether the ports will be dedicated to PPP or SLIP, whether autodetection of PPP or SLIP will be used, and if a modem is attached to any of the ports, how it will be configured.

   To configure a port's use of PPP or SLIP, see Chapter 9. To configure modems, see Chapter 10.

2. Create the Sites

   If users will be starting up custom sites (by entering a username that matches an existing site name), those sites must be created. See *Creating a New Site* on page 3-3 for instructions.

3. Configure Authentication

   Two types of authentication can be configured: use of the server login password, and username/password pairs for individual users.

   A. Login Password

   In order to use a login password, a port must be in character mode. See Chapter 9, *Ports,* to configure a port's use of modes.

   Determine a login password and set the password using the **Set/Define Server Login Password** command. Then enable the use of the login password on the appropriate port(s) using the **Set/Define Ports Password** command.

Figure 3-11: Defining Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
Local>> DEFINE PORT 3 PASSWORD ENABLED
```

NOTE: *LRS passwords are case-independent, even when enclosed in quotes.*

By default, incoming Telnet and Rlogin connections are not required to enter the login password. To require the login password, use the **Set/Define Server Incoming** command, described on page 13-128.

B. Username/Password Authentication

Enable authentication on the appropriate ports.

Figure 3-12: Enabling Authentication

```
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
```

If authentication should be performed before PPP or SLIP is running (while the port is still in character mode), ensure that autodetection of PPP and SLIP is disabled (see Figure 3-13). If the port automatically detects and runs PPP or SLIP, there will be no way to authenticate the user because the local prompt cannot be accessed.

Keep in mind that PPPdetect and SLIPdetect will only need to be disabled on ports that have PPP and / or SLIP enabled.

Figure 3-13: Disabling Autodetection of PPP and SLIP

```
Local>> DEFINE PORT 2 PPPDETECT DISABLED
Local>> DEFINE PORT 2 SLIPDETECT DISABLED
```

In order for SLIP users to perform authentication, SLIPdetect **must** be disabled. SLIP users will only be able to authenticate incoming connections while the port is in character mode; once the port is running SLIP (for example, if the port is dedicated to SLIP using the Set / Define Port SLIP Dedicated command), authentication cannot be performed.

If the port is configured to automatically run PPP, and you'd like to use CHAP or PAP to obtain a username and password from the incoming caller, enable remote CHAP and / or PAP authentication on the desired port.

Figure 3-14: Enabling CHAP Authentication

```
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 PPP PAP REMOTE
```

NOTE: *CHAP and PAP may both be enabled on the same port.*

If incoming connections will be entering usernames to start a custom site, ensure that the site has a local password. Callers will be required to enter this password in order to start the site.

Figure 3-15: Configuring Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION LOCAL "gorilla"
```

Configure any databases that will be used for authentication and add the appropriate usernames and passwords. See Chapter 12, *Security*, for configuration instructions.

3.7 Outgoing LAN to LAN Connections

When the LRS receives a packet, it will consult its routing table to determine the best route to the packet's destination. If the specified route points to a site, a connection to the site may be initiated. The connection will be subject to any restrictions defined for the site, such as a startup filter or time of day restrictions.

While a connection to the remote router is initiated, a limited number of packets will be buffered until the connection is formed. When the connection is successful, the packets will be sent.

NOTE: *To restrict outgoing connections, see Chapter 12, Security.*

3.7.1 Ports

Each site must specify which LRS port(s) may be used for outgoing connections. More than one port may be specified; for example, site **dallas** might specify that port 2 or port 3 could be used for outgoing connections.

When the LRS attempts to make a connection to a site, it will attempt to use one of the specified ports. If the port is busy (in use with another connection), it will attempt to make a connection using another specified port. The LRS uses the port priority setting to determine which ports to try and in what order. In the following example, site dallas will try port 2 first, then port 3.

Figure 3-16: Port Priority for Sites

```
Local>> DEFINE SITE dallas PORT 2 PRIORITY 1
Local>> DEFINE SITE dallas PORT 3 PRIORITY 2
```

If all ports are busy, the LRS will time out the site for a few minutes and then try again. The connection timeout between call attempts is user configurable. See **Define Site Time Failure** on page 13-46.

More than one site may specify a particular port. For example, site **dallas** and site **seattle** might specify that port 3 may be used for connections. If site dallas is using port 3 at a certain time and site seattle is started, seattle will attempt a connection using another specified port. If no other port is specified for site seattle, it will wait until port 3 becomes available.

NOTE: *To learn how incoming calls use ports and sites, see Incoming LAN to LAN and Remote Node on page 3-9.*

3.7.2 Telephone Numbers

Each site may specify one port-independent telephone number and one or more port-specific telephone numbers. A port-independent telephone number is typically used if all ports are configured to call the same number, for example, if the ports are calling a telephone hunt group. Port-independent telephone numbers should be used whenever possible; this frees a site to dial the remote site's number from any of the ports the site is associated with.

Port-specific telephone numbers are used when a particular LRS port should call a specific number at the remote site. These numbers will override a port-independent telephone number. For example, in order to get the most efficient use out of connected modems, a site might specify that when port 2 (connected to a high speed modem) is used, another high speed modem should be dialed. When port 3 (connected to a slow speed modem) is used, the LRS should dial another slow speed modem.

If a site does not have a telephone number defined, the LRS assumes either that there's a direct connection between the LRS and the remote host, or that a chat script (see Chapter 4, *Additional Remote Networking*) will be used to communicate with the remote host.

3.7.3 Authentication

The remote site may require that the LRS authenticate itself by sending a username and password. The username that the LRS sends is (by default) the site name. To send a different username, use the **Define Site Authentication Username** command, described on page 13-32.

The password sent is a site-specific password called the **remote password**. The remote password is used only for outgoing connections, and must be sent via PPP. See *Configure Authentication* on page 3-16 for configuration instructions.

SLIP does not support authentication. To perform authentication, SLIP users must use **chat scripts**. See *Chat Scripts* on page 4-7.

3.7.4 Setting up Outgoing LAN to LAN Connections

To configure the LRS for outgoing connections, complete the steps in the following sections.

3.7.4.1 Configure Ports

All ports that will support outgoing connections must be configured for dynamic connections. Use the following command:

Figure 3-17: Permitting Outgoing Connections

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

NOTE: *For more information on port configuration, see Chapter 9, Ports.*

3.7.4.2 Configure Modems

Enable modem operation on the port(s) used for outgoing calls. Then assign a **modem profile** to the port using the Define Port Modem Type command.

Figure 3-18: Enabling Modem Operation

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 5
```

NOTE: *A modem profile automatically sets up a port for a specific type of modem. Define Ports Modem Type is listed on page 13-27. Modem profiles and complete modem configuration instructions are discussed in Chapter 10, Modems.*

3.7.4.3 Create a Site

Every outgoing connection must use a site. Each site is initially created with a default set of configurations. To display the current configuration, use the **List Site** command:

Figure 3-19: Listing a Site's Configuration

```
Local>> LIST SITE irvine PORTS
```

NOTE: *To create a site, see Creating a New Site on page 3-3.*

List Site can be used with a number of parameters, which display different aspects of a site's configuration. For example, the **List Site Ports** will display all ports associated with the site.

3.7.4.4 Select Port(s) to Use for Dialing Out

Once a site is created, the port(s) that it will use to dial the remote location must be defined. Each site must be associated with at least one port. Use the following command:

Figure 3-20: Associating a Site With a Port

```
Local>> DEFINE SITE irvine PORT 2
```

NOTE: *The Define Site commands are listed individually beginning on page 13-31.*

3.7.4.5 Assign A Telephone Number to the Port or Site

If the site will be used with modems, at least one telephone number must be specified so that the site can dial a remote host. The number may be assigned specifically for use with a particular port, or for use with any port. To assign a port-specific telephone number, use the **Define Site Port Telephone** command:

Figure 3-21: Assigning a Port Telephone Number

```
Local>> DEFINE SITE irvine PORT 2 TELEPHONE 547-9549
```

To assign a telephone number to the site that may be used with any port, use the **Define Site Telephone** command:

Figure 3-22: Assigning a Site Telephone Number

```
Local>> DEFINE SITE irvine TELEPHONE 867-5309
```

A port-specific telephone number will override a site telephone number. For example, site **irvine** may be configured to use the number **635-9202** on any port it's using, but only the number **845-7000** when it's using port 3.

3.7.4.6 Configure Authentication

When an outgoing connection is attempted, the remote router may or may not require the LRS to authenticate itself. One of the following scenarios will generally apply:

- The remote router uses CHAP or PAP to prompt the LRS to authenticate itself

  This scenario is the most common; the configuration instructions in this section assume that CHAP or PAP will be used.

- The remote router requires a login password

  In this case, the LRS will need to use a chat script to communicate this password to the remote router. See Chapter 4, *Additional Remote Networking*, for instructions.

- The remote router does not require authentication

  The instructions in this section will not be necessary. Continue to *Configure Routing* on page 3-17.

Before configuring authentication, ensure that you have the username and password required to log into the remote router. In addition, determine whether the remote router will use PAP or CHAP to transmit the username and password.

Configure the username and remote password to be transmitted.

Figure 3-23: Defining Local Username and Password

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME “doc_server”
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE “giraffe”
```

If CHAP will be used, enable CHAP on the site. To use PAP to transmit the username and password, enable PAP on the site.

Figure 3-24: Enabling CHAP / PAP Authentication

```
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE irvine AUTHENTICATION PAP ENABLED
```

3.7.4.7 Configure Routing

Static routes to the sites must be entered in the IP and IPX routing tables. To configure IP Routing, see Chapter 5, *IP*. To configure IPX routing, see Chapter 6, *IPX*.

3.8 Monitoring Networking Activity

To monitor current remote networking activity, use the **Show Site** or **Monitor Site** command. Show Site enables you to display the activity associated with a particular site, including the number of packets received and transferred, idle time, current state of the site’s ports, and configuration of its associated protocols (for example, IP). Monitor Site will update and redisplay this information at three-second intervals.

Table 3-2: Show / Monitor Site Commands

Command	Description
Show / Monitor Sites	Lists currently running sites.
Show / Monitor Site <sitename>	Displays the site’s configuration.
Show / Monitor Site <sitename> Counters	Displays the site’s current performance.
Show / Monitor Site <sitename> Status	Shows all sites that have attempted or completed connections.
Show / Monitor Site <sitename> Status	Shows cumulative statistics for this site. Statistics are reset upon boot.

During active connections, Show / Monitor Site commands will display the current state of the site or of its assigned ports. The state of the port or site depends on the activity taking place. For exam-

ple, a port may be in an idle state, then transition to an on-line state when it begins transferring packets. The possible site states are listed in Table 3-3.

Table 3-3: Site States

Site State	Activity During State
Idle	The site is idle.
Startup	A user, PPP, or SLIP requested that the site start running.
Waiting	The site is waiting for a port to connect.
Connect	The site is connected and passing packet traffic.
Logout	The site was instructed to shut down.
Closing	The site is shutting down PPP or SLIP.
Freeing	The site is removing itself from memory.
NVR	A **List Site** command was used to display site information. The site's configuration is displayed, not its current activity.

The possible port states of ports assigned to the sites are listed in Table 3-4.

Table 3-4: State of Ports Assigned to a Site

Port State	Activity During State
Idle	The site is not currently using this port. The port may be in use by other sites.
Dial	The remote modem is being dialed.
Chat	The chat script defined in the site is being executed. See Chapter 4, *Additional Remote Networking* for a definition of chat scripts.
Link	PPP is being negotiated with the remote router or remote node. (This state does not apply to SLIP users).
Ready	PPP negotiation has been completed. (This state does not apply to SLIP users).
Online	Traffic is being forwarded to the remote site.

3.9 Examples

3.9.1 LAN to LAN - Calling one Direction Only

An LRS in a remote office in Dallas must call an LRS at the company headquarters in Seattle. This LAN to LAN connection must meet the following criteria:

- IP users in a remote office in Dallas must connect to IP network 192.0.1.0, which is located at the company headquarters in Seattle.
- Novell users in Dallas must connect to the Novell file server called MServ in Seattle. This file server has the internal network number 1234abcd.
- The NetWare network in Seattle uses frame type 802.3 and network number 56ce.
- The NetWare network in Dallas uses frame type 802.2 and network number ab12.
- There are no NetWare network numbers in the range 0x131-0x133.
- The LRS in Seattle never calls Dallas.
- Both IP and IPX traffic must be transferred.
- The LRS in Seattle must support character mode users as well as the LRS in Dallas.
- After 60 seconds of idle time, the connection between Dallas and Seattle should be timed out.

The configurations for the Dallas and Seattle offices are shown on the following two pages.

3.9.1.1 LRS in Dallas

This LRS must be configured for outgoing LAN to LAN connections.

Figure 3-25: Dallas LRS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>>
Local>> DEFINE SITE SEATTLE AUTHENTICATION USERNAME “dallas”
Local>> DEFINE SITE SEATTLE AUTHENTICATION REMOTE “xyz”
Local>> DEFINE SITE SEATTLE AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE SEATTLE IDLE 60
Local>> DEFINE SITE SEATTLE PORT 2
Local>> DEFINE SITE SEATTLE TELEPHONE 2065551234
Local>>
Local>> DEFINE IP ROUTE 192.0.1.0 SITE SEATTLE 2
Local>>
Local>> DEFINE IPX FRAME 802.2 NETWORK ab12
Local>> DEFINE IPX FRAME 802.2 ENABLED
Local>> DEFINE IPX NETRANGE 130
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX SERVICE MServ 4 1234abcd 00-00-00-00-00-01 451 2
Local>> DEFINE IPX ROUTE 1234abcd SITE SEATTLE 2 10
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

The **Initialize Server Delay 0** command will reboot the LRS; when the unit has rebooted, changes made with the Define commands will be in effect.

3.9.1.2 LRS in Seattle

This LRS must be configured in the following way:

Figure 3-26: Seattle LRS Configuration

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>> DEFINE PORT 2 PPPDETECT ENABLED
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>> LOGOUT PORT 2
Local>>
Local>> DEFINE SITE dallas AUTHENTICATION LOCAL “xyz”
Local>> DEFINE IPX FRAME 802.3 ENABLED
Local>> DEFINE IPX FRAME 802.3 NETWORK 56ce
Local>> DEFINE IPX NETRANGE 140
Local>> DEFINE IPX ROUTING ENABLED
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

3.9.2 LAN to LAN - Bidirectional (Symmetric) Calling

An LRS in a remote office in Dallas must be able to call an LRS at the company headquarters in Seattle. This LAN to LAN connection must meet the following criteria:

- The LRS in Seattle must also be able to call Dallas.
- Both IP and IPX traffic must be transferred.
- IP users in Dallas must connect to IP network 192.0.1.0 in Seattle. IP users in Seattle must connect to IP network 192.0.2.0 in Dallas.
- Novell users in Dallas must connect to the Novell file server called MServ in Seattle. This file server has the internal network number 1234abcd. There are no file servers located in Dallas.
- The network in Seattle uses frame type 802.3 and network number 56ce. The network in Dallas uses frame type 802.2 and network number ab12.
- There are no NetWare network numbers in the range 0x141-0x143.
- Both remote access servers are to be dedicated to this purpose. No other applications are to be supported.
- After 60 seconds of idle time, the connection between Dallas and Seattle should be timed out.
- The LRS in Seattle expects the username **dallas** and the password **xyz**. The LRS in Dallas expects the username **seattle** and the password **abc**.

3.9.2.1 LRS in Dallas

This LRS must be configured for incoming and outgoing LAN to LAN connections:

Figure 3-27: Dallas LRS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
Local>>
Local>> DEFINE SITE SEATTLE AUTHENTICATION USERNAME “dallas”
Local>> DEFINE SITE SEATTLE AUTHENTICATION LOCAL “abc”
Local>> DEFINE SITE SEATTLE AUTHENTICATION REMOTE “xyz”
Local>> DEFINE SITE SEATTLE AUTHENTICATION CHAP
Local>> DEFINE SITE SEATTLE IDLE 60
Local>> DEFINE SITE SEATTLE PORT 2
Local>> DEFINE SITE SEATTLE TELEPHONE 2065551234
Local>>
Local>> DEFINE IP ROUTE 192.0.1.0 SITE SEATTLE 2
Local>>
Local>> DEFINE IPX FRAME 802.2 NETWORK ab12
Local>> DEFINE IPX FRAME 802.2 ENABLED
Local>> DEFINE IPX NETRANGE 130
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX SERVICE MServ 4 1234abcd 00-00-00-00-00-01 451 2
Local>> DEFINE IPX ROUTE 1234abcd SITE SEATTLE 2 10
Local>>
Local>> INITIALIZE SERVER DELAY 0
```

The **Initialize Delay 0** command will reboot the LRS; when the unit has rebooted, changes made with the Define commands will be in effect.

3.9.2.2 LRS in Seattle

The Seattle LRS will have different authentication, telephone, site and router information than the LRS in Dallas. In all other respects, it is configured identically to the Dallas LRS.

Figure 3-28: Seattle LRS Configuration

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 2 SPEAKER DISABLED
Local>>
Local>> DEFINE SITE DALLAS AUTHENTICATION USERNAME “seattle”
Local>> DEFINE SITE DALLAS AUTHENTICATION LOCAL “xyz”
Local>> DEFINE SITE DALLAS AUTHENTICATION REMOTE “abc”
Local>> DEFINE SITE DALLAS AUTHENTICATION CHAP
Local>> DEFINE SITE DALLAS IDLE 60
Local>> DEFINE SITE DALLAS TELEPHONE 2145556789
Local>>
Local>> DEFINE IP ROUTE 192.0.2.0 SITE SEATTLE 2
Local>>
Local>> DEFINE IPX FRAME 802.3 ENABLED
Local>> DEFINE IPX FRAME 802.3 NETWORK 56ce
Local>> DEFINE IPX NETRANGE 130
Local>> DEFINE IPX ROUTING ENABLED
Local>>
Local>> INITIALIZE DELAY 0
```

3.9.3 Remote Node

This example sets up ports 2 and 3 to support IP and IPX remote node users via PPP. All users will use temporary copies of the default site and may authenticate with CHAP, PAP, or chat scripts. Modems on port 2 and 3 will be automatically configured.

IP users will be forced to use either IP address 192.0.1.7 or 192.0.1.8. One IP user **wwwserver**, must have the same address (192.0.2.6) each time it logs in.

3.9.3.1 Configuring the Port

Figure 3-29: Configuring the Port

```
Local>> DEFINE PORT 2-3 PPPDETECT ENABLED
Local>> DEFINE PORT 2-3 PPP ENABLED
Local>> DEFINE PORT 2-3 PPP CHAP REMOTE
Local>> DEFINE PORT 2-3 PPP PAP REMOTE
Local>> DEFINE PORT 2-3 AUTHENTICATE ENABLED
Local>> DEFINE PORT 2-3 MODEM ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 1
Local>> DEFINE PORT 3 MODEM TYPE 2
```

3.9.3.2 Configure IP to Allocate IP Addresses to Incoming Users

Figure 3-30: Configuring IP

```
Local>> DEFINE IP IPADDRESS 192.0.1.6
Local>> DEFINE IP ETHERNET POOL 192.0.1.7 192.0.1.8
Local>> DEFINE IP ETHERNET PROXY-ARP ENABLED
```

3.9.3.3 Configure IPX Network Range

Figure 3-31: Configuring IPX

```
Local>> DEFINE IPX NETRANGE 500
```

3.9.3.4 Configure Range of IP Addresses for Users of Default Site

Figure 3-32: Configuring Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.7 192.0.1.8
```

3.9.3.5 Configure a Static IP Address Site

Figure 3-33: Configuring Static IP Address

```
Local>> DEFINE SITE wwwserver REMOTEIP 192.0.2.6
Local>> DEFINE SITE wwwserver IPX DISABLED
Local>> DEFINE SITE wwwserver AUTHENTICATION LOCAL “monkey”
```

3.10 Troubleshooting

The following table discusses some common problems that occur with remote networking configuration and proposes solutions for each.

Table 3-5: Common Remote Networking Problems

Problem	Remedy
Outgoing LAN to LAN site does not dial the modem.	Ensure that the site has ports and at least one telephone number assigned. Ensure that Modem Control is enabled (**Define Ports Modem Control** on page 13-20), and the modem profile is defined on the port. Ensure that the port's access is set to Dynamic or Remote (see **Set/Define Ports Access**, page 13-104). Ensure that routing is set correctly. **Show Site** should display the site as *waiting*, *dialback*, *startup*, or *connect*. See *IP Routing* (page 5-11) and *Routing* (page 6-2) for more information. Ensure that connections are allowed during this time. **Show Site** *SiteName* **Time** should show that the site is Enabled. If the site is already running, **Show Site** *SiteName* **Time** should display the next attempt time as "Any Time."
Modem dials, but does not connect.	Enable the modem's speaker using the **Define Ports Modem Speaker** command (page 13-26). Determine if the remote node is busy. Ensure that the correct number is being called. Check the Error Correction and Compression configuration.
Chat script doesn't complete.	Enable chat script logging using the **Set/Define Logging** command (page 13-96).
Modem connects but connection drops.	Ensure that authentication is defined correctly on the outgoing site using **Define Site Authentication** on page 13-32. Authentication databases must be set up properly. Enable PPP and Site Logging using the **Set/Define Logging** command (page 13-96). Ensure that the usernames / passwords being used match the expected usernames / passwords on the remote site. Make sure the correct PPP authentication type (PAP or CHAP) is enabled on the outgoing site with **Define Site Authentication** (page 13-32).

Table 3-5: Common Remote Networking Problems, cont.

Problem	Remedy
Connection is established, but traffic does not flow.	Determine if the modems are passing data by checking the send and receive lights on the LRS and the modem; the lights should be flashing. Ensure that routes are configured correctly by using the **Show/Monitor/List IP Routes** (page 13-149) and **Show/Monitor/List IPX Routes** (page 13-151) commands. Enable IP and IPX logging using the **Set/Define Logging** command (page 13-96). Check the packet filters, if any (**Show/Monitor/List Filter**). The packets may be restricted by one of the configured rules.
Link keeps starting up for unknown reason.	Using the **Set/Define Logging** command (page 13-96), set IP logging to level 2 or greater to see which host is causing the problem.

3.11 Quick Reference

Managing Connections			
To	**Use This Command**	**Example(s)**	**What Example Does**
Manage Connections Using a Custom Site	Define Site, page 13-31.	`DEFINE SITE dallas`	Creates a custom site named “dallas”. When a connection is made to a remote LRS in Dallas, “dallas” manages the connection, including when the link is brought up and down. See *Managing Connections With Sites* on page 3-2 for more information.
Display a Site’s Configuration (Custom Site or Default Site)	Show / Monitor / List Sites, page 13-161.	`LIST SITE default`	Displays information about the default site, including whether PPP or SLIP is used, CHAP / PAP status, and any filter lists associated with the site. See *Displaying Existing Sites* on page 3-3 for more information.
Edit a Custom or Default Site Configuration	Define Site <characteristic>, beginning on page 13-31.	`DEFINE SITE irvine AUTHENTICATION PAP DISABLED`	Disables PAP authentication for site “irvine”. See *Editing Sites* on page 3-5 for more information.
Delete a Site	Purge Site, page 13-54.	`PURGE SITE irvine`	Deletes site “irvine”. See *Deleting Sites* on page 3-5 for more information.
		`PURGE SITE default`	Restores the default site to its factory default configuration; any changes will be removed.

IP Address Assignment

To	Use This Command	Example(s)	What Example Does
Restrict Incoming Callers to a Range of Addresses	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.250`	Incoming callers will be assigned an IP address between 192.0.110 and 192.0.1.250. Each time the caller successfully connects to the LRS, this address will be assigned. See *Specifying IP Address Range for a Site* on page 5-16 for more information.
Restrict Incoming Callers to a Particular IP Address	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108`	Incoming callers will be assigned IP address 192.0.1.108. Each time the caller successfully connects to the LRS, this address will be assigned. See *Specifying Specific IP Address for a Site* on page 5-16 for more information.
Dynamically Assign IP Addresses to Incoming Callers From an Address Pool	Set / Define IP All / Ethernet Pool, page 13-82.	`DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59`	Incoming callers will be assigned a dynamic IP address between 192.0.1.50 and 192.0.1.59. See *IP Address Pools* on page 5-15 for more information.
	Set / Define IP All / Ethernet Proxy-ARP, page 13-82.	`DEFINE IP ETHERNET PROXY-ARP ENABLED`	Enables proxy ARPing; the LRS will respond to ARP requests for the addresses in the pool. See *Proxy ARP* on page 5-14 for more information.

IP Routing

To	Use This Command	Example(s)	What Example Does
Configure a Static Route to Remote Hosts (For Outgoing LAN to LAN Connections)	Set / Define IP Route, page 13-87.	`SET IP ROUTE 198.8.8.0 NEXTROUTER 192.0.1.9 4`	Creates an entry in the IP routing table; packets to 198.8.8.0 will be sent to the router 192.0.1.9. The route will have a metric of 4. See *Outgoing LAN to LAN* on page 3-7 for more information.
Use RIP to Automatically Learn Routing Information	No command needed -- RIP is enabled by default on the default site and all custom sites.		

IPX Address Assignment

To	Use This Command	Example(s)	What Example Does
Define the Range of IPX Network Numbers Assigned to the LRS Serial Ports	Set / Define IPX Netrange, page 13-92.	`DEFINE IPX NETRANGE 0x100`	LRS serial ports will be assigned IPX network numbers starting from 0x101, and extending to the sum of 0x100 + the total number of ports. On the LRS16, this range of network numbers is 0x101 to 0x116. See *IPX Address Assignment* on page 3-6 for more information.

IPX Routing

To	Use This Command	Example(s)	What Example Does
Configure a Static Route to Remote IPX Networks (For Outgoing LAN to LAN Connections)	Set / Define IPX Route, page 13-93.	`SET IPX ROUTE 1234 NEXTROUTER 45af-00-00-ab-12-e2-38`	Creates an entry in the IPX routing table; packets to IPX network 1234 will be sent to router 45af-00-00-ab-12-e2-38. See *Outgoing LAN to LAN* on page 3-7 for more information.
Use RIP to Automatically Learn Routing Information	No command needed -- RIP is enabled by default on the default site and all custom sites.		See *Incoming LAN to LAN* on page 3-7 for more information.

Incoming LAN to LAN and Remote Node (Overall Configuration)

To	Use This Command	Example(s)	What Example Does
Configure Ports	See Chapter 9, *Ports*.		
Create a Custom Site	Define Site, page 13-31.	`DEFINE SITE irvine`	Creates a custom site named “irvine”. See *Managing Connections With Sites* on page 3-2 for more information.
Force Users to Enter a Login Password	1. Set / Define Server Login Password, page 13-129.	`DEFINE SERVER LOGIN PASSWORD badger`	Defines “`badger`” as the login password. See on page 3-12 and Chapter 12, Security, for more information.
	2. Set / Define Ports Password Enabled, page 13-116.	`DEFINE PORT 2 PASSWORD ENABLED`	Incoming callers on port 2 will be forced to enter the login password, “`badger`”.

Incoming LAN to LAN and Remote Node (Overall Configuration), cont.

To	Use This Command	Example(s)	What Example Does

Force Users to Enter a Username / Password Pair Before PPP / SLIP Runs	1. Define Ports PPPdetect Disabled, page 13-30.
	
	or Set / Define Ports SLIPdetect Disabled, page 13-120.
		`DEFINE PORT 2 PPPDETECT DISABLED`
		
		`DEFINE PORT 2 SLIPDETECT DISABLED`
			Disables autodetection of PPP / SLIP on port 2.
			
			See on page 3-12 or *Automatic Protocol Detection* on page 9-4 for more information.

	2. Set / Define Ports Authenticate Enabled, page 13-104.	`DEFINE PORT 2 AUTHENTICATE ENABLED`	Incoming callers on port 2 will be forced to enter a username / password pair. This pair will be checked against any configured authentication databases. See on page 3-12 or *Chapter 12, Security*, for more information.

Use PAP or CHAP to Obtain the Username and Password From the Incoming Caller	Define Ports PPP, page 13-29.	`DEFINE PORT 2 PPP CHAP REMOTE`
		
		`DEFINE PORT 2 PPP PAP REMOTE`
			When username / password authentication is required on port 2, PAP or CHAP will be used to obtain the username / password from the remote host.
			
			See on page 3-12 or *Chapter 12, Security*, for more information.

Configure Authentication Databases	Set / Define Authentication, page 13-62.	`DEFINE AUTHENTICATION NETWARE PRIMARY bozo_serv`	Defines NetWare file server “bozo_serv” as the primary authentication database. See on page 3-12 or *Chapter 12, Security*, for more information.
Enable Callers to Start a Custom Site When Entering a Username / Password Pair	Define Site Authentication Local, page 13-32.	`DEFINE SITE irvine AUTHENTICATION LOCAL “linus”`	When an incoming caller is prompted to enter a username / password pair, entering “irvine” and the password “linus” will start site “irvine”. See on page 3-12 or *Chapter 12, Security* for more information.

Outgoing LAN to LAN (Overall Configuration)

To	Use This Command	Example(s)	What Example Does
Configure Ports to Support Outgoing Connections	Set / Define Ports Access Remote, page 13-104.	`DEFINE PORT 2 ACCESS REMOTE`	Enables outgoing connections on port 2. See *Port Doesn't Automatically Run PPP or SLIP* on page 3-12 or *Accessing a Port* on page 9-1 for more information.
Configure the Modem for Outgoing Calls	1. Define Ports Modem Control Enabled, page 13-20.	`DEFINE PORT 2 MODEM ENABLED`	Enables modem operation on port 2. See *Configure Modems* on page 3-15 or *Outgoing Calls* on *page 10-7* for more information.
	2. Define Ports Modem Type, page 13-27.	`DEFINE PORT 2 MODEM TYPE 5`	Assigns modem profile 5 to port 2. See *Configure Modems* on page 3-15 or *Modem Profiles* on page 10-2 for more information.
Create a Site to Connect to a Particular Remote Host	Define Site, page 13-31.	`DEFINE SITE dallas`	Creates a custom site named "dallas". See *Managing Connections With Sites* on page 3-2 for more information.
Edit a Site's Configuration	Define Site <characteristic>, beginning on page 13-31.	`DEFINE SITE dallas AUTHENTICATION PAP DISABLED`	Disables PAP authentication for site "dallas". See *Editing Sites* on page 3-5.
Associate a Site With a Port or Ports	Define Site Port, page 13-43.	`DEFINE SITE dallas PORT 2`	Associates site "dallas" with port 2. See *Select Port(s) to Use for Dialing Out* on page 3-16 for more information.

Outgoing LAN to LAN (Overall Configuration), cont.

To	Use This Command	Example(s)	What Example Does
Define the Telephone Number Used to Dial the Remote Host	Define Site Port Telephone, page 13-43.	`DEFINE SITE dallas PORT 2 TELEPHONE 547-9549`	When an outgoing connection attempt is made on port 2 using site “dallas”, “547-9549” will be dial the remote host. See *Assign A Telephone Number to the Port or Site* on page 3-16 for more information.
Send a Login Password to the Remote Host	See Chapter 4, *Additional Remote Networking*.		
Configure a Username and Password to Transmit to a Remote Host	1. Define Site Authentication Username, page 13-32.	`DEFINE SITE dallas AUTHENTICATION USERNAME “doc_server”`	When site “dallas” is used, if the remote host requires that the LRS authenticate itself, the username “doc_server” will be sent. See *Configure Authentication* on page 3-16 or *Offering Authentication Information to the Incoming Caller* on page 12-3 for more information.
	2. Define Site Authentication Remote, page 13-32.	`DEFINE SITE dallas AUTHENTICATION REMOTE “secret”`	The password “secret” will be sent.

Use PAP or CHAP to Transmit the Username and Password to the Remote Host	Define Site Authentication PAP / CHAP, page 13-32.	`DEFINE SITE irvine AUTHENTICATION CHAP ENABLED`
		
		`DEFINE SITE irvine AUTHENTICATION PAP ENABLED`
			When the remote host requires that the LRS authenticate itself, PAP or CHAP will be used to transmit the username / password to the remote host.
			
			See *Configure Authentication* on page 3-16 or Chapter 12, *Security*, for more information.

Configure IP / IPX Routing	To configure IP routing, see Chapter 5, *IP*. To configure IPX routing, see Chapter 6, *IPX*.		

Monitoring Connections

To	Use This Command	Example(s)	What Example Does
List Currently Running Sites	Show / Monitor / List Sites, page 13-161.	`SHOW SITE`	Displays all active sites. See *Monitoring Networking Activity* on page 3-17 for more information.
Displays a Site's Configuration	Show / Monitor / List Sites, page 13-161.	`SHOW SITE IRVINE IP`	Displays IP configuration information for site "irvine". See *Monitoring Networking Activity* on page 3-17 for more information.
Displays a Site's Current Performance	Show / Monitor / List Sites Counters, page 13-161.	`SHOW SITE IRVINE COUNTERS`	Displays the current performance of site "irvine". See *Monitoring Networking Activity* on page 3-17 for more information.
Display all Sites that Have Attempted or Completed Connections	Show / Monitor / List Sites Status, page 13-161.	`SHOW SITE STATUS`	Displays statistics for all sites that have been active since the LRS was booted. See *Monitoring Networking Activity* on page 3-17 for more information.

4 Additional Remote Networking

4 - Additional Remote Networking

This chapter discusses how to “fine-tune” remote networking and related features on your LRS. Performance and cost issues are covered, as well as how to manage bandwidth on demand, use direct connections and leased lines, and restrict access to the LRS.

4.1 Security

4.1.1 Authentication

Authentication may be used to restrict users to a particular configuration when they log into a port. When a username is entered in the local authentication database, a series of commands may be associated with that user. These commands (including starting a site) will be executed when the user is successfully authenticated.

To execute commands when a user logs into the LRS, complete the following steps.

1. Ensure that authentication databases have been configured using the **Set/ Define Authentication** command (page 13-62).
2. Associate commands with a username by entering the **Set/Define Authentication User Command** command. When the user is successfully authenticated, these commands will be executed.

Figure 4-1: Restricting User to Particular Site

```
Local>> DEFINE AUTHENTICATION USER “bob” COMMAND “set ppp dialin_users”
```

In the example above, when user **bob** logs into the LRS, he will automatically run site **dialin_users.**

Authentication must then be enabled on each port that will be used for incoming logins.

NOTE: *See Chapter 12, Security, for a comprehensive discussion of authentication.*

4.1.2 Filter Lists

Filters enable the LRS to restrict packet traffic. Each filter specifies a particular rule, for example, only IP packets are permitted passage. Packets that pass the filter are forwarded; all others are discarded.

Filters are organized into ordered filter lists, referenced by name. For example, a filter named **firewall** may permit forwarding of packets that match a particular IP rule, but deny passage to packets that match a generic rule.

Filter lists are associated with sites. Table 4-1 describes the available filter lists and how they are used.

Table 4-1: Types of Filter Lists

Type of Filter List	Purpose
Idle	Determines whether the site will remain active. Packets that pass the filter will reset the site's idle timer, preventing the site from being timed out.
Incoming	Determines whether to forward incoming packets received from a remote site. Packets that pass the filter will be forwarded.
Outgoing	Determines whether to forward outgoing packets to a remote site. Packets that pass the filter will be forwarded.
Startup	Determines whether a site will initiate a connection to a remote site. When a packet passes the filter, the LRS will initiate an outgoing connection. (If an outgoing connection currently exists, this filter will be ignored).

When a site with an associated filter list receives a packet, the LRS compares the packet against each filter starting with the first filter on the list. If the packet matches any of the filters, the packet is forwarded or discarded according to the filter's specification. If the packet does not match any of the filters in the list, it is not forwarded.

The order filters appear in a list is very important. For example, consider the following filter list:

1. Allow any packet
2. Deny all IP traffic matching a particular rule

When this filter list is associated with a site, all packets are forwarded. Packets are compared to filters in the order in which the filters appear in the list. Because all packets match the specification of "any packets," all packets are forwarded without being compared to the second filter.

Switching the order of the filters has a significant effect. Examine the filter list below, where the order of the above two filters is reversed:

1. Deny all IP traffic matching a particular rule
2. Allow any packet

When this filter list is used, all IP traffic matching the specified rule is discarded. Therefore, some IP packets are discarded without being compared to the second filter.

To prevent all packet traffic from a particular protocol (for example, all IP packets), filter lists do not need to be used. Use the **Define Site IP/IPX Disabled** command:

Figure 4-2: Preventing IPX Packet Traffic

```
Local>> DEFINE SITE irvine IPX DISABLED
```

Configuring filter lists involves two primary steps: creating the filter list, and associating the list with a particular site. See *Setting up Filter Lists* on page 12-24 for complete configuration instructions.

4.1.3 Restricting IP Addresses

To enhance security, incoming callers can be restricted to a specific IP address or range of addresses. This restriction may be defined in each site. See *Remote Networking IP Address Assignment* on page 5-15 for more information.

4.1.4 Restricting Incoming Logins to a Particular Site

If the username has been configured to run a series of commands when it's authenticated (one of these commands may be starting a particular site), these commands will be executed. Executing a particular site automatically when a user logs in can force a user to use a specific configuration; see *Forcing Execution of Commands* on page 12-8.

4.1.5 Restricting Authenticated Logins by a Single User

The LRS can be configured to prevent a single PPP or Local mode user from making multiple authenticated connections to the LRS. If two users attempt to log into authenticated ports with the same username, only the first user will be allowed to connect. See *Restricting Multiple Authenticated Logins* on page 12-20 for details.

4.2 IP Configuration

4.2.1 RIP

RIP (Routing Information Protocol) packets enable the LRS to broadcast its known routes and receive routing information from other routers. Each site may configure RIP in a number of ways.

4.2.1.1 Disabling RIP

By default, LRS sites will both listen for and send RIP packets. However, in some situations, RIP should be disabled. For example, if the routers on both sides of a link have been pre-configured with all necessary routing information (with static routes), learning routing information through RIP updates won't be necessary.

To disable RIP on a particular site, use the **Define Site IP RIP** command:

Figure 4-3: Disabling RIP

```
Local>> DEFINE SITE irvine IP RIP DISABLED
```

If you want the LRS to either listen for or send RIP packets, but not both, you can selectively disable one or the other. The following example turns of listening for RIP packets.

Figure 4-4: Disabling RIP Listen

```
Local>> DEFINE SITE irvine IP RIP LISTEN DISABLED
```

4.2.1.2 Interval Between RIP Updates

When RIP sending is enabled, the LRS will send RIP updates every thirty seconds by default. This number can be adjusted; for example, the update interval may be raised so that RIP updates are sent every minute to reduce network traffic.

To configure the update interval, use the **Define Site IP RIP Update** command. The interval must be specified in seconds; intervals between 10 and 255 seconds are permitted.

Figure 4-5: Adjusting RIP Update Interval

```
Local>> DEFINE SITE irvine IP RIP UPDATE 60
```

4.2.1.3 Configuring the Metric

Each RIP packet lists known routes and the "cost" associated with each of these routes. Each LRS site may configure the cost of its interface; all routes learned through the site will be associated with that cost.

When a router determines a route to a particular destination, a route with a lower cost is more likely to be included in the route. Configuring a higher RIP cost on a particular site makes the interface a less desirable route to other destinations.

To set the site's IP RIP metric, use the **Define Site IP RIP Metric** command.

Figure 4-6: Configuring a Site's RIP Metric

```
Local>> DEFINE SITE irvine IP RIP METRIC 4
```

In the example above, all routes learned through site **irvine** will be associated with cost 4. The higher the cost number, the less desirable the route.

NOTE: *If IP RIP sending is disabled on a site, the Update and Metric values will be ignored.*

4.2.2 Header Compression

Each site may enable or disable compression of IP header information. When a site is created, IP header compression will be enabled by default.

To disable IP header compression, use the following command:

Figure 4-7: Disabling IP Header Compression

```
Local>> DEFINE SITE irvine IP COMPRESS DISABLED
```

NOTE: *For complete IP configuration instructions, see Chapter 5, IP.*

4.2.3 NetBIOS Nameserver (NBNS)

Windows 95 users can run NetBIOS over IP and use a primary or secondary NetBIOS nameserver (NBNS) for name resolution. This allows Windows 95 clients to use the Network Neighborhood browser without any additional configuration on the Windows 95 host. For more information, see *Using the NetBIOS Nameserver (NBNS)* on page 5-18.

4.3 IPX Configuration

4.3.1 RIP and SAP

RIP and SAP packets enable the LRS to broadcast its known routes and services and obtain this information from other routers. Each site may configure RIP and SAP in a number of ways.

When a new site is created, RIP and SAP Listen and Update are enabled. During connections controlled by this site, the LRS will listen to RIP and SAP packets and will send RIP and SAP updates when information has changed. In some situations (for example, to reduce network traffic), RIP and / or SAP should be disabled.

To edit a site's RIP or SAP configuration, use the **Define Site IPX RIP/SAP** command. Figure 4-8 displays some examples.

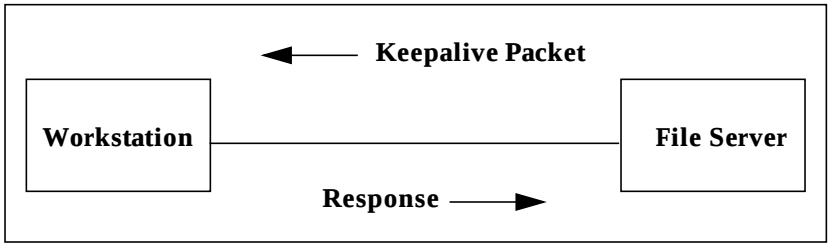
Figure 4-8: RIP and SAP Configurations

```
Local>> DEFINE SITE irvine IPX RIP SEND ENABLED
Local>> DEFINE SITE irvine IPX SAP LISTEN DISABLED
```

4.3.2 Spoofing

When an IPX file server is connected to a workstation or another file server, it will send **keepalive** packets to the remote host. It will expect a response in return; the response will let the file server know that the workstation or file server is still connected.

Figure 4-9: Keepalive Packet



When an LRS is used to connect a remote workstation to a file server, or to connect two networks, the keepalive packet traffic may keep a connection active when there isn't any interactive traffic. For example, if a keepalive packet destined for a remote workstation is routed through a communication server such as the LRS, the communications server will normally bring up a connection to the workstation to forward the packet if a connection isn't currently in place.

To reduce the cost of initiating connections simply for keepalive packet traffic, the LRS can be configured to send these packets and responses to and from the file server and workstation, or between two file servers. This is called **spoofing.**

In the remote node case, the file server will send keepalive packets and responses for both file servers (if two file servers are connected) or for the file server and workstation. This enables the link between the LRS and the remote host to remain idle until there is interactive packet traffic. Figure 4-10 displays an example.

Figure 4-10: LRS Spoofing For Workstation

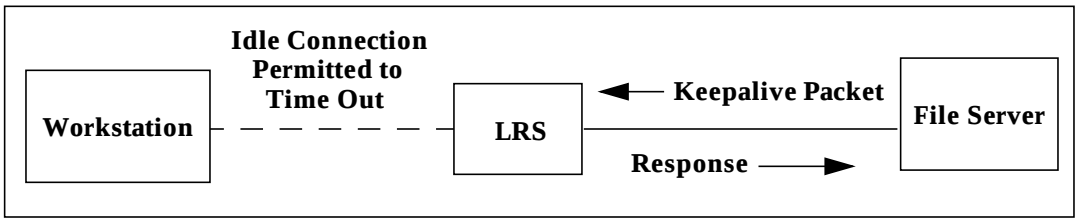
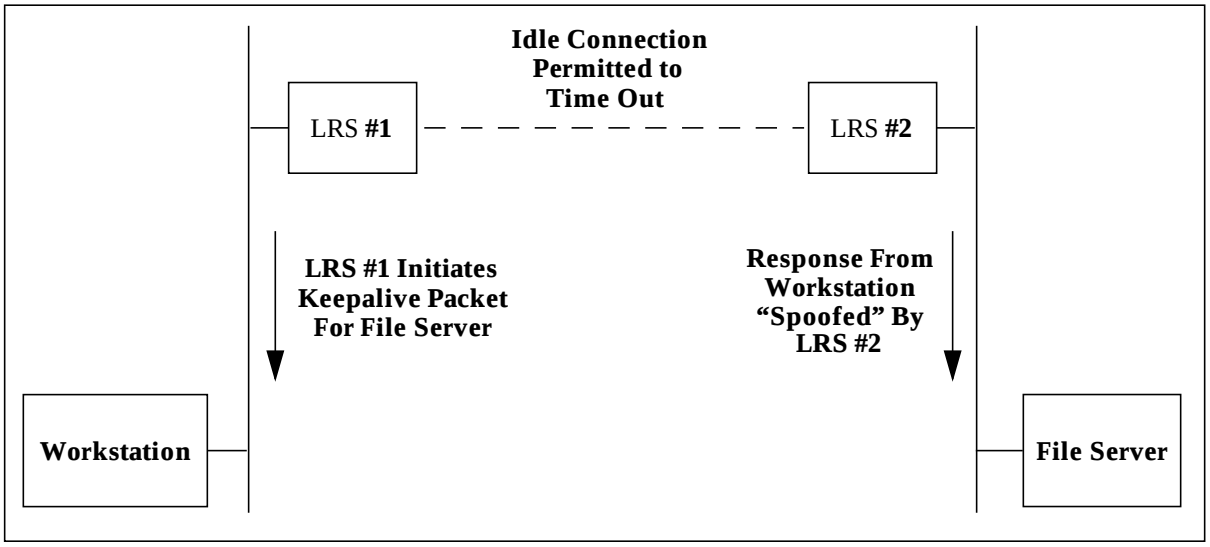


Figure 4-11 displays a LAN to LAN spoofing example, where two LRS's are connected. In this case, the servers send the keepalive packet and the response for the workstation and file server; the keepalive traffic is never transmitted across the link between the two servers.

Figure 4-11: Spoofing in LAN to LAN Connection



If LRS #1 does not hear from the workstation within a set time period, it will assume that the workstation is no longer connected. It will then initiate a connection to LRS #2 and inform the server that it should stop spoofing the workstation's response to the file server.

Spoofing is enabled by default. To disable spoofing, use the **Define Site IPX Keepalive** command.

Figure 4-12: Disabling IPX Spoofing

```
Local>> DEFINE SITE irvine IPX KEEPALIVE DISABLED
```

4.3.3 Header Compression

Each site may enable or disable compression of IPX header information. By default, header compression is enabled; to disable it, use the following command:

Figure 4-13: Disabling IPX Header Compression

```
Local>> DEFINE SITE irvine IPX COMPRESS DISABLED
```

NOTE: *For a complete discussion of IPX routing, refer to Chapter 6, IPX.*

4.4 Chat Scripts

Chat scripts enable the LRS to communicate with virtually any type of equipment at the remote site. They are typically configured to send a string of characters, then wait to receive a particular string in return.

For example, the LRS might log into a remote site that has a login program. Using a chat script defined for the site, the LRS could send carriage returns until the login prompt is returned, send a username, wait for the password prompt, and send a password.

4.4.1 Creating a Chat Script

Chat scripts are defined one line at a time following a given syntax. A chat script to be used for outgoing connections from a particular site can be created with **Define Site Chat** commands. These commands enable you to do the following: send a particular string, replace, add, or delete existing lines in the script, expect a particular string, and configure timeout periods.

For example, to configure the script to send or expect strings, use the following command:

Figure 4-14: Sending and Expecting Strings

```
Local>> DEFINE SITE irvine CHAT SEND “hello?”
Local>> DEFINE SITE irvine CHAT EXPECT “login:”
```

NOTE: *Chat script expect strings are case-sensitive.*

4.4.2 Editing and Adding Entries

To replace, delete, or insert entries, specify the line numbers. Figure 4-15 displays a few examples.

Figure 4-15: Editing Script Entries

```
Local>> DEFINE SITE irvine CHAT REPLACE 1 EXPECT “login:”
Local>> DEFINE SITE irvine CHAT DELETE 4
Local>> DEFINE SITE irvine CHAT AFTER 3 EXPECT “login:”
Local>> DEFINE SITE irvine CHAT BEFORE 3 EXPECT “login:”
```

To determine the number of a particular line, display the script using the **List Site Chat** command. All chat script entries for that site will be displayed.

4.4.3 Configuring Timeouts

The **Define Site Chat Timeout** command enables you to configure the timeout after an Expect command, or a delay before a Send command is executed. Figure 4-16 displays some examples.

Figure 4-16: Setting Timeouts and Delays

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT “login:”
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 SEND “hello?”
```

The first command in Figure 4-16 will cause the LRS to wait two seconds for a response from the remote host after sending an Expect command. If no response is received after two seconds, the chat script will fail or return to the previous fail marker. The second command will send the “hello?” string after a 4-second delay.

The default Send timeout (delay before a Send command is executed) is 0; in other words, strings will be sent right away. The default timeout for Expect commands is 30 seconds.

4.4.4 Setting Markers

The **Fail** parameter sets a marker in a chat script for a Timeout command. When the Timeout associated with an Expect command expires (the expected string is not received within the specified number of seconds) the LRS will return to the last command containing the Fail parameter. The script will be executed from that point, continuously looping if the Expect command repeatedly fails.

Figure 4-17: Expect / Fail Script

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL
Local>> DEFINE SITE irvine CHAT SEND “\r“
Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT “login:”
```

The script in Figure 4-17 will send a carriage return, then wait for two seconds while a “login:” string is expected. If the “login:” string is not received within two seconds, the chat script will loop back to the Fail command and continue running from that point. Each time the Expect command fails (the “login:” string is not received within two seconds), the Fail counter is decremented one value. When the Expect command has failed four times (the “login:” string is never received), the looping will stop and the chat script will exit.

NOTE: *For more information on characters that can be sent as part of the chat string, see* *Define NetWare Internal on page 13-35.*

4.5 Bandwidth On Demand

The following sections explain bandwidth on demand concepts and outline the basic configuration needed to utilize LRS bandwidth on demand functionality. For more detailed instructions on setting up both sides of a bandwidth on demand connection, refer to *Multilink PPP* on page 8-4.

4.5.1 Remote Node Connections

Remote Node sites have a fixed bandwidth. The LRS cannot add or remove bandwidth for Remote Node connections.

4.5.2 LAN to LAN Connections

By default, sites will only attempt to bring up one port to a remote site in a LAN to LAN connection. If the amount of incoming data on the Ethernet exceeds the current bandwidth of the serial port (and the LRS is configured not to dial up additional bandwidth), **congestion** occurs and the extra data is discarded.

To avoid congestion, the LRS enables you to customize a site's use of bandwidth. As it is needed, additional bandwidth will be added. The LRS will assign more ports to the site until it has enough bandwidth or reaches a certain threshold. When it is no longer needed, the extra bandwidth will be removed.

NOTE: *Some protocols can detect congestion and will avoid it by sending smaller amounts of data at one time.*

4.5.2.1 How Bandwidth is Controlled

A site's use of bandwidth is controlled by the following factors:

- The **initial** and **maximum bandwidth** allotted to the site. These are static values.
- The **threshold** at which additional bandwidth should be added. This threshold is a percentage of the currently-dialed bandwidth.
- The **threshold** at which unnecessary (unused) bandwidth should be removed. This threshold is a percentage of the currently-dialed bandwidth.
- The **period of time** during which the current bandwidth usage is measured.
- The **delay** between bandwidth adjustments.

By default, additional bandwidth will not be added to a connection. In order for a connection to have flexible bandwidth (bandwidth that is added and removed as necessary), the site's maximum bandwidth must be configured, as well as the thresholds at which bandwidth is added and removed.

NOTE: *The initial bandwidth allotted to the site may also be configured. This is optional.*

The thresholds at which bandwidth is added and removed should have some room between them to regulate how often bandwidth is added and removed. It is recommended to set the "add bandwidth" threshold to a percentage between 80 and 100 percent; the "remove bandwidth" threshold should generally bet set to less than 50%. If the threshold values are set too close to one another, the connections will **thrash**; in other words, bandwidth will be continuously added and dropped.

The order in which ports are selected to be added and removed is controlled by a priority setting; when LRS bandwidth needs change, ports with the highest priority are the first to be added and the last to be removed.

Bandwidth is controlled by the host that initiates the call. If the LRS initiates a call, it controls the bandwidth for each site. If the LRS receives an incoming call, the bandwidth is controlled by the remote host.

The LRS will always use at least one port for a connection, even if the traffic is below the "remove bandwidth" threshold. If this is not desired behavior, the last connection can be controlled by the idle timer.

NOTE: *To configure the idle timer, see Set/Define Server Inactivity on page 13-127.*

4.5.2.2 Disadvantages of Additional Bandwidth

Increasing bandwidth by bringing up additional links has two disadvantages: increased cost and reduced resources. Phone rates will go up as more phone lines are used, and fewer ports will be available for other purposes. Assess your needs carefully before increasing bandwidth.

4.5.2.3 Configuring Bandwidth Allocated to Sites

To configure bandwidth, complete the configurations in the following sections.

4.5.2.3.1 Estimating Each Port's Bandwidth

Before sites can be configured to use particular bandwidths, the bandwidth of each LRS port must be estimated in bytes per second. This estimate should be made based upon two factors: the amount of compression expected for typical data on this site, and the fastest data transfer rate that the local and remote modems can support.

The LRS will truncate the bandwidth setting to the nearest 100 bytes per second. For example, a setting of 5790 will be truncated to 5700.

Consider the following example. Site irvine may use LRS port 2 and port 3 (if needed) for connections. A V.34 modem with a baud rate of 28800 bits per second is attached to each port. The remote modems are also V.34 modems with the same baud rate. Compression is enabled and a 2:1 compression rate is expected, which will increase the data transfer between the modems to 57600 bits per second.

The bandwidth for ports 2 and 3 should be estimated as follows:

Figure 4-18: Estimating a Port's Bandwidth

```
Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 5800
Local>> DEFINE SITE irvine PORT 3 BANDWIDTH 5800
```

NOTE: *If you are using 8 bits, no parity, and 1 stop bit, the modem will actually transmit ten bits for each byte.*

If the modems attached to a series of LRS ports are all going to be calling similar remote modems, these ports should be set to the same bandwidth estimates. In addition, if several ports have compression enabled, you should assume that the compression rate on each port will be the same (for example, a 2:1 compression rate). Avoid using small variations in bandwidth estimates.

It is important to make bandwidth estimates correctly. The LRS will attempt to reduce the total number of ports in use by using higher bandwidth ports (of the same priority) first until the bandwidth goal is met.

4.5.2.3.2 Assigning Port Priority Numbers

Priority numbers enable a site to determine which of its assigned ports it should use first for outgoing calls. The highest priority ports, those with higher priority numbers, will be used first. As additional bandwidth is needed, lower priority ports will be used in descending order of priority.

To assign priority numbers to a site's ports, use the following command:

Figure 4-19: Assigning Priority Numbers

```
Local>> DEFINE SITE irvine PORT 2 PRIORITY 2
```

NOTE: *By default, all ports are assigned a priority of* ***1.***

4.5.2.3.3 Specifying the Bandwidth Measurement Period

A period must be specified (in seconds) during which the LRS will measure a site's use of bandwidth. The measurement taken during this period will be compared to the Add and Remove values (see below) to determine if bandwidth should be added or removed. Short periods may lead to "thrashing".

Figure 4-20: Specifying Measurement Period

```
Local>> DEFINE SITE irvine BANDWIDTH PERIOD 60
```

4.5.2.3.4 Specifying when Bandwidth is Added or Removed

Determine when bandwidth will be added to or removed from a site. This is specified in terms of a percentage; when a site's bandwidth use on its currently-dialed ports reaches or falls below this percentage, bandwidth will be added or removed as appropriate.

Figure 4-21: Determining When Bandwidth Will Be Added/Removed

```
Local>> DEFINE SITE irvine BANDWIDTH ADD 90
Local>> DEFINE SITE irvine BANDWIDTH REMOVE 40
```

4.5.2.3.5 Configuring the Delay Between Bandwidth Adjustments

Determine the minimum period of time between one adjustment in bandwidth (addition or removal) and a following adjustment. Configure this delay using the **Define Site Bandwidth Holddown** command; by default, this timer is set to 60 seconds.

Figure 4-22: Configuring the Holddown Timer

```
Local>> DEFINE SITE irvine BANDWIDTH HOLDDOWN 30
```

The holddown timer helps to limit the “thrashing” caused by rapid adjustments in bandwidth. When the holddown timer is used in conjunction with a short bandwidth measurement period, the site will respond quickly to initial changes in packet traffic without thrashing.

In the example above, the holddown timer is set to 30 seconds. When bandwidth is added to site irvine, additional bandwidth cannot be added until 30 seconds have passed. Bandwidth changes in the opposite direction (addition or subtraction) require a delay of double the holddown timer, for example, when bandwidth is removed from irvine, it cannot be added for 60 seconds.

4.5.2.3.6 Configuring the Maximum Bandwidth Allotted to a Site

To configure a site’s maximum bandwidth, use the **Define Site Bandwidth Maximum** command. The amount must be specified in bytes per second.

Figure 4-23: Specifying Maximum Bandwidth

```
Local>> DEFINE SITE irvine BANDWIDTH MAXIMUM 11500
```

The maximum bandwidth value acts as a “ceiling.” In the example above, site irvine may receive additional bandwidth until the bandwidth reaches the configured number of bytes per second.

4.5.2.4 Displaying Current Bandwidth Settings

To display a site’s current bandwidth settings, use the **List Site Bandwidth** command.

Figure 4-24: Current Bandwidth Settings

```
Local>> LIST SITE irvine BANDWIDTH
LRS16 Version 1.1/101                    Name:              LRS_0C0021
   Hardware Addr: 00-80-a3-0c-00-21      Uptime:          1 Day 02:56
   Site Name:                 irvine     Period:                  60
   Add @ Utilization:       Disabled     Remove @            Disabled
   Maximum Bandwidth:            100     Initial Bandwidth:       100
   Multilink:               Disabled     Hold Down Timer:       01:00
   Input Utilization:              0%    Output Utilization:       0%
   Next Adjust Up:          Any Time     Next Adjust Down:   Any Time
   Target Bandwidth:                0    Waiting Bandwidth:         0
   On-line Bandwidth:               0
               Average Period    -- Input --   -- Output --    - Dropped -
                (in seconds)    Bytes/Second   Bytes/Second   Bytes/Second
   Size Total:               4             0              0              0
   Size Total:              60             0              0              0
```

To display how the LRS is currently managing a particular site’s use of bandwidth, use the **Show Site Bandwidth** command.

4.5.2.5 Restoring Default Bandwidth Settings

To return a site’s bandwidth parameters to their default values, use the following command:

Figure 4-25: Restoring Default Bandwidth Values

```
Local>> DEFINE SITE irvine BANDWIDTH DEFAULT
```

4.6 Performance and Cost Issues

4.6.1 Increasing Performance

4.6.1.1 Filtering Unwanted Data

To reduce the use of bandwidth for unwanted packet traffic, each site may configure an incoming and an outgoing **filter list**. Packets will be compared to these filter lists as they are received or generated. If they do not pass the filter, they will be discarded. See *Filter Lists* on page 4-1 for more details.

4.6.1.2 Compressing Data and Correcting Errors

The amount of data that can be transmitted at once (throughput) can be increased by using data compression. Data compression enables a device such as a modem to transfer a larger amount of data at once. When compression is used, uncompressed data arrives on the modem's serial port and the modem compresses the data before sending it over the phone line.

The disadvantage of compression is increased **latency**, the time required to transfer data from one place to another. Compression increases latency due to the time required to compress the data before it is sent. Error correction can also increase latency, as the data must be checked for integrity after it is received.

In situations where the delay is undesirable (for example, during interactive use over a long distance line), compression and error correction should not be used. These options are enabled by default on the LRS; to disable them, use the following commands:

Figure 4-26: Disabling Error Correction and Compression

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION DISABLED
Local>> DEFINE PORT 2 MODEM COMPRESSION DISABLED
```

NOTE: *For a complete discussion of compression and error correction, see Chapter 10, Modems.*

4.6.1.3 Adding Bandwidth

Like compression, adding bandwidth can increase throughput. Sites can be configured to automatically bring up additional connections when more bandwidth is needed, for example, when the amount of data to be transmitted exceeds the bandwidth of the port.

How "aggressively" a site will add bandwidth can be controlled with two factors: the period during which the use of bandwidth is measured, and the percentage at which bandwidth is added.

For example, to increase bandwidth for small or periodic increases in traffic, reduce the measurement time period. A similar effect could be obtained by reducing the percentage utilization at which bandwidth is increased. To require a sustained increase in traffic to increase bandwidth, the measurement time period and the utilization percentage should be increased. See *Bandwidth On Demand* on page 4-9 for more information.

4.6.1.4 Header Compression

Each site may be configured to compress the header information on IP (TCP only) and/or IPX packets before they are forwarded.

When IP or IPX headers are compressed, the LRS replaces the packet's header information with a **slot number**. This number is assigned dynamically, and denotes that the packet originated from a particular connection (for example, a Telnet session). When the destination receives the packet, it will decompress the header, replacing the representative slot number with the complete header information.

Header compression is most useful for interactive traffic, for example, Telnet sessions. Compressing the header information for interactive traffic decreases the delay before data is transferred. In other words, if a key is pressed at a Telnet session, the time required to echo that character back to the user's terminal will be reduced.

To use header compression, configure the number of slots (connections) supported on the site. This number should be slightly above the anticipated number of connections; in the event that more connections are made than expected, additional slots will be available for these connections. To configure IP header compression, see *Header Compression* on page 4-4. To configure IPX header compression, see *Header Compression* on page 4-7.

NOTE: *The LRS uses Van Jacobson TCP compression, discussed in RFC 1144.*

4.6.2 Reducing Cost

4.6.2.1 Inactivity Logouts

The LRS can be configured to log out a particular site after a certain period of inactivity (referred to as **idle time**). To configure an inactivity timeout, the site must be allocated a maximum idle time in seconds using the Define Site Idle command:

Figure 4-27: Setting Site Idle Time

```
Local>> DEFINE SITE irvine IDLE 600
```

The site may then be associated with an **idle time filter list**. When a site receives packets, it compares them to this list. Packets that "pass" the filter list will reset the idle timer to zero. If no packets pass the list or traffic is not received within the idle time, the site will be timed out. (If an idle time filter list is not used, any packet traffic sent by the site will reset the idle timer.)

NOTE: *Incoming packet traffic does not reset the idle timer if there is no idle time filter.*

Idle time filter lists enable the LRS to keep a site active for specific types of traffic, disconnecting the site if this traffic isn't sent. For example, imagine that a particular site was intended for interactive traffic. Using an idle filter list, the site could ensure that other traffic (for example, email) wouldn't keep the connection active.

NOTE: *To configure an idle time filter, see Filter Lists on page 4-1.*

4.6.2.2 Restricting Packets that will Initiate a Connection

To prevent unwanted packets from initiating a connection, each site may be associated with a **startup filter list**. Packets destined for a remote site are compared to this list; if they do not pass the filter, they are discarded.

Startup filter lists are only intended to prevent unwanted connections. If a connection is already in place, the list is ignored. To configure a startup filter, see *Filter Lists* on page 4-1.

4.6.2.3 Reducing the Number of Ports Used

When additional links are brought up to increase bandwidth, phone charges will increase. Reducing the number of ports or reducing the site's maximum bandwidth can reduce total cost; see **Purge Site** on page 13-54 and **Define Site Bandwidth** on page 13-34 for details.

4.6.2.4 Using Higher Speed Modems

The time used to transfer data can be reduced by using the highest speed modems available. To ensure that high speed modems are used before low speed modems, priority numbers may be assigned to each site's ports. If high speed modems are attached to ports with high priority numbers, they will be dialed before other modems.

4.6.2.5 Restricting Connections to Particular Times

Sites can be configured to permit outgoing connections only within particular time ranges on particular days. For example, outgoing connections can be restricted to Monday through Friday, between 9 a.m. and 5 p.m.

4.6.2.5.1 Determining if Site Restrictions are Appropriate

Sites don't necessarily need to be configured to restrict connections; applications can be restricted to run only at particular times. Before configuring a site, it is important to consider whether it's appropriate for a remote application or an LRS site to control the access restriction.

4.6.2.5.2 Setting up Site Restrictions

To configure a time range, use the **Define Site Time Add** command. The time range may be within one day, or may span from one day to another day. (If a second day isn't specified, the time period is assumed to take place entirely on the first day specified). The beginning and end times of the range must be specified in 24-hour format. Some examples are displayed below.

Figure 4-28: Adding Time Ranges

```
Local>> DEFINE SITE irvine TIME ADD MON 8:00 17:00
Local>> DEFINE SITE irvine TIME ADD TUES 23:00 WED 6:00
Local>> DEFINE SITE irvine TIME ADD WED 8:00 THURS 8:00
```

NOTE: *Up to ten time ranges may be specified.*

Next, specify whether connections will be permitted or prevented during these times using the **Define Site Time Default** command. **Enabled** permits outgoing connections, except during the time ranges stated. **Disabled** prevents outgoing connections, except during the time ranges stated.

Figure 4-29: Enabling Connections During Time Range

```
Local>> DEFINE SITE irvine TIME DEFAULT ENABLED
```

Configurable time ranges are based on a Sunday-to-Saturday week. To configure access that spans the weekend hours, see *Controlling Access During Weekend Hours* on page 4-21.

4.6.2.5.3 Getting Timesetting Information

In order to restrict packet traffic during the specified times, the LRS must get accurate time information from one of three sources: an IP timeserver, an IPX timeserver, or from the LRS' internal clock.

To configure an IP timeserver, see **Set/Define IP Timeserver** on page 13-90. To configure an IPX timeserver, see **Set/Define IPX Timeserver** on page 13-95. To set the LRS internal clock, see **Set/Define Server Clock** on page 13-126. To configure the LRS time zone, see **Set/Define Server Timezone** on page 13-136.

To display the site restrictions you've configured, use the **List Site Time** command:

Figure 4-30: Displaying Site Restrictions

```
Local>> LIST SITE irvine TIME
     LRS Version B1.1/102int(951128) Name: DOC_SERVER
     Hardware Addr: 00-80-a3-0b-00-5b uptime: 3 Days 12:07
     20:42:54
     Access default: Enabled

     01) Mon 08:00 - Mon 17:00 Disabled
     02) Tue 23:00 - Wed 06:00 Disabled
     03) Wed 08:00 - Thu 08:00 Disabled

     Success Timeout: 0:01
     Failure Timeout:0:30
```

4.6.2.6 Increasing Requirements for Adding Additional Bandwidth

The LRS will periodically measure how much bandwidth a particular port is using; the period of time during which this measurement is taken may be configured differently for each site. When the measurement period is short, a temporary increase in network traffic may cause the site to bring up additional connections to increase bandwidth, increasing cost. If a site's bandwidth utilization is measured (averaged) over a longer period of time, a temporary increase in network traffic will have less impact on whether or not additional bandwidth is added.

Another way to reduce cost is to increase the percentage utilization required to add additional connections. If a site is permitted to use up to 80% of the total currently-dialed bandwidth on a particular port (rather than, for example, 25%), the site will be less likely to require additional connections to increase bandwidth.

4.6.3 Controlling Frequency of Calls

The success and failure timers can be used to control how aggressive the LRS will be when attempting connections. Two commands control this behavior:

- **Define Site Time Success** sets the time lapse between attempts to connect to a remote site after a successful connection has been made.
- **Define Site Time Failure** sets the time lapse between attempts to connect to a remote site when a connection attempt fails.

If the last connection attempt succeeded and the success timer is set to a high value (for example, 20 minutes), the LRS will wait for a longer period of time before attempting a new connection. If the LRS was not able to connect for some reason, setting the failure timer to a low value (for example, 5 seconds) will cause the LRS to retry the connection at short intervals until it succeeds.

In Figure 4-30, the LRS is configured to allow a new connection attempt almost immediately upon completion of a successful connection. If the last attempt to connect to the site failed, the LRS will wait 30 seconds before attempting another connection. It will continue to retry the connection every 30 seconds until it succeeds.

4.7 Using the LRS Without Dialup Modems

The LRS may be configured to allow Remote Node and LAN to LAN functionality without using modems; dial-on-demand features will be ignored.

4.7.1 Situations Where Dialup Modems Are Not Used

There are four primary situations in which the LRS may be used without modems:

Direct connections	Two LRS units are linked with a serial cable.
Statistical multiplexors	Multiplexors (stat-mux) allow multiple serial lines to run over a single leased line. The stat-mux must support asynchronous serial communication.
Synchronous leased lines	Lines are leased from the telephone company and dedicated to synchronous serial communication between two fixed locations.
Analog leased lines	Analog lines are ordinary telephone lines leased from the telephone company and used in conjunction with standard modems. The modems must have leased line capabilities.

4.7.1.1 Direct Connections

Two buildings may be linked with a serial cable. Two LRS units may use the serial cable to connect two networks together.

4.7.1.2 Statistical Multiplexors

Two locations may have statistical multiplexors (commonly called **stat-muxes**) in place. These stat-muxes may be used to connect two LRS's. Often a series of commands will have to be sent to the stat-mux to connect to the remote LRS; chat scripts make sending these commands easy and relatively error-free.

NOTE: *Chat Scripts are described on page 4-7.*

The LRS assumes an 8-bit data path. If you are using SLIP, all characters must be sent and received unchanged by the intervening communications equipment. PPP has a feature called ACCM which causes the LRS to avoid sending user-specified control characters. If the equipment connecting the LRS cannot send certain control characters, configure PPP and ACCM on the LRS port.

NOTE: *ACCM is discussed in detail in Character Escaping on page 8-1.*

4.7.1.3 Synchronous Leased Lines

The LRS supports asynchronous serial connections. Most leased lines are synchronous. Devices which convert between synchronous and asynchronous serial signals exist, but they may result in some performance loss. The current LRS units are not always the best solution for synchronous leased line applications.

4.7.1.4 Analog Leased Lines

To use an LRS with analog leased lines, the modems on each end of the connection must support leased line mode and should use asynchronous serial communication.

NOTE: *See your modem's documentation to configure the modem for leased line mode.*

4.7.2 Configuration Issues

The LRS should initiate the connection at boot time and should not time out the connection.

The following configuration is recommended:

- Idle timeouts are disabled
- RTS / CTS flow control is used between the LRS and the communications equipment.
- If RTS / CTS flow control is not supported, XON / XOFF flow control may be used in conjunction with PPP. If flow control cannot be used, use PPP and monitor the port for checksum errors which may be the result of disabled flow control.
- The port is dedicated to PPP or SLIP
- PPP or SLIP starts automatically
- The port is configured to support incoming and outgoing connections
- Modem control is disabled

In the following examples (both SLIP and PPP), the LRS has an IP address of 192.0.1.1, and must connect to another router with IP address 192.99.99.99.

4.7.2.1 PPP

Figure 4-31 displays the commands required if PPP is used. Both sides of the leased line should be configured using these commands.

Figure 4-31: LRS Configuration Without Modems: PPP

```
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IP IPADDRESS 192.0.1.1
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 SPEED 19200
Local>> DEFINE PORT 2 FLOW CONTROL CTS
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE SITE port2 IDLE 0
```

If static routing is to be used on the line, routes pointing to the site **port2** will be required:

Figure 4-32: Configuring Static Routing

```
Local>> DEFINE SITE port2 IP RIP DISABLED
Local>> DEFINE SITE port2 IPX RIP DISABLED
Local>> DEFINE SITE port2 IPX SAP DISABLED
Local>> DEFINE SITE IP ROUTE 192.99.99.0 SITE port2 2
Local>> DEFINE IPX ROUTE 12ab SITE port2
```

4.7.2.2 SLIP

Figure 4-33 displays the commands required if SLIP is used. Both sides of the leased line should be configured using these commands.

Figure 4-33: LRS Configuration Without Modems: SLIP

```
Local>> DEFINE IP IPADDRESS 192.0.1.1
Local>> DEFINE PORT 2 ACCESS DYNAMIC
Local>> DEFINE PORT 2 SPEED 19200
Local>> DEFINE PORT 2 FLOW CONTROL CTS
Local>> DEFINE PORT 2 SLIP DEDICATED
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE SITE port2 PROTOCOL SLIP
Local>> DEFINE SITE port2 IDLE 0
Local>> DEFINE SITE port2 IP REMOTEADDRESS 192.99.99.99
```

If static routing is to be used on the line, routes pointing to the site **port2** will be required:

Figure 4-34: Configuring Static Routing

```
Local>> DEFINE SITE port2 IP RIP DISABLED
Local>> DEFINE IP ROUTE 192.99.99.0 SITE port2 2
```

4.8 Monitoring Networking Activity

To monitor current networking activity, use the **Show/Monitor Site** command. This command displays the activity associated with a particular site, including bandwidth utilization, spoofing, chat scripts, port connections, and networking errors.

Show / Monitor Site command is particularly useful when allotting bandwidth to a site. Periodically monitoring a site's use of bandwidth will enable you to determine if the bandwidth configuration is appropriate and to make adjustments when necessary.

Figure 4-35: Displaying Bandwidth Utilization

```
Local>> SHOW SITE irvine BANDWIDTH
```

NOTE: *For information on port and site states, see Table 3-3 on page 3-18.*

4.9 Examples

4.9.1 Creating a Chat Script

Figure 4-36 displays a sample chat script. This script will send a series of text strings to the remote host, and will expect particular strings in return. If an expected string is not received from the remote host, the script will loop up to four times before the entire script fails.

Figure 4-36: Creating a Chat Script

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL
Local>> DEFINE SITE irvine CHAT SEND “”
Local>> DEFINE SITE irvine CHAT EXPECT “login:”
Local>> DEFINE SITE irvine CHAT SEND “user”
Local>> DEFINE SITE irvine CHAT EXPECT “word:”
Local>> DEFINE SITE irvine CHAT SEND “password”
```

4.9.2 Creating a Simple Firewall

Firewalls are used to protect a network or networks from unauthorized access. To set up a firewall, a filter list is used; packet traffic is compared to the filters in the list to determine whether or not it will be forwarded. In general, firewalls prevent all packet traffic, with the exception of traffic to a particular service or services.

In this example, a network policy prevents all IP and IPX traffic, permitting only ICMP ping packets and email. Telnet connections are permitted to only one secure host (192.0.1.4) on the local network.

The LRS is calling site **memphis**. Before the firewall between the LRS and memphis can be configured, IPX must be disabled.

Figure 4-37: Disabling IPX

```
Local>> DEFINE SITE memphis IPX DISABLED
```

Next, a filter list for IP traffic must be created. This list is called **mem**.

Figure 4-38: Creating IP Filter

```
Local>> DEFINE FILTER mem CREATE
Local>> DEFINE FILTER mem ALLOW IP ICMP
Local>> DEFINE FILTER mem ALLOW IP TCP DPORT EQ SMTP
Local>> DEFINE FILTER mem ALLOW IP DST 255.255.255.255 192.0.1.4 TCP DPORT EQ TELNET
Local>> DEFINE FILTER mem ADD DENY ANY
```

Finally, the **mem** filter list must be associated with site memphis as an incoming filter list.

Figure 4-39: Assigning mem Filter List to Site memphis

```
Local>> DEFINE SITE memphis FILTER INCOMING mem
```

NOTE: *For a more complex firewall example, see Creating a Firewall on page 12-31.*

4.9.3 Controlling Access During Weekend Hours

Configurable time ranges are based on a Sunday-to-Saturday week. If you want to allow or restrict access for a time period that spans Saturday and Sunday, you need to use multiple commands.

The following example restricts access during the weekend hours between 5:00 p.m. on Friday and 6:00 a.m. on Monday. Two commands are used to configure the necessary blocks of time: one that spans Friday evening to Saturday just before midnight, and one that spans midnight on Sunday to Monday morning.

Figure 4-40: Disabling Connections During the Weekend

```
Local>> DEFINE SITE irvine TIME ADD FRI 17 SAT 23:59
Local>> DEFINE SITE irvine TIME ADD SUN 0 MON 6
```

NOTE: *In the above example, it is assumed that the access default is "Enabled," in which case connections are restricted during the specified time periods.*

The following example achieves the same result by first adding a time range from Monday morning to Friday evening. The access default is then set to Disabled, which allows connections only during the specified time period.

Figure 4-41: Enabling Connections During Weekdays only

```
Local>> DEFINE SITE irvine TIME ADD MON 6 FRI 17
Local>> DEFINE SITE irvine TIME DEFAULT DISABLED
```

4.10 Quick Reference

Security			
To	**Use This Command**	**Example(s)**	**What Example Does**
Restrict Users to a Particular Configuration	Set / Define Authentication User Command, page 13-72.	`DEFINE AUTHENTICATION USER bob COMMAND set ppp dialin_users`	When user “bob” logs in, PPP is automatically started, and he is attached to site “dialin_users”. See *Authentication* on page 4-1 or *Forcing Execution of Commands* on page 12-19 for more information.
Filter Packet Traffic	1. Set / Define Filter, page 13-74.	`DEFINE FILTER firewall ADD 1 DENY IP SRC 192.0.1.0 255.255.255.0`	Creates a filter list named “firewall”. The “Add” parameter adds one rule to the list; all IP packets originating from host 192.0.1.0 are denied passage through the LRS. See *Filter Lists* on page 4-1 or *Packet Filters and Firewalls* on page 12-22 for more information.
	2. Define Site Filter Idle, page 13-37.	`DEFINE SITE irvine FILTER IDLE firewall`	When an LRS connection using site “irvine” receives packet traffic, it’s compared to filter “firewall”. If the traffic is permitted passage, it resets “irvine’s” idle timer, preventing the site from timing out and disconnecting.
	or Define Site Filter Incoming, page 13-37.	`DEFINE SITE irvine FILTER INCOMING firewall`	When an LRS connection using site “irvine” receives incoming packet traffic, it is compared to filter “firewall”. If the traffic does not pass the filters in “firewall”, it is discarded.
	or Define Site Filter Outgoing, page 13-37.	`DEFINE SITE irvine FILTER OUTGOING firewall`	When an LRS connection using site “irvine” attempts to forward outgoing packet traffic, it is compared to filter “firewall”. If the traffic does not pass the filters in “firewall”, it is discarded.

Security, cont.

To	Use This Command	Example(s)	What Example Does
Filter Packet Traffic, cont.	or Define Site Filter Startup, page 13-37.	`DEFINE SITE irvine FILTER STARTUP firewall`	When the LRS receives packet traffic destined for site “irvine”, it’s compared to filter “firewall”. If the traffic is permitted passage, the LRS will initiate a connection to the remote host using “irvine”.

Prevent all IP / IPX Packet Traffic from Being Forwarded	Define Site Filter IP or IPX, page 13-37.	`DEF FILTER phoenix ADD DENY IP`
		OR
		`DEF FILTER phoenix ADD DENY IPX`
			Prevents IP or IPX packets from being forwarded.

Restrict Incoming Callers to a Particular IP Address or Range of Addresses	See *Remote Networking IP Address Assignment* on page 5-15.		

IP Configuration

To	Use This Command	Example(s)	What Example Does
Assign a Unique IP Address to a Site	Define Site IP Address, page 13-39.	`DEFINE SITE irvine IP ADDRESS 192.0.1.220`	Assigns the IP address 192.0.1.220 to “irvine’s” IP interface. See *Specifying Specific IP Address for a Site* on page 5-16 for more information.
Disable RIP	Define Site IP RIP Disabled, page 13-39.	`DEFINE SITE irvine IP RIP DISABLED`	Disables RIP sending and listening for site “irvine”. See *Disabling RIP* on page 4-3 or *RIP* on page 5-14 for more information.
Adjust the Interval Between RIP Updates	Define Site IP RIP Update, page 13-39.	`DEFINE SITE irvine IP RIP UPDATE 60`	Sets “irvine’s” interval between RIP updates to 60 seconds. See *Interval Between RIP Updates* on page 4-4 or *RIP* on page 5-14 for more information.

IP Configuration, cont.

To	Use This Command	Example(s)	What Example Does
Make a Site a More or Less Desirable Route to Other Destinations	Define Site IP RIP Metric, page 13-39.	`DEFINE SITE irvine IP RIP METRIC 4`	Sets “irvine’s” RIP metric to 4. The higher the metric value, the less desirable the site is as a route to other destinations. See *Configuring the Metric* on page 4-4 or *RIP* on page 5-14 for more information.
Enable or Disable IP Header Compression	Define Site IP Compress, page 13-39.	`DEFINE SITE irvine IP COMPRESS DISABLED`	Disables IP header compression for site “irvine”. See *Header Compression* on page 4-4 for more information.

IPX Configuration

To	Use This Command	Example(s)	What Example Does

Configure RIP or SAP	Define Site IPX RIP / SAP, page 13-41.	`DEFINE SITE irvine IPX RIP SEND`
		
		`DEFINE SITE irvine IPX SAP DISABLED`
			Site “irvine” will forward IPX RIP packets.
			
			Disables IPX SAP on site “irvine”.
			
			See *RIP and SAP* on page 4-5 or *Dynamically Added Entries* on page 6-3 for more information.

Disable “Spoofing” of Keepalive Packets and Responses	Define Site IPX Keepalive Disabled, page 13-41.	`DEFINE SITE irvine IPX KEEPALIVE DISABLED`	Disables keepalive spoofing on site “irvine”. See *Spoofing* on page 4-5 for more information.
Enable or Disable IPX Header Compression	Define Site IPX Compress, page 13-41.	`DEFINE SITE irvine IPX COMPRESS DISABLED`	Disables IPX header compression for site “irvine”. See *Header Compression* on page 4-7 for more information.

Chat Scripts

To	Use This Command	Example(s)	What Example Does
Send a String to the Remote Host	Define Site Chat Send, page 13-35.	`DEFINE SITE irvine CHAT SEND "hello?"`	On outgoing connections, "irvine" will send the string "hello?" to the remote host. See *Creating a Chat Script* on page 4-7 for more information.
Expect a String From the Remote Host	Define Site Chat Expect, page 13-35.	`DEFINE SITE irvine CHAT EXPECT "login:"`	On outgoing connections, "irvine" will expect the string "login:" from the remote host. See *Creating a Chat Script* on page 4-7 for more information.
Configure a Timeout Period in the Script	Define Site Chat Timeout, page 13-35.	`DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT "login:"`	On outgoing connections, "irvine" will wait 2 seconds to receive the string "login:" from the remote host. After 2 seconds, if the string hasn't been received, the next line of the script will be executed. See *Configuring Timeouts* on page 4-8 for more information.

Determine When a Chat Script Will "Give Up"	Define Site Chat Fail, page 13-35.	`DEFINE SITE irvine CHAT TIMEOUT FAIL 4`
		
		`DEFINE SITE irvine CHAT AFTER 1 SEND "hello?"`
		
		`DEFINE SITE irvine CHAT AFTER 2 TIMEOUT 2 EXPECT "login:"`
			In this chat script, "irvine" will send a "hello" string, and wait 2 seconds to receive a "login:" string from the remote host. If the string isn't received within 2 seconds, the script will loop, and the "hello?" string will be sent again.
			
			The script may execute a total of four times. If the "login:" string isn't received on the fourth attempt, the script will fail completely.
			
			See *Setting Markers* on page 4-8 for more information.

Chat Scripts, cont.

To	Use This Command	Example(s)	What Example Does
Add, Replace, or Delete Script Entries	Define Site Chat Replace / Before / After / Delete, page 13-35.	`DEFINE SITE irvine CHAT REPLACE 1 EXPECT "login:"`	Replaces line 1 of the script with "Expect 'login:'".
		`DEFINE SITE irvine AFTER 3 EXPECT "login:"`	Inserts "Expect 'login:'" after line 3 of the script.
			See *Editing and Adding Entries* on page 4-7 for more information.

Configuring LAN to LAN Bandwidth

To	Use This Command	Example(s)	What Example Does
Assign a Priority Number to Each Port	Define Site Port Priority, page 13-43.	`DEFINE SITE irvine PORT 2 PRIORITY 5`	When site "irvine" is used, port 2 will have priority 5. The port with the highest priority number will be used first for outgoing calls; if additional bandwidth is needed, ports will be used in descending priority order.
			See *LAN to LAN Connections* on page 4-9 or *Assigning Port Priority Numbers* on page 4-11 for more information.
Estimate the Bandwidth of Each Port	See *Estimating Each Port's Bandwidth* on page 4-10.		
Specify the Period During Which Bandwidth Will Be Measured	Define Site Bandwidth Period, page 13-34.	`DEFINE SITE irvine BANDWIDTH PERIOD 60`	When site "irvine" is used, the bandwidth usage will be measured during 60-second periods.
			See *LAN to LAN Connections* on page 4-9 or *Specifying the Bandwidth Measurement Period* on page 4-11 for more information.

Configuring LAN to LAN Bandwidth, cont.

To	Use This Command	Example(s)	What Example Does
Configure the Initial / Maximum Bandwidth Allotted to a Site	Define Site Bandwidth Initial / Maximum, page 13-34.	`DEFINE SITE irvine BANDWIDTH MAXIMUM 500`	Sets irvine's maximum bandwidth value to 500 bytes per second. If bandwidth needs to be added during a connection, it may be added until it reaches this value. See *LAN to LAN Connections* on page 4-9 or *Configuring the Maximum Bandwidth Allotted to a Site* on page 4-12 for more information.

Control When Bandwidth is Added or Removed	Define Site Bandwidth Add / Remove, page 13-34.	`DEFINE SITE irvine BANDWIDTH ADD 90`
		
		`DEFINE SITE irvine BANDWIDTH REMOVE 40`
			If "irvine" is using at least 90% of its currently-dialed bandwidth, additional bandwidth will be added. If it's using less than 40% of its currently-dialed bandwidth, bandwidth will be removed.
			
			See *LAN to LAN Connections* on page 4-9 or *Specifying when Bandwidth is Added or Removed* on page 4-11 for more information.

Display a Site's Current Bandwidth Configuration	Show / Monitor / List Sites Bandwidth, page 13-161.	`LIST SITE irvine BANDWIDTH`	Displays irvine's current bandwidth settings. See *LAN to LAN Connections* on page 4-9 or *Monitoring Networking Activity* on page 4-19 for more information.
Restore a Site's Default Bandwidth Settings	Define Site Bandwidth Default, page 13-34.	`DEFINE SITE irvine BANDWIDTH DEFAULT`	Restores the factory default bandwidth settings for site "irvine". See *LAN to LAN Connections* on page 4-9 or *Restoring Default Bandwidth Settings* on page 4-12 for more information.

Improving Performance

To	Use This Command	Example(s)	What Example Does
Filter Unwanted Packet Traffic	See Filtering Unwanted Data on page 4-13.		
Increase Throughput Using Data Compression	Define Ports Modem Compression Enabled, page 13-19.	`DEFINE PORT 2 MODEM COMPRESSION ENABLED`	Enables data compression on port 2. See *Compressing Data and Correcting Errors* on page 4-13 for more information.
Decrease Latency By Disabling Error Correction	Define Ports Modem Errorcorrection Disabled, page 13-22.	`DEFINE PORT 2 MODEM ERRORCORRECTION DISABLED`	Disables automatic error correction on port 2. See *Compressing Data and Correcting Errors* on page 4-13 for more information.
Decrease Latency By Disabling Data Compression	Define Ports Modem Compression Disabled, page 13-19.	`DEFINE PORT 2 MODEM COMPRESSION DISABLED`	Disables data compression on port 2. See *Compressing Data and Correcting Errors* on page 4-13 for more information.
Decrease Latency By Enabling IP/IPX Header Compression	Define Site IP Compress, page 13-39 or Define Site IPX Compress Disabled, page 13-41.	`DEFINE SITE irvine IP COMPRESS DISABLED`	Disables IP header compression on site “irvine”. See *Header Compression* on page 4-13 for more information.
Increase Throughput By Adding Bandwidth	See *Adding Bandwidth* on page 4-13.		

Reducing Cost

To	Use This Command	Example(s)	What Example Does
Configure Site Inactivity Logouts	1. Define Site Idle, page 13-38. 2. See Define Site Filter Idle on page 13-37.	`DEFINE SITE irvine IDLE 600`	Sets a maximum idle time of 600 seconds for site “irvine”. See *Inactivity Logouts* on page 4-14 for more information.
Prevent Unwanted Packets From Initiating a Connection	See Define Site Filter Startup on page 13-37.		
Reduce Phone Rates by Reducing the Number of Ports Used for a Connection	Purge Site Port, page 13-54.	`PURGE SITE IRVINE PORT 3`	Removes port 3 from site “irvine”. When “irvine” makes a connection, port 3 will no longer be used. See *Reducing the Number of Ports Used* on page 4-15 for more information.
Reduce Transfer Time by Using Higher Speed Modems	See *Using Higher Speed Modems* on page 4-15.		
Restrict Connections to Particular Times	1. Define Site Time Add, page 13-46.	`DEFINE SITE irvine TIME ADD MON 8:00 17:00`	Adds a time range; the range is from 8:00 a.m. Monday to 5:00 p.m. Monday. See *Restricting Connections to Particular Times* on page 4-15 for more information.
	2. Define Site Time Default Enabled / Disabled, page 13-46.	`DEFINE SITE irvine TIME DEFAULT ENABLED`	Connections will be permitted during configured time ranges.
		`DEFINE SITE irvine TIME DEFAULT DISABLED`	Connections will be prevented during configured time ranges.
Increase Requirement For Adding Bandwidth	See *Increasing Requirements for Adding Additional Bandwidth* on page 4-16.		

Using the LRS Without Modems

To	Use This Command	Example(s)	What Example Does
Configure the Receiver of the Connection	1. Define Site Idle None, page 13-38.	`DEFINE SITE irvine IDLE NONE`	Disables inactivity timeouts for site irvine. See *Configuration Issues* on page 4-18 for more information.
	2. Define Ports PPP Dedicated, page 13-28. or Define Ports SLIP Dedicated, page 13-31.	`DEFINE PORT 2 PPP DEDICATED`	Dedicates port 2 to PPP.
	3. Define Ports Modem Control Disabled, page 13-20.	`DEFINE PORT 2 MODEM CONTROL DISABLED`	Disables modem control on port 2.
Configure the Initiator of the Connection	1. Define Site Idle None, page 13-38.	`DEFINE SITE irvine IDLE NONE`	Disables inactivity timeouts for site irvine.
	2. Define Ports PPP Dedicated, page 13-28. or Define Ports SLIP Dedicated, page 13-31.	`DEFINE PORT 2 PPP DEDICATED`	Dedicates port 2 to PPP.
	3. Set / Define Ports Autostart Enabled, page 13-106.	`DEFINE PORT 2 AUTOSTART ENABLED`	Configures port 2 to start automatically. Because it's dedicated to PPP, PPP will automatically start.
	4. Set / Define Ports Access Dynamic, page 13-104.	`DEFINE PORT 2 ACCESS DYNAMIC`	Configures port 2 to support incoming and outgoing connections. This is the default.
	5. Define Ports Modem Control Disabled, page 13-20.	`DEFINE PORT 2 MODEM CONTROL DISABLED`	Disables modem control on port 2.
	6. Define Site Port Telephone None, page 13-43.	`DEFINE SITE irvine PORT TELEPHONE NONE`	Clears any currently-defined port telephone number. This is the default.
	7. Define Site Telephone None, page 13-45.	`DEFINE SITE irvine TELEPHONE NONE`	Clears any currently-defined site telephone number. This is the default.

Monitoring Network Activity

To	Use This Command	Example(s)	What Example Does
Display a Site's Current Activity, Including its Use of Bandwidth	Show / Monitor / List Sites, page 13-161.	`SHOW SITE irvine BANDWIDTH`	Displays bandwidth statistics for site "irvine". See *Monitoring Networking Activity* on page 4-19 or *Monitoring Networking Activity* on page 3-17 for more information.

5 IP

5 - IP

This chapter explains some important concepts about IP addressing, configuration, and routing. This information is only necessary for those using the IP protocol.

To configure IP for remote networking, see Chapter 3, *Basic Remote Networking*, and Chapter 4, *Additional Remote Networking*. For specific IP commands, see Chapter 13, *Command Reference*.

5.1 IP Addresses

Each TCP/IP node on a network has a unique IP address. This address provides the information needed to forward packets on the local network and across multiple networks if necessary.

IP addresses are specified as **n.n.n.n**, where each **n** is a number from 0 to 254; for example, 192.0.1.99. The LRS must be assigned a unique IP address to use TCP/IP functionality.

5.1.1 Overview

IP addresses contain three pieces of information: the **network**, the **subnet**, and the **host**.

5.1.1.1 Network Portion

The **network** portion of the IP address is determined by the network type: Class A B, or C.

Table 5-1: Network Portion of IP Address

Network Class	Network Portion of Address
Class A	First byte (2nd, 3rd, and 4th bytes are the host)
Class B	First 2 bytes (3rd and 4th bytes are the host)
Class C	First 3 bytes (4th byte is the host)

In most network examples, the host portion of the address is set to zero.

Table 5-2: Available IP Addresses

Class	Reserved	Available
A	0.0.0.0 127.0.0.0	1.0.0.0 to 126.0.0.0
B	128.0.0.0 191.255.0.0	128.1.0.0 to 191.254.0.0
C	192.0.0.0 223.255.255.0	192.0.1.0 to 223.255.254.0
D, E	224.0.0.0 to 255.255.255.254 255.255.255.255	None

Consider the IP address **36.1.3.4.** This address is a class A address, therefore, the network portion of the address is 36.0.0.0 and the host portion is 1.3.4.

5.1.1.2 Subnet Portion

The subnet portion of the IP address represents which **subnetwork** the address is from. Subnetworks are formed when an IP network is broken down into smaller networks using a **subnet mask**.

NOTE: *Subnetworks and subnet masks are discussed in Subnet Masks on page 5-4.*

A router is required between all networks and all subnetworks. Generally, hosts can send packets directly only to hosts on their own subnetwork. All packets destined for other subnets are sent to a router on the local network.

5.1.1.3 Host Portion

The host portion of the IP address is a unique number assigned to identify the host.

5.1.2 Setting the LRS IP Address

To set the IP address, use one of the following methods: an ARP entry and the Ping command, a BOOTP or RARP reply, or a terminal connected to the serial console port. All methods of setting the address are discussed in the following sections; choose the method that is most convenient for you.

To access the LRS, hosts must know the LRS IP address. This is typically configured in the host's **/etc/hosts** file (UNIX) or via a nameserver. For configuration instructions, refer to the host's documentation.

5.1.2.1 Using an ARP Entry and the Ping Command

If the LRS has no IP address, it will set its address from the first directed IP ICMP (ping) packet it receives. To generate such a packet, create an entry in a UNIX host's ARP table. The entry should specify the intended LRS IP address and its current Ethernet address, which is located on the bottom of the unit.

Figure 5-1: Adding to the ARP Table

```
# arp -s 192.0.1.228 00:80:a3:xx:xx:xx
```

NOTE: *Creating an ARP entry requires superuser privileges on the host.*

Ping the server using the following command:

Figure 5-2: Ping Command

```
unix% ping 192.0.1.228
```

When the server receives the ping packet, it will notice that its own IP address is not currently set and will send out broadcasts to see if anyone else is using this address. If no duplicates are found, the server will use this IP address and will respond to the ping packet. The LRS will **not** save this learned IP address permanently. It is intended as a temporary measure to enable EZCon to communicate with the server or allow an administrator to Telnet to the LRS **remote console port** (port 7000).

NOTE: *The remote console port is discussed in Remote Console Connections on page 5-9.*

To make the IP address permanent, use the **Define IP Address** command.This command requires privileged status.

Figure 5-3: Telnetting to Console Port

```
% telnet xxx.xxx.xxx.xxx 7000
Trying xxx.xxx.xxx.xxx
Connected to xxx.xxx.xxx.xxx
Escape character is '^]'
# access (not echoed)

Lantronix LRS16 Version n.n/n (yymmddd)
Type Help at the 'Local>' prompt for assistance.

Enter Username> bob
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> DEFINE IP ADDRESS 192.0.1.99
```

5.1.2.2 Using a BOOTP or RARP Reply

The LRS's IP address can be configured when the unit boots using information supplied by a host-based RARP or BOOTP server. For configuration information, see the host-based man pages.

Many BOOTP daemons will not reply to a BOOTP request if the download filename in the configuration file does not exist. To get the BOOTP daemon to respond, create a file with the same pathname specified in the configuration file.

5.1.2.3 From the Serial Console Port

To define the IP address from the serial console port, connect a terminal to the LRS and press the Return key.

If the LRS is booting when you press the Return key, a Boot> prompt appears. This prompt enables you to enter a special set of commands, the **Boot Configuration Program** (BCP) commands. To configure the IP address at this prompt, enter the following command:

Figure 5-4: Configuring IP Address Using BCP

```
Boot> SET SERVER IPADDRESS 192.0.1.221
```

NOTE: *For more information on Boot Configuration Program commands, refer to Appendix B of your Installation Guide.*

If the LRS is running when you press the Return key, a Local_1> prompt will be displayed. The **1** represents port 1, the serial console port. To set the IP address at this prompt, you will need to become the privileged user by issuing the following commands:

Figure 5-5: Becoming Privileged User

```
Local_1> SET PRIVILEGED
Password> system (not echoed)
```

Once you've obtained privileged access, use the **Set/Define IP Address** command:

Figure 5-6: Set / Define IP Address

```
Local_1>> DEFINE IP ADDRESS 192.0.1.221
```

5.2 Subnet Masks

IP networks can be divided into several smaller networks by subnetting. When a network is subnetted, some of the host portion of each address is given to the network portion of the address. The amount is governed by the **subnet mask**. All hosts must agree on the subnet mask for a given network.

For example, IP address **128.1.150.35** is on a class B network. The network portion of this address is **128.1**. This large network can be broken down into 254 networks using a subnet mask of **255.255.255.0**, which makes the network portion **128.1.150**.

It is not always necessary to divide a network into subnetworks. To determine whether subnetting is required, a number of factors should be considered, including the network size and whether or not network traffic needs to be isolated in a particular area.

When the IP address is configured, a default subnet mask will be created. The default subnet mask depends on the class of the LRS IP address; for example, if you assigned the LRS a class B IP address, the default subnet mask will be 255.255.0.0.

If your network is divided into subnetworks, you will need to create a custom subnet mask; the default subnet mask will not be correct for your network. To override the default subnet mask, use the **Set/Define IP Subnet Mask** command.

Figure 5-7: Setting Subnet Mask

```
Local>> DEFINE IP SUBNET MASK 255.255.0.0
```

It is also possible to learn a subnet mask from BOOTP, though not all BOOTP server implementations support sending subnet masks. Check your BOOTP server's documentation.

To display the subnet mask, use the **Show IP** command:

Figure 5-8: Show IP Output

```
Local>> SHOW IP
LRS16 Version B1.1/102int(951128)       Name:              DOC_SERVER
      Hardware Addr: 00-80-a3-0b-00-5b  Uptime:            1 Day      22:49
      IP Address: 192.0.1.221           Subnet Mask:       255.255.255.0
```

The LRS will not change the subnet mask once it is set. If the LRS IP address is changed to a different class, for example, from a class B to a class C address, the subnet mask will remain a class B address.

The LRS supports CIDR (classless routing). CIDR allows Internet Service Providers (ISPs) to group blocks of class C networks into larger networks. Your ISP will provide you with the appropriate subnet mask. If you enter a CIDR subnet mask with the Set / Define IP Subnet Mask command, the LRS will display a reminder that classless routing is being used.

Figure 5-9: Using Classless Routing

```
Local>> DEFINE IP ADDRESS 192.0.1.1
Local>> DEFINE IP SUBNET 255.255.240.0
%Info: Supernet (CIDR) mask set.
```

5.3 Name Resolving

TCP / IP hosts generally have an alphanumeric host name, such as **athena**, as well as a numeric IP address, such as **192.0.1.35**. As a text host name may be easier to remember than an IP address, users may use this name to refer to the host during a Telnet connection attempt.

Network hosts do not understand alphanumeric (text) host names. When a text name is used, the LRS must translate it into its corresponding IP address. This translation process is called **name resolution**.

To resolve a name, the LRS can use one of two resources: its local name table, or the **Domain Name Service (DNS)**. For example, suppose user Bob wishes to Telnet to **athena.com**. The LRS will consult its local host table; if the name doesn't exist, the LRS will attempt to resolve the name using the DNS. If the name cannot be resolved, the IP address must be entered in order to access the host.

Some host names and IP addresses are added to the local host table by **rwho** packets, periodically broadcasted by UNIX hosts that support the rwho protocol. If addresses are not learned from rwho packets and DNS is not available, hosts may be manually added to the table. See page 5-6 for instructions.

To use the DNS, the LRS must know the IP address of the DNS server, called the **Domain Name Server**. See the following page for configuration instructions.

5.3.1 Configuring the Domain Name Service (DNS)

To use the DNS for name resolution, use the **Set/Define IP Nameserver** command:

Figure 5-10: Setting Domain Name Server

```
Local>> DEFINE IP NAMESERVER 192.0.1.166
```

To specify a backup nameserver, use the Set / Define IP Secondary Nameserver command. If the first nameserver isn't available, requests will be sent to the secondary server.

5.3.2 Specifying a Default Domain Name

A default domain name may be configured using the **Set/Define IP Domain** command. This domain name will be automatically appended to any host name during name resolution.

Figure 5-11: Configuring Default Domain Name

```
Local>> DEFINE IP DOMAIN ctcorp.com
```

In the example above, the default domain name is **ctcorp.com**. If user Bob typed **telnet athena**, the LRS would automatically append the domain suffix and attempt to resolve **athena.ctcorp.com**.

If a host name is entered that ends with a period (“.”) the LRS will not add the domain suffix to the hostname for resolution.

5.3.3 Adding Hosts to the LRS Host Table

If the DNS is not available on your network, hosts may be manually entered in the local host table using the **Set/Define Hosts** command.

Figure 5-12: Adding Host to Local Host Table

```
Local>> DEFINE HOST athena 192.0.1.15
```

To display the current entries in the host table, use the **Show Hosts** command.

Figure 5-13: Displaying Host Table Entries

```
Local>> SHOW HOSTS
IP Address              Host          TTL
192.0.1.15              ATHENA        8 min (Rwho)
192.0.1.123             MERCURY       8 min (Rwho)
```

To remove an entry from the host table, use the **Clear/Purge Host** command.

Figure 5-14: Deleting a Host From the Host Table

```
Local>> PURGE HOST mercury
```

5.4 Sessions

When you log into an LRS port to connect to a network service, your connection is referred to as a **session**. A network service may be an interactive login to a TCP / IP host, a connection to a modem on the LRS, another server, etc.

NOTE: *The word "sessions" in this manual is used to describe interactive connections; PPP or SLIP connections are not referred to as sessions.*

The following section explains how to establish sessions and set up connection characteristics. Specific port configuration and other session characteristics are discussed in Chapter 9, Ports.

To display the current sessions, use the **Show Sessions** command. The port number and username will be displayed, along with the connection type and current number of sessions.

Figure 5-15: Displaying the Current Sessions

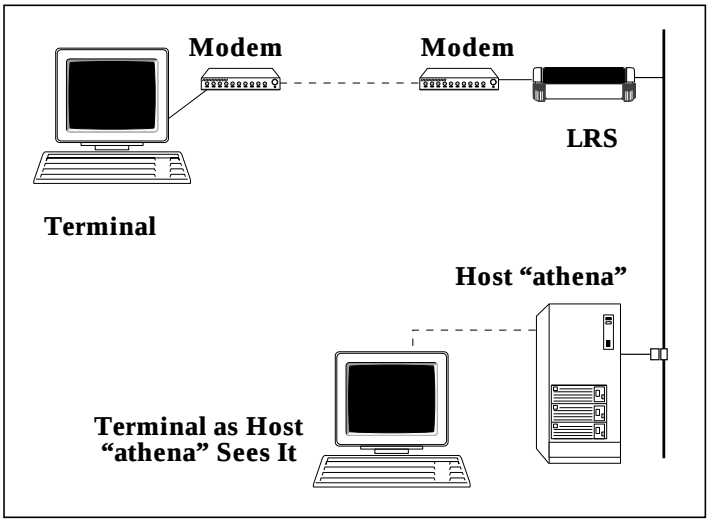
```
Local>> SHOW SESSIONS
Port 17:   bob          Telnet Login     Current: 2
           Session 1    Telnet:ATHENA    Interactive  (Cr,Del)
           Session 2    Telnet:HERCULES  Interactive  (Cr,Del)
```

5.4.1 Establishing Sessions

5.4.1.1 Telnet and Rlogin

Telnet is an industry-standard network protocol that enables users anywhere on a network to access a remote host and start a terminal session. Telnet connections do not require that either end of the connection know the hardware / software used on the other end; for example, if user **Bob** connects to host **athena** (see Figure 5-16), athena doesn't know what terminal type Bob is using, and Bob doesn't know athena's platform or operating system.

Figure 5-16: Telnet Connections



Rlogin connections are similar to Telnet connections, however, Rlogin enables trusted users to log into a host without password verification.

5.4.1.1.1 Outgoing Telnet/Rlogin Connections

To establish an outgoing Telnet connection, use the **Telnet** command. To establish an outgoing Rlogin connection, use the **Rlogin** command. A text host name or an IP address may be specified.

Figure 5-17: Outgoing Telnet / Rlogin Connections

```
Local>> TELNET athena
Local>> TELNET 192.0.1.15
Local>> RLOGIN 192.0.1.15
```

NOTE: *For information on resolving host names, see Name Resolving on page 5-5.*

By default, Telnet and Rlogin connections will be made to a preset port number. To connect to a different port number, use the Telnet / Rlogin commands in conjunction with a port number (prefaced by a colon).

Figure 5-18: Telnetting to a Specific Port Number

```
Local>> TELNET athena:145
```

If the LRS port used has been configured with a terminal type (for example, VT100), this information will be sent to the remote host during the session. To configure the terminal type, use the Set / **Set/Define Ports TermType** command:

Figure 5-19: Setting Term Type

```
Local>> DEFINE PORT 2 TERMTYPE VT100
```

Rlogin can be a security problem. When an outgoing Rlogin connection is attempted, the LRS will send the username specified when the user logged into the LRS. If a user is not authenticated during the LRS login process, an unauthorized username may be used to Rlogin to remote hosts. The easiest way to avoid this problem is to disable outgoing Rlogin connections:

Figure 5-20: Disabling Outgoing Rlogin Connections

```
Local>> DEFINE SERVER RLOGIN DISABLED
```

Another way to secure your network is to ensure that the LRS is not a trusted host on any UNIX hosts on the network. This solution is not foolproof, however, a user could still add the LRS to a UNIX hosts's **.rhost** file.

5.4.1.1.2 Incoming Telnet/Rlogin Connections

By default, the LRS will permit incoming Telnet and Rlogin connections. If this poses a security problem on your network, these connections can be disabled, restricted with a password requirement, or restricted using the IP security table.

To disable incoming Telnet / Rlogin connections, use the **Set/Define Server Incoming** command:

Figure 5-21: Disabling Incoming Telnet / Rlogin Connections

```
Local>> DEFINE SERVER INCOMING NONE
```

To require the login password for incoming Telnet / Rlogin connections, use this command:

Figure 5-22: Requiring the Login Password

```
Local>> DEFINE SERVER INCOMING PASSWORD
```

To restrict incoming Telnet and Rlogin connections using the IP security table, see *IP Security* on page 5-10.

5.4.1.2 Remote Console Connections

The remote console port, designated as **port 7000**, provides users with a "failsafe" way to log into the LRS. Remote console logins cannot be disabled, therefore, if incoming logins are disabled, a remote console login will be the only way to remotely access the LRS.

The remote console prompt cannot be changed, even with the **Set/Define Server Prompt** command. If your configuration requires that a script be used to communicate with the LRS, the script can depend on receiving the same prompt from the LRS each time that it runs.

EZCon uses the remote console port to configure the LRS. To display the remote console prompt within EZCon, see the EZCon online help.

5.4.1.2.1 Logging Into the Remote Console Port

To Telnet to the remote console port, use the **Telnet** command. Specify the IP address of the LRS followed by the remote console port number.

Figure 5-23: Telnetting to Remote Console Port

```
% telnet xxx.xxx.xxx.xxx 7000
Trying xxx.xxx.xxx.xxx
Connected to xxx.xxx.xxx.xxx
Escape character is '^'
#
```

At the **#** prompt, type the login password. The default login password is **access**.

NOTE: *To change this password, see Set/Define Server Login Password on page 13-129.*

Figure 5-24: Entering Login Password

```
# access (not echoed)
Version n.n/n(yymmdd)
Type HELP at the 'Local>' prompt for assistance.
Enter username> bob
```

5.4.1.2.2 Configuring the Remote Console Port

Remote console connections are associated with a virtual (rather than physical) port. For virtual port configuration instructions, see *Virtual Ports* on page 9-17.

The remote console port cannot be associated with preferred or dedicated services or protocols. To ensure that the remote console port is always accessible, it cannot be restricted using IP security or username / password authentication.

5.5 IP Security

IP security allows an administrator to restrict incoming and outgoing TCP / IP sessions, access to ports, and print jobs. Connections are allowed or denied based upon the source IP address for incoming connections and print jobs and the destination IP address for outgoing connections.

IP security for connections can be set to Incoming Enabled / Disabled, Outgoing Enabled / Disabled, or Both. Incoming refers to users on other hosts attempting to log into the LRS. Outgoing refers to local users connecting to other TCP / IP hosts. The Both parameter enables or disables both Incoming and Outgoing connections. IP security for printing can be set to Enabled or Disabled. The printing setting affects both LPR and RTEL print jobs from the specified hosts.

NOTE: *By default, there aren't any IP security restrictions.*

IP security will not affect the remote console port. To secure the remote console port, ensure that the login password has been changed from the default login password (see Set / Define Server Login Password, page 13-129).

5.5.1 Configuring the Security Table

To add an entry to the table, specify an IP address, a list of affected ports, and what type of restriction is desired. The IP address must be four segments of 0-255 each; for example, the address **131.67** is not valid. Figure 5-25 displays two example entries:

Figure 5-25: Setting Server Access

```
Local>> DEFINE IP SECURITY 192.0.1.255 OUTGOING DISABLED PORT 3
Local>> DEFINE IP SECURITY 192.0.5.255 PRINTING DISABLED
```

NOTE: *Set is valid wherever Define is shown in Figure 5-25 and Figure 5-26.*

The first command affects addresses from 192.0.1.1 through 192.0.1.254 using the 255 "wildcard" network address segment. It prevents port 3 from beginning sessions to hosts with these addresses. The second command addresses from 192.0.5.1 through 192.0.5.254 using the wildcard segment. It prevents nodes in that range from sending print jobs to the server.

A 255 in any segment applies to all numbers in that range— 192.0.1.255 includes 192.0.1.1, 192.0.1.2, and so on. A trailing zero in any address segment is shorthand for "all addresses in this range, both incoming and outgoing disabled, for all ports." For example, the following two commands are equal:

Figure 5-26: Set IP Security Command

```
Local>> DEFINE IP SECURITY 192.0.1.0
Local>> DEFINE IP SECURITY 192.0.1.255 OUTGOING DISABLED INCOMING DISABLED
```

Finally, port zero corresponds to the virtual ports (that is, users who log into the server from the network). If no ports are specified on the command line, the command will affect all local and virtual ports.

NOTE: *For a description of virtual ports, see Virtual Ports on page 9-17.*

5.5.1.1 Clearing Table Entries

Individual entries can be cleared by doing a Clear (or Purge) IP Security with no parameters other than the address:

Figure 5-27: Clear IP Security Command

```
Local>> CLEAR IP SECURITY 192.0.1.102
```

The entire security table can be cleared with the following command:

Figure 5-28: Clearing Security Table

```
Local>> CLEAR IP SECURITY ALL
```

5.5.2 Using the Security Table

Applying the entries in the table may look confusing at first, but the process is rather straightforward. There are two basic rules for checking a TCP / IP connection for legality. First, a more specific rule takes precedence over a less specific one. For example, if connections to 192.0.1.255 are disabled but connections to 192.0.1.78 are enabled, a connection to 192.0.1.78 will succeed. Second, in the absence of any rule that applies to a connection, access is allowed. If this is not desired, include an entry of the following form:

Figure 5-29: Using the IP Security Table

```
Local>> SET IP SECURITY 255.255.255.255 INCOMING DISABLED OUTGOING DISABLED
```

This is the least specific rule in the table, and will ensure that connections fail unless otherwise allowed by another entry (recall that all ports are included in the rule by default).

If no entries are defined in the table, all connection attempts will succeed. Also, if the user making the connection is the privileged user (see the Set Privileged command), the connection will be allowed regardless of the entries in the table.

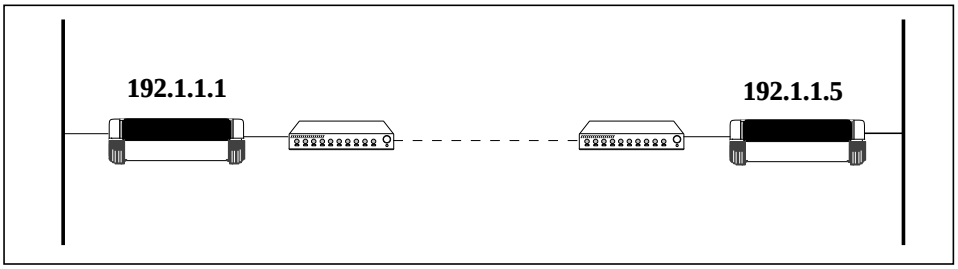
5.6 IP Routing

TCP / IP internets are usually broken down into **networks**. Each host on a particular network can only see hosts on its network; to transfer network traffic to other networks, **routers** (also called **gateways**) are required. Routers are typically connected to two or more networks.

The LRS serves as a router for the networks that it is directly connected to. To determine the path to other routers on the network, the LRS will listen to network broadcast packets (for example, RIP packets); routers will advertise themselves in these packets.

The LRS must be positioned between two networks in order for routing to work correctly. If two or more LRSs are used, the units cannot be on the same network (as in Figure 5-30).

Figure 5-30: Two LRSs Used to Link the Same Network



5.6.1 How Packets are Routed

When an IP host tries to send a packet, it looks to see if the destination address is on the same network as the host's IP address. If it is, the host sends the packet directly to its destination. If the packet is destined for a different network, the host sends it to a router (in this case, the LRS).

When the LRS receives the packet, it examines the packet's destination address, determines the most efficient route to this address, and forwards the packet to this location. The "most efficient route" is determined using two factors: the network that the address is part of and the LRS routing table (see *Routing Tables*, below).

5.6.2 Routing Tables

The LRS uses a routing table to keep track of which networks are reachable, and the shortest route to each network. A typical routing table entry consists of the destination network, and which router is the best path to that network. Routing tables also keep track of the **cost** or **metric** required to get to a given network.

5.6.2.1 Types of Routes

There are three types of routes: host, network, and default.

5.6.2.1.1 Host Routes

A Host Route is a route to a single host. Generally a host route is entered for each Remote Node that logs into the LRS.

5.6.2.1.2 Network Routes

A network route is a route to another network. A network route is used if a host route to the destination doesn't exist.

5.6.2.1.3 Default Routes

A default route is used if a more specific host or network route isn't available. It is used to cut down on the size of routing tables and dynamic routing protocol updates. If, for example, the LRS is the only path for network packets to reach a much larger group of networks, the LRS can be configured to advertise itself as the default route.

NOTE: *See Set/Define IP Route Default on page 13-87 and Define Site IP Default on page 13-39.*

An LRS in a small sales office might have a default route that points to the corporate headquarters. The LRS doesn't need to know about all of the routes on the headquarters network. It only knows to send all otherwise unspecified traffic to the central location, where it will be routed to the final destination.

5.6.2.2 How Routes are Added to the Table

Entries may be added to the routing table in three ways: locally, statically, or dynamically.

5.6.2.2.1 Locally

When a route is added locally, it is automatically determined from the LRS IP address and network mask. The LRS always keeps a local route to the Ethernet that it is attached to; this route is never deleted.

5.6.2.2.2 Statically

Statically-entered routes are entered and removed by the administrator. These routes are used when dynamic routes cannot be.

To add a static route to the routing table, use the **Set/Define IP Route** command. A destination and a path to that destination must be specified. The destination may be an IP network, subnetwork, or host.

The path may be another router on the Ethernet or a site. To specify that the route is to another router, use the **Nextrouter** parameter. To specify that the route is to a site, use the **Site** parameter. The Site parameter indicates that a particular site should be started to forward the packet. The site will handle any remote connections necessary to forward the packet (for example, dialing another LAN).

A **metric** will be associated with the route to indicate its "cost". The LRS will use the route to determine the most efficient route; routes with a lower cost will be chosen over routes with a higher cost. If a metric is not specified, the LRS will assign a metric of 1 to the route.

Figure 5-31: Adding Static Routes

```
Local>> DEFINE IP ROUTE 192.5.4.0 NEXTROUTER 192.0.1.1 4
Local>> DEFINE IP ROUTE 192.5.3.0 SITE dallas
```

In the above example, the first command specifies that the route to network 192.5.4.0 is through another router, 192.0.1.1. The route was assigned a metric of 4.

The second command specifies that the route to network 192.5.3.0 is through site dallas. As a metric is not specified, the LRS will assign this route a metric of 1. When LRS receives traffic destined for network 192.5.3.0, if this route is determined to be the most efficient route, site dallas will be started and will forward the packet.

To enter a static default route, use the **Set/Define IP Route Default** command:

Figure 5-32: Adding Default Routes

```
Local>> DEFINE IP ROUTE 192.0.1.0 DEFAULT SITE internet
Local>> DEFINE IP ROUTE 192.0.2.0 DEFAULT NEXTROUTER 192.0.1.1 2
```

5.6.2.2.3 Dynamically

These routes are automatically learned from other routers on the network, and are managed by a dynamic routing protocol. The LRS currently supports one dynamic routing protocol, RIP. Routes are automatically entered when new networks come on line, and automatically removed if the networks are no longer reachable.

Dynamic routes learned via sites are the exception; they are never timed out. The LRS assumes that these networks are reachable by bringing up a link. This allows the LRS to learn about extended networks at the remote site without the administrator's intervention.

5.6.3 RIP

RIP (Routing Information Protocol) is the dynamic routing protocol supported by the LRS.

NOTE: *RIP is described in RFC-1058.*

NOTE: *Throughout this manual the term "RIP" refers to RIP version 1; therefore, the LRS does not support discontiguous subnets or VLSM.*

5.6.3.1 Configuring RIP

RIP is automatically enabled on all LRS interfaces (including sites). For a complete discussion of RIP options, including disabling RIP, see *RIP* on page 4-3.

5.6.3.2 Trusted Routers

Normally RIP listens to routing table updates from any source. This can lead to problems if a misconfigured host accidentally begins sending incorrect information via RIP. It may also lead to security or denial of service attacks by a malicious user who is capable of sending false RIP messages.

The LRS can be configured to listen only to RIP updates from a list of trusted IP addresses. A sophisticated attacker could still send RIP updates as one of the trusted addresses and potentially defeat the system. See **Set/Define IP Trusted** on page 13-90 for details.

5.6.4 Proxy ARP

Proxy ARPing enables the LRS to respond to ARP requests for other addresses. When Proxy ARPing is enabled, the LRS will respond to ARP requests for all addresses in its routing table.

Proxy ARPing allows remote nodes to appear as if they were on the same Ethernet segment as the LRS. This feature is particularly useful for hosts that do not support RIP; the Ethernet hosts will not need to use routing information to forward traffic destined for these hosts.

To enable proxy ARP, use the **Set/Define IP All/Ethernet Proxy-ARP** command:

Figure 5-33: Enabling Proxy ARP

```
Local>> DEFINE IP ETHERNET PROXY-ARP ENABLED
```

The LRS will not respond to ARP requests for routes learned from the Ethernet, or for routes that aren't explicitly listed in the LRS routing table.

5.6.5 Remote Networking IP Address Assignment

By default, all sites use “unnumbered” IP interfaces. The IP address of the LRS’s Ethernet will be used as the LRS’s IP address on all serial ports. This reduces the amount of required configuration, in addition, it eliminates the need to allocate a separate IP network for each port.

NOTE: *For an example of IP address assignment setup, see IP Address Assignment for Remote Networking on page 5-21.*

5.6.5.1 Incoming Connections

When the LRS receives an incoming connection request (remote node or LAN to LAN), an IP address is negotiated for the caller. The address agreed upon depends on the caller’s requirements; some don’t have a specific address requirement, while others must use the same IP address each time they log into the LRS.

NOTE: *PPP negotiation is covered in Chapter 8, PPP.*

If an incoming caller does not require the same address for each login, a dynamic address can be assigned from an **address pool**. See *IP Address Pools* on page 5-15 for configuration instructions.

Some remote nodes or remote routers cannot be dynamically assigned an IP address. For example, a remote node may offer a service to other hosts on its network. If the other hosts are statically configured to use that IP address to contact the remote node, the node’s IP address must not change.

In this situation, two courses of action may be taken: the caller may be permitted to choose any address, or may be restricted to a specific address or range of addresses.

Permitting the caller to choose an address presents a number of risks. If the caller chooses an unacceptable IP address (for example, the address of a server), it could affect the accuracy of routing tables elsewhere on the network. In addition, the caller could choose an IP address intended for another host, compromising network security.

To avoid routing and security problems, the LRS should restrict incoming callers to a particular address or range of addresses. This restriction may be defined in each site to force each caller to use a unique IP address; see *Specifying IP Address Range for a Site* on page 5-16 for configuration instructions.

5.6.5.1.1 IP Address Pools

An address pool is a range of IP addresses that have been reserved for allocation to incoming callers. The range is defined for the entire server; in other words, an address pool cannot be defined for each site.

To define an address pool, use the **Set/Define IP Ethernet Pool** command. The beginning and end of the address range must be specified.

Figure 5-34: Defining IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

NOTE: ***Set/Define IP All Pool*** *is not a valid command. The Ethernet parameter must be used.*

Ensure that the address pool is at least as large as the number of serial ports that can accept incoming connections. If all addresses in the pool are in use, incoming callers will not be assigned an IP address.

The LRS will automatically add host routes to the routing table for all addresses in the pool. When an address from the pool is assigned to an incoming caller, the route to the address will be announced in RIP broadcasts.

Addresses in the pool are automatically added to the LRS ARP table. If proxy ARPing is enabled (see *Proxy ARP* on page 5-14), the LRS will respond to ARP requests for these addresses, even when they aren't currently assigned. This enables the LRS to defend the addresses in the pool; other hosts will not be able to use them.

5.6.5.1.2 Specifying IP Address Range for a Site

Each site may specify a particular range of acceptable IP addresses. When an incoming caller requests to use a specific address, it will be compared to this range. If the address falls within this range, the connection will be permitted, if not, the connection attempt will fail.

To specify the beginning and end of the range, use the **Define Site IP Remoteaddress** command. Two addresses must be specified: the beginning of the range, and the end of the range.

Figure 5-35: Specifying Range of Addresses

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.250
```

Callers will not be permitted to use IP addresses with the host part of the address set to zero or -1. These addresses are reserved to identify broadcast packets. If the range that you specify includes such an address (for example, 192.4.5.0 or 192.4.5.255) and a caller requests this address, the connection will not be permitted.

RADIUS can also be used to set the IP address range for a site. See *Framed-IP-Address* on page E-3 for more information.

5.6.5.1.3 Specifying Specific IP Address for a Site

To require that incoming callers to a particular site use a specific IP address, use the **Define Site IP Remoteaddress** command. Specify only one address. (If two addresses were specified, a range would be defined.)

Figure 5-36: Specifying Specific IP Address

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108
```

When an incoming caller requests an IP address, it will be compared to this address. If there's a match, the caller will use the address. If the addresses do not match, the LRS will terminate the call (hang up).

5.6.5.2 Outgoing Connections

By default, when a new site is defined, the LRS IP address on that interface will be the IP address defined with the **Define Site IP Address** command.

Communication with a particular remote host may require that the LRS have a certain IP address on that interface. For example, a remote host may require that RIP updates be received from a particular IP address, or an address within a certain range. In these cases, a site-specific IP address

may be configured for a particular interface. For example, site **irvine** may configure the LRS IP address on its interface as 193.20.339.2, and site **dallas** may configure the LRS address on its interface as 193.20.338.0.

NOTE: *The LRS cannot be assigned an IP address by the remote host.*

To change the IP address for a particular site's interface, use the **Define Site IP Address** command:

Figure 5-37: Defining IP Address For Site

```
Local>> DEFINE SITE irvine IP ADDRESS 192.0.1.220
```

5.6.5.3 SLIP

SLIP does not support negotiation of IP addresses. If a SLIP user requires the same IP address for each login, the user may enter the address using the **Set SLIP** command.

Figure 5-38: Specifying IP Address with Set SLIP Command

```
Local>> SET SLIP irvine 192.0.1.35
```

If the port receiving the incoming call is dedicated to SLIP, a specific IP address may be assigned via a custom site. To define the address for the site, use the **Define Site IP Remoteaddress** command.

Figure 5-39: Specifying IP Address for a Custom Site

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108
```

If the user does not require the same address for each login, an address may be dynamically assigned from the address pool. To configure the range of addresses in the pool, use the **Set/Define IP Ethernet Pool** command. The beginning and end of the address range must be specified.

Figure 5-40: Defining IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

All incoming SLIP users that do not use a custom site will use the default site for the connection. To require that default site users use an IP address from the pool, use the **Define Site Default IP Remoteaddress** command:

Figure 5-41: Using the Address Pool for the Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.100 192.0.1.105
```

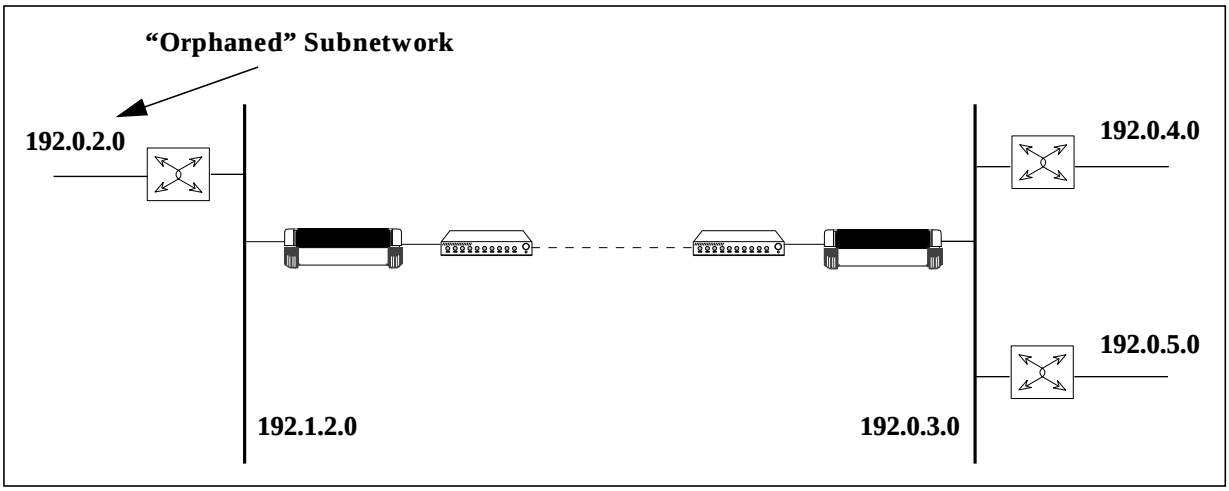
5.6.6 Routing Implementations Not Supported by the LRS

5.6.6.1 Discontinuous Subnetworks

When dividing a network into subnetworks, ensure that subnetworks are contiguous. The LRS uses RIP to learn routing information; if subnetworks are not contiguous, RIP cannot correctly inform the LRS of the route to a particular network.

Figure 5-42 gives an example of discontinuous subnetworks.

Figure 5-42: Discontinuous Subnetworks



5.6.6.2 Variable Length Subnet Masks

Variable length subnet masks divide networks into subnetworks of different sizes. For example, if network 128.1.0.0 used variable length subnet masks, the subnet 128.1.4.0 might have subnet mask 255.255.255.0, and subnet 128.1.224.0 might have subnet mask 255.255.255.240.

When the LRS is used, each network may have a subnet mask of a different length, however, all subnetworks within a particular network must use the same subnet mask.

5.6.7 Using the NetBIOS Nameserver (NBNS)

Windows 95 users can run NetBIOS over IP and use the DNS for name resolution, or a primary or secondary NetBIOS nameserver (NBNS).

To specify a NetBIOS nameserver, use the following command. A secondary NetBIOS nameserver can be configured if desired.

Figure 5-43: Setting Domain Name Server

```
Local>> DEFINE IP NBNS 192.0.1.178
```

NBNS will allow Windows 95 clients to use the Network Neighborhood browser without any additional configuration on the Windows 95 host.

NOTE: *NBNS is also called WINS.*

5.7 Displaying the IP Configuration

The Show IP commands display IP configuration information, including information about the IP router, IP interfaces, and IP address of the remote host. To display the basic IP router configuration, use the **Show IP** command without any additional parameters.

Figure 5-44: Show IP Output

```
Local>> SHOW IP
       LRS Version B1.1/102int(951128)         Name:                      DOC_SERVER
       Hardware Addr: 00-80-a3-0b-00-5b        Uptime:                    3 Days 02:07

       IP Address:       192.0.1.53            Subnet Mask:               255.255.255.0
       Nameserver:       (undefined)           Backup Nameserver:         (undefined)
       Domain Name:      (undefined)           Host Limit:                200
       Timeserver:       (undefined)           Backup Timeserver:         (undefined)
       IP Routing:       Enabled

                         Received     Sent     Seconds since zeroed:      270144
IP     Frames:           431535       13520    Errors:                    0
       Fragments:        0            0
TCP    Frames:           4616         4046     Connect Failure Reasons:   0000
       Invalid Frames:   1            0        Invalid Packet Reasons:    0030
       Retransmissions:               0

ICMP   Frames:           5            3        ICMP Reasons:              0045
```

The **Show IP Interface** command displays a one-line summary for each interface that the router has. There will always be an interface for the Ethernet, as displayed in Figure 5-45. When sites are active, interfaces to these sites will be displayed.

The *Uptime* field displays how long (in days:hours:minutes format) each interface has been active. The *Lastin* field displays the duration since the last packet arrived on a particular interface. The *Lastout* field displays the duration since the interface sent outgoing traffic.

Figure 5-45: Show IP Interface Output

```
Local>> SHOW IP INTERFACE
   LRS16 Version B1.1/102int(951128)          Name:                DOC_SERVER
   Hardware Addr: 00-80-a3-0b-00-5b           Uptime:              3 Days 02:07
Name         IP Address    Remote IP Address    Uptime     Lastin     Lastout
Ethernet     192.0.1.221                        74:07:04   0:00       0:00
```

When used in conjunction with a particular site name, the **Show IP Interface** command displays information about the site's interface, including its IP address, subnet mask, IP address of the remote host, and RIP statistics.

Figure 5-46: Show IP Interface for a Particular Site

```
Local>> SHOW IP INTERFACE irvine
  LRS16 Version B1.1/102int(951128)     Name:                          DOC_SERVER
  Hardware Addr: 00-80-a3-0b-00-5b      Uptime:                  3 Days 02:07
                                                                       20:42:54
  Name                             bob         Type:                      Dialup
  Netstate:                    Running         Device/Refcount:          lm0:/002
  IP Address:              192.0.1.221         Remote Address:       192.0.1.245
  Netmask:                 255.255.255.        Network:                192.0.1.0
                                      0
  TimeToLive Cost:                   0         Largest Packet (MTU):        1500
  Pool Range Start:        (undefined)         Pool Range End:       (undefined)
  Pool Status:                 Invalid         Pool Addresses In Use:          0

  Listen to RIP Packets:       Enabled         Send RIP Packets:          Enabled
  Rip Update Time (seconds):        30         Rip Metric:                      1
  Default Interface:           Disabled        Trusted Routers:           Disabled
  Proxy Arp:                   Disabled

  Packets In:                       622        Packets Out:                  1190
  Packets In Filtered:                0        Packets Out Filtered:            0
  Packet Errors:                      0        Uptime:                      04:03
  Last Packet In:                  0:00        Last Packet Out:              0:00
  Last Routed Packet In:           0:00        Last Round Packet:            0:00
```

The **Show IP Route** command [Figure 5-47, page 5-21] displays the routes currently in the LRS routing table.

The *Source* field indicates how the route was added to the table; statically, locally, or from RIP.

The *Timer* field displays how long (in minutes:seconds format) the LRS will continue to use this route. For static and local routes, this field will display a series of dashes (-----); these routes are never timed out.

If a “T” is displayed to the right of the Timer value, the value represents the route’s time-to-live. If a RIP update for the route is not received within this time period, the route will be marked as unreachable, and the T will be changed to a “D” to denote that the route is invalid, but isn’t ready to be deleted yet. If “Exp” is displayed, the route is about to be deleted from the table.

The *Interface* field displays the interface used to forward packet traffic.

Figure 5-47: Show IP Route Output

```
Local>> SHOW IP ROUTE
       LRS16 Version B1.1/102int(951128)          Name:           DOC_SERVER
       Hardware Addr: 00-80-a3-0b-00-5b           Uptime:        3 Days 02:07
Destination     Next Router     Metric    Source    Timer         Interface
Default Route   192.0.1.70      3         RIP       02:31T        Ethernet
192.4.4.0       192.0.1.202     3         RIP       02:51T        Ethernet
192.0.1.0       192.0.1.57      2         Local     ------        Ethernet
192.3.5.0       192.0.1.238     1         RIP       02:48T        Ethernet
```

5.8 Examples

5.8.1 IP Address Assignment for Remote Networking

An LRS handles incoming calls from a series of remote node users. Two of these users, Bob and Frank, have special IP address requirements.

The LRS must be configured to do the following:

- Assign the same IP address to Bob each time he logs in.
- Permit Frank to select his own IP address.

NOTE: *In general, allowing user-selected IP addresses is not recommended. It poses some security risks and could result in duplicate IP addresses.*

- Dynamically assign IP addresses to the remaining remote node users from an IP address pool. Only five LRS ports have been configured to accept incoming calls, therefore, only five IP addresses must be included in the pool.

Bob will use site **bob** when he logs into the LRS. At authentication time, he will be prompted for the site's local password, **badger**. He will be assigned IP address **192.0.1.108**.

Figure 5-48: Configuring Site bob

```
Local>> DEFINE SITE bob IP REMOTEADDRESS 192.0.1.108
Local>> DEFINE SITE bob AUTHENTICATION LOCAL "badger"
```

When Frank logs into the LRS, he will use site **frank**, which requires that he enter the password **wallaby**. No remote IP address is defined for this site, therefore, Frank may use any IP address he wishes.

Figure 5-49: Configuring Site frank

```
Local>> DEFINE SITE frank AUTHENTICATION LOCAL "wallaby"
```

To create the IP address pool, use the following command:

Figure 5-50: Creating IP Address Pool

```
Local>> DEFINE IP ETHERNET POOL 192.0.1.100 192.0.1.105
```

All incoming callers that do not specify a particular site (such as bob or frank) will use the default site for the connection. To require that default site users use an IP address from the pool, use the **Define Site Default IP Remoteaddress** command.

Figure 5-51: Using the Address Pool for the Default Site

```
Local>> DEFINE SITE DEFAULT IP REMOTEADDRESS 192.0.1.100 192.0.1.105
```

5.8.2 General IP Setup

The following figure illustrates the commands required for the average IP setup:

Figure 5-52: General IP Configuration

```
Local>> DEFINE IP ADDRESS 192.0.1.11
Local>> DEFINE IP SUBNET 255.255.255.0
Local>> DEFINE IP NAMESERVER 192.0.1.45
Local>> DEFINE IP SECONDARY NAMESERVER 192.0.1.184
Local>> DEFINE IP DOMAIN “ctcorp.com”
Local>> DEFINE IP TIMESERVER 192.0.1.45
Local>> DEFINE IP SECONDARY TIMESERVER 192.0.1.455
```

5.8.3 Adding Static Routes

All IP packets to unknown networks must be forwarded to Internet gateway router **192.0.1.110**. A default route to this router must be configured on the LRS, and the route must be included in RIP updates to other routers. The route must have a metric of 2.

Figure 5-53: Default Route to Router

```
Local>> DEFINE IP ROUTE DEFAULT NEXTROUTER 192.0.1.110 2
```

Another router, **192.0.1.99**, provides access to the network **192.1.1.0**. This route must also be assigned a metric of 2.

Figure 5-54: Static Route to Router

```
Local>> DEFINE IP ROUTE 192.1.1.0 NEXTROUTER 192.0.1.99 2
```

5.8.4 Default Routes to a Site

All IP packets to an unknown network must be forwarded to the Internet access provider. Site **internet** is used to manage connections to this location.

A default route to internet must be configured on the LRS. The route must be included in RIP updates to other routers; it must have a metric of two.

Figure 5-55: Default Route to Site

```
Local>> DEFINE IP ROUTE DEFAULT SITE internet 2
```

5.9 Troubleshooting

If you've configured IP and you're experiencing problems with the LRS, check the following:

- Ensure that the IP address is unique. Duplicate IP addresses (the most common IP problem) can cause a number of problems, including failed connections, inconsistent results, and crashes.
- Ensure that the IP address is in the same network range as the other hosts on the network.
- Ensure that the subnet mask matches those of the other hosts on the network.

The table below discusses some common problems, their causes, and possible remedies:

Table 5-3: Troubleshooting

Problem	Possible Cause	Remedy
An IP address has been defined for the unit, but the unit doesn't respond.	Duplicate addresses on the network.	Use the List IP command. If the address is displayed, but doesn't appear when the **Show IP** command is used (after a reboot), check for duplicate addresses on your system.
The IP address doesn't seem to work.	Use of a restricted IP address.	Some network ranges are reserved. Table 5-2 on page 5-1 lists the reserved and available IP addresses. Note that the LRS will not grab its own random IP address; an IP address must be set by the system administrator based on the network to which the LRS belongs.
The LRS cannot contact hosts on the same IP network.	Incorrect subnet mask.	Make sure that the subnet mask is set correctly. Make sure that the LRS's IP address is in the same IP network as the target.
The LRS cannot contact hosts on another IP network.	A route to the other network may not exist.	Ensure that all routers between the LRS and the remote host are functioning properly. Use **Show IP Route** to see all of the routes and routers the unit knows.

5.10 Quick Reference

Setting the IP Address

To	Use This Command	Example(s)	What Example Does
Use an ARP Entry and the Ping Command	See *Using an ARP Entry and the Ping Command* on page 5-2.		
Use a BOOTP or RARP Reply	See the host-based man pages.		
Use the Serial Console Port	First connect a terminal to the serial console port and press the Return key.		
	If the unit is booting when the Return key is pressed, use the Set Server IPaddress command.	`Boot> SET SERVER IPADDRESS 192.0.1.221`	Sets the server's IP address to 192.0.1.221. See *From the Serial Console Port* on page 5-3 for more information.
	If the unit is not booting, use Set / Define IP IPaddress, page 13-85.	`DEFINE IP ADDRESS 192.0.1.221`	Sets the server's IP address to 192.0.1.221.

Setting the Subnet Mask

To	Use This Command	Example(s)	What Example Does
Override the Default Subnet Mask	Set / Define IP Subnet Mask, page 13-89.	`DEFINE IP SUBNET MASK 255.255.255.0`	Creates a custom subnet mask of 255.255.255.0.

Name Resolving

To	Use This Command	Example(s)	What Example Does
Set the Default Domain Name	Set / Define IP Domain, page 13-84.	`DEFINE IP DOMAIN ctcorp.com`	Appends “ctcorp.com” to host names during name resolution. See *Specifying a Default Domain Name* on page 5-6 for more information.
Configure the Domain Name Server	Set / Define IP Nameserver, page 13-86.	`DEFINE IP NAMESERVER 192.0.1.166`	Designates host at 192.0.1.166 as the IP nameserver. See *Configuring the Domain Name Service (DNS)* on page 5-6 for more information.
Configure a Backup Nameserver	Set / Define IP Nameserver, page 13-86.	`DEFINE IP SECONDARY NAMESERVER 192.0.1.167`	If the primary nameserver isn’t available, nameserver requests will be sent to host 192.0.1.167 See *Configuring the Domain Name Service (DNS)* on page 5-6 for more information.

Configuring the Host Table

To	Use This Command	Example(s)	What Example Does
Add Hosts to the Local Host Table	Set / Define Hosts, page 13-81.	`DEFINE HOST Betty 192.0.1.67`	Adds host “Betty” at IP address 192.0.1.67 to the local host table. See *Adding Hosts to the LRS Host Table* on page 5-6 for more information.
Display the Host Table Entries	Show / Monitor / List Hosts, page 13-149.	`SHOW HOSTS`	Displays the current entries in the host table.
Remove an Entry from the Host Table	Clear / Purge Hosts, page 13-6.	`PURGE HOST mercury`	Removes host “mercury” from the LRS host table.

Establishing Sessions

To	Use This Command	Example(s)	What Example Does
Display the Current Sessions	Show / Monitor Sessions, page 13-161.	`SHOW SESSIONS`	Displays all current sessions. See *Sessions* on page 5-7 for more information.
Establish an Outgoing Telnet / Rlogin Session	Connect Telnet, page 13-12.	`CONNECT TELNET athena`	Forms a Telnet connection to host “athena”. See *Outgoing Telnet/Rlogin Connections* on page 5-8 for more information.
		`TELNET athena:145`	Establishes a Telnet connection to host “athena” using port 145.
	Connect Rlogin, page 13-12.	`RLOGIN 192.0.1.15`	Establishes an Rlogin connection to host 192.0.1.15.
Configure the Terminal Type of the LRS Port	Set / Define Ports Telnet Pad, page 13-121.	`DEFINE PORT 2 TERMTYPE VT100`	Sends termtype “VT100” to remote host during sessions. See *Outgoing Telnet/Rlogin Connections* on page 5-8 for more information.
Disable Outgoing Rlogin Connections	Set / Define Server Rlogin, page 13-134.	`DEFINE SERVER RLOGIN DISABLED`	Disables outgoing Rlogin connections. See *Outgoing Telnet/Rlogin Connections* on page 5-8 for more information.
Disable Incoming Telnet / Rlogin Connections	Set / Define Server Incoming None, page 13-128.	`DEFINE SERVER INCOMING NONE`	Disables incoming Telnet and Rlogin connections. See *Incoming Telnet/Rlogin Connections* on page 5-8 for more information.
Require the Login Password for Incoming Telnet / Rlogin Connections	Set / Define Server Incoming Password, page 13-128.	`DEFINE SERVER INCOMING PASSWORD`	Requires the login password for incoming Telnet and Rlogin connections. See *Incoming Telnet/Rlogin Connections* on page 5-8 for more information.

Establishing Sessions, cont.

To	Use This Command	Example(s)	What Example Does
Connect to the Remote Console Port	Connect Telnet <*IP address*> 7000, page 13-12.	`TELNET 192.0.1.345 7000`	Connects to the remote console port (port 7000) of LRS 192.0.1.345. See *Logging Into the Remote Console Port* on page 5-9 for more information.

Security

To	Use This Command	Example(s)	What Example Does
Add an Entry to the IP Security Table	Set / Define IP Security, page 13-88.	`DEFINE IP SECURITY 192.0.1.254 OUTGOING DISABLED PORT 3`	Adds an entry to the IP security table; this entry prevents the LRS from initiating connections on port 3 to host 192.0.1.254. See *IP Security* on page 5-10 for more information.
Delete an Entry From the Security Table	Clear / Purge IP Security, page 13-7.	`PURGE IP SECURITY 192.0.1.102`	Deletes the security table entry associated with 192.0.1.102. See page 5-11 for more information.
Clear the Entire Security Table	Clear / Purge IP Security All, page 13-7.	`PURGE IP SECURITY ALL`	Clears all entries in the IP security table. See page 5-11 for more information.
Prevent All Connections Unless Specifically Enabled in the Table	Set / Define IP Security Incoming Disabled Outgoing Disabled, page 13-88.	`DEFINE IP SECURITY 255.255.255.255 INCOMING DISABLED OUTGOING DISABLED`	Prevents all connections unless an entry is in the IP security table that specifically permits a particular type of connection. See *Using the Security Table* on page 5-11 for more information.

Routing

To	Use This Command	Example(s)	What Example Does
Define a Static Route	Set / Define IP Route, page 13-87.	`DEFINE IP ROUTE 192.5.4.0 NEXTROUTER 192.0.1.1 4`	Specifies that the route to network 192.5.4.0 is through router 192.0.1.1. Assigns a metric of 4 to this route. See *Statically* on page 5-13 for more information.
		`DEFINE IP ROUTE 192.5.3.0 SITE dallas`	Specifies that the route to network 192.5.3.0 is through site “dallas”.
Designate a Default Route	Set / Define IP Route Default, page 13-87.	`DEFINE IP ROUTE 192.0.1.0 DEFAULT SITE internet`	If the LRS receives a packet destined for a network that it cannot find a route for, it will route the packet through site “internet”. See *Statically* on page 5-13 for more information.

RIP

To	Use This Command	Example(s)	What Example Does

Configure the LRS to Only Listen to RIP Updates From Trusted Addresses	1. Set / Define IP Trusted, page 13-90.	`DEFINE IP TRUSTED 192.0.1.67`
		
		`DEFINE IP TRUSTED 192.0.1.254`
			Adds 192.0.1.67 and 192.0.1.254 to the list of trusted routers.
			
			See *Trusted Routers* on page 5-14 for more information.

	2. Set / Define IP All / Ethernet Trusted, page 13-82.	`DEFINE IP ALL TRUSTED ENABLED`	IP interfaces will only listen to RIP updates from the routers in the trusted router list.
Reply to ARP requests for Non-local Networks	Set / Define IP All / Ethernet Proxy-ARP Enabled, page 13-82.	`DEFINE IP ALL PROXY-ARP ENABLED`	When the LRS receives ARP requests for routing information, it will send an ARP reply in response. See *Proxy ARP* on page 5-14 for more information.

Proxy ARPing

To	Use This Command	Example(s)	What Example Does
Enable Proxy ARPing	Set / Define IP All / Ethernet Proxy-ARP Enabled, page 13-82.	`DEFINE IP ALL PROXY-ARP ENABLED`	Enables proxy ARPing for all addresses in the LRS routing table. See *Proxy ARP* on page 5-14 for more information.

Assigning Remote Networking IP Addresses

To	Use This Command	Example(s)	What Example Does
Define an IP Address Pool	Set / Define IP All / Ethernet Pool, page 13-82.	`DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59`	The addresses 192.0.1.50 through 192.0.1.59 will be dynamically assigned to incoming callers. See *IP Address Pools* on page 5-15 for more information.
Define an IP Address Range for a Site's Incoming Callers	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.250`	Requires that incoming callers to site "irvine" use an IP address within the range 192.0.1.110-192.0.1.250. See *Specifying IP Address Range for a Site* on page 5-16 for more information.
Define a Specific IP Address for a Site's Incoming Callers	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.108`	Requires that incoming callers to site "irvine" use IP address 192.0.1.108.
Change the IP Address for a Site's Interface (for Outgoing Connections)	Define Site IP Address, page 13-39.	`DEFINE SITE irvine IP ADDRESS 192.0.1.220`	Assigns IP address 192.0.1.220 to site "irvine". See *Outgoing Connections* on page 5-16 for more information.
Use a Particular IP Address During a SLIP Connection (Port in Character Mode)	Set SLIP, page 13-145.	`SET SLIP irvine 192.0.1.35`	Starts SLIP from character mode, using site "irvine" and assigning address 192.0.1.35 to the incoming caller.

Displaying IP Information

To	Use This Command	Example(s)	What Example Does
Display the Basic IP Configuration	Show / Monitor / List IP, page 13-149.	`SHOW IP`	Displays basic IP configuration information, including information about the IP router, interfaces, and the IP address of the remote host. See *Displaying the IP Configuration* on page 5-19 for more information.
Display Summary Information About Each IP Interface	Show / Monitor / List IP Interface, page 13-149.	`SHOW IP INTERFACE`	Displays a one-line summary for each interface that the router has. See *Displaying the IP Configuration* on page 5-19 for more information.
Display the Routes Currently in the LRS Routing Table	Show / Monitor / List IP Route, page 13-149.	`SHOW IP ROUTE`	Displays all routes currently in the LRS routing table. See *Displaying the IP Configuration* on page 5-19 for more information.

6 IPX

6 - IPX

This chapter explains some important concepts about IPX NetWare setup and routing. This information is only necessary for those using the IPX protocol.

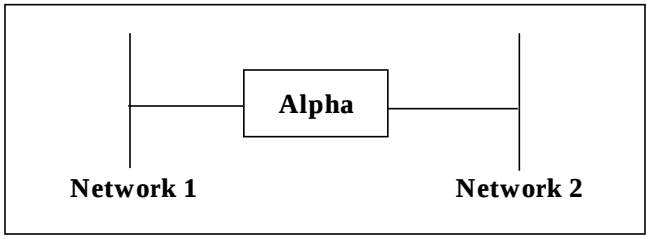
To configure IPX for remote networking, see Chapter 3, *Basic Remote Networking*, and Chapter 4, *Additional Remote Networking*. For specific IPX commands, see Chapter 13, *Command Reference*.

6.1 IPX Networks

The IPX router allows multiple IPX networks to be connected and traffic to pass between them. Each IPX network has a unique network number. Every node on a given IPX network uses the same network number.

For a node on one IPX network to talk to a node on another IPX network, the packets must go through an IPX router that knows how to talk on both IPX networks. This is depicted in Figure 6-1, where IPX network 1 and IPX network 2 are both attached to IPX router Alpha.

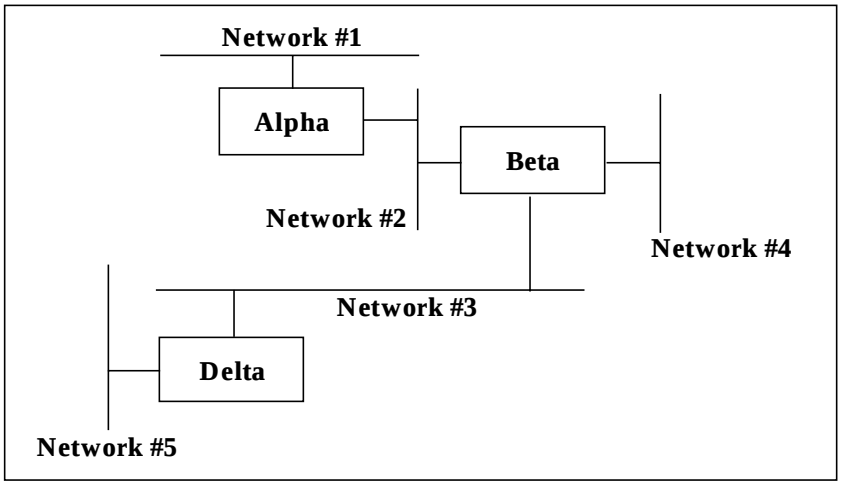
Figure 6-1: Simple IPX Routing



Alpha is configured with two interfaces, one using IPX network number 1 and the other using IPX network number 2. Packets from nodes on network 1 which are destined for nodes on network 2 are actually sent to Alpha which then sends the packets to network 2, and vice-versa. Thus no traffic goes directly between the two networks; they all go through the router.

In Figure 6-2, IPX networks 3, 4, and 5 are added. Note that there is a router between each network. A router is required; nodes on different IPX networks cannot communicate directly to one another.

Figure 6-2: More Complex IPX Routing



6.1.1 Internal and External Networks

Some NetWare nodes such as file servers and routers use an **internal network number**. This number is unique across the IPX network. It is a different network than the network associated with the network connection, which for clarity will be referred to as the **external network**.

For example, when addressing IPX packets to a file server, the destination network number is the file server's internal network number. Since workstations don't have internal networks, when addressing packets to a workstation, the destination network is the external network number.

The internal network number for the LRS is the last four bytes of the unit's Ethernet address, for example, **a3001234**. If necessary, this number can be changed to a unique number (two IPX nodes can't have the same internal network number).

6.1.2 IPX Address Assignment

Every IPX network (including all serial links to remote sites) must be assigned a unique IPX network number. When the LRS is initially configured, a range of IPX network numbers (called a **netrange**) must be defined. The LRS uses the netrange to allocate a network number to each port.

To specify the base number of the range, use the **Set/Define IPX Netrange** command. Each serial port is assigned an IPX network number equalling the base number plus its port number.

Figure 6-3: Defining IPX Netrange

```
Local>> DEFINE IPX NETRANGE 0x100
```

NOTE: *The complete syntax of Set/Define IPX Netrange is listed on page 13-92.*

6.2 Routing

Routers accept packets from one network that are destined for another network, then direct them to the appropriate destination. Routers may seem similar to bridges, but there's an important distinction: bridges forward packets based on the destination Ethernet address, while routers forward packets based on the destination IPX address.

NOTE: *Bridges operate on the Data Link Layer, while routers operate on the Network Layer.*

The LRS examines the destination address of each packet and sends the packet to its destination using the most efficient route. The "most efficient route" is determined by two factors: the network that the address is part of (See *IPX Networks* on page 6-1) and the router's Routing Table.

6.2.1 Routing Table

The IPX router uses a routing table to keep track of which networks are reachable, and the shortest route to each network. A routing table entry consists of the destination network and the router that is the best path to that network. Routing tables also keep track of the **cost** or **metric** required to get to a given network.

Entries may be added to the routing table in three ways: locally, statically, or dynamically.

6.2.1.1 Locally Added Entries

A locally-added route is automatically determined from the LRS IPX network number. The LRS always keeps a local route to the Ethernet to which it is attached.

6.2.1.2 Statically Added Entries

Statically-entered routes are entered and removed by the administrator. These routes are used when dynamic routes cannot be. For example, before an LRS dials a remote site, it has no routes to networks at the remote site. The LRS cannot forward packets to these networks unless static routes are defined for them. These routes should be set with the **site** parameter, because sites are often the most direct connection method. Static routes can also point to routers on the Ethernet.

To configure a static route, use the **Set/Define IPX Route** command. The following example configures a static route to site **irvine**.

Figure 6-4: Configuring a Static Route

```
Local>> DEFINE IPX ROUTE direct SITE irvine 2 50
```

In the above example, two routers are between this router and the destination, and 50 is the allowed time delay, in seconds, that it takes to get to the destination network.

6.2.1.3 Dynamically Added Entries

Dynamic routes are automatically learned from other routers on the network, and are managed by a dynamic routing protocol. The LRS currently supports one dynamic routing protocol, RIP (see *RIP and SAP*, below).

Dynamic routes are automatically entered when new networks come on line, and automatically removed if the networks are no longer reachable. Dynamic routes learned via sites are the exception—they are never timed out. The LRS assumes that these networks are reachable by bringing up a link. This allows the LRS to learn about extended networks at the remote site without the administrator's intervention.

6.2.2 RIP and SAP

RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) packets enable the LRS to broadcast its known routes and services and obtain this information from other routers. Each site may configure RIP and SAP in a number of ways. When a new site is created, the site will listen to RIP and SAP packets by default, and will send RIP and SAP updates when information has changed.

NOTE: *In some situations (for example, to reduce network traffic), RIP and SAP should be disabled. For configuration instructions, see RIP and SAP on page 4-5.*

6.2.3 Routing with File Servers

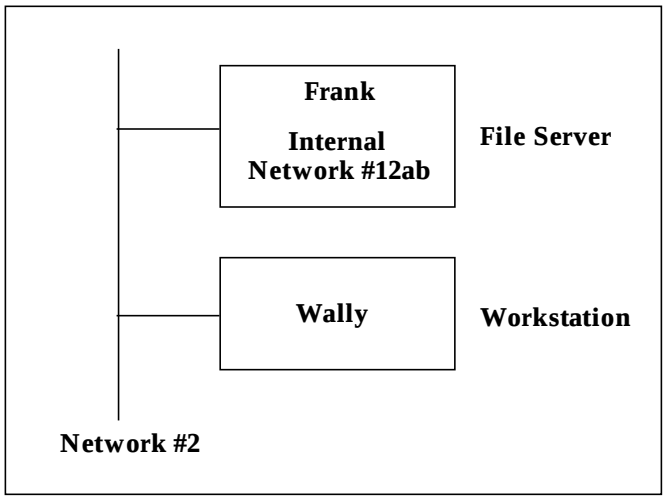
Novell file servers (version 3.11 and above) function as IPX routers, typically routing to their internal networks. File servers have a network number associated with each Ethernet port that is configured for IPX and one internal network number that governs routing between the Ethernet ports.

NOTE: *Your NetWare workstation must use VLM client version 1.20 or greater when connecting to a file server across a router. Versions prior to 1.20 show a decrease in general performance and may have trouble routing between different frame types.*

When the file server sends SAP messages, it is advertising the services it offers as available on this internal network. It also sends out RIP packets announcing that it knows how to get to this internal network.

When a workstation connects to a file server the destination network number is actually the file server's internal network, not the Ethernet's network. This is illustrated in Figure 6-5. In this figure, file server **Frank** and workstation **Wally** are both connected to the Ethernet.

Figure 6-5: Routing to Internal Network Number



The network number for the Ethernet segment is **2**, but Frank's internal network number is **12ab**. Wally cannot access network 12ab directly so it goes through Frank's routing agent, which "internally routes" packets to 12ab.

6.2.3.1 Workstation to File Server Connections

When the client shell is loaded on Wally it sends a SAP request for the nearest file server (see Figure 6-5). The routing process on Frank receives this SAP request and sends a reply containing the IPX address of Frank's file server service.

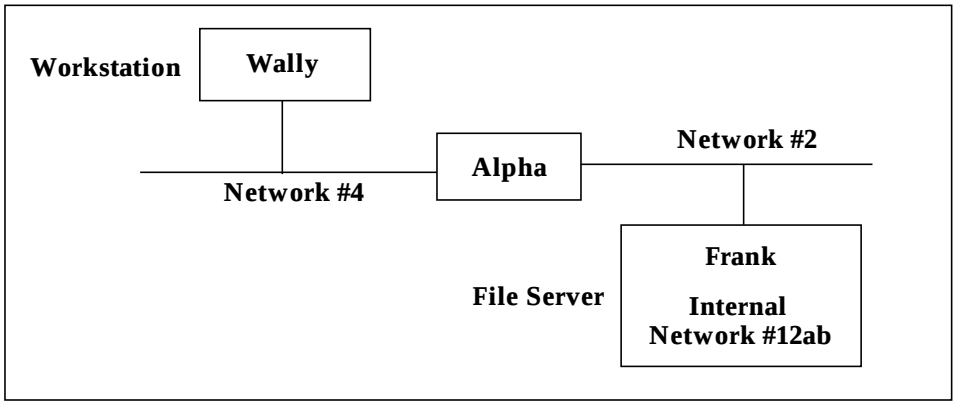
The IPX address consists of the network number, the node number, and the socket number. The network number is Frank's internal network number (**12ab**), the node number is usually **00-00-00-00-00-01**, and the socket number is **0x0451**.

After Wally receives this SAP reply, it sends a RIP request for network 12ab. Frank knows how to get to network 12ab, so it sends a RIP reply to Wally saying that it can handle the packet transfer. Wally then sends packets to Frank's routing process which internally routes the packets to the correct file server process.

Figure 6-6 shows an additional router, Alpha, between Wally and Frank. When Wally tries to connect to Frank, Alpha will perform the function of Frank's routing process, replying to Wally's RIP

and SAP requests. The end result is that packets from Wally are sent to router Alpha which sends them to Frank's routing process, which internally routes to them to the file server process.

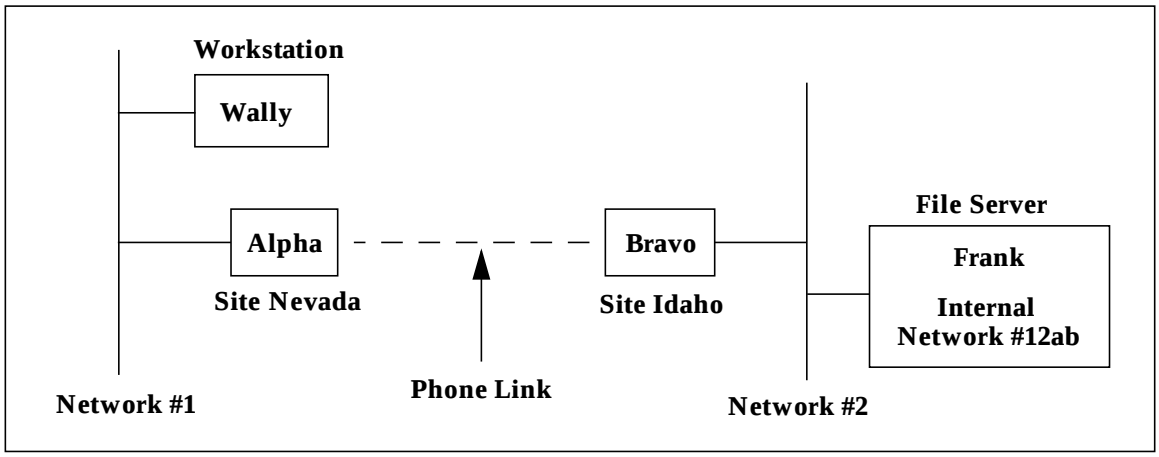
Figure 6-6: Router Between Workstation and File Server



6.3 LAN to LAN Routing

Figure 6-7 depicts two networks separated by a phone link. Now there are three routers between Wally and the file server: **Alpha**, **Bravo**, and Frank's routing process (**Frank**).

Figure 6-7: File Server and Workstation Separated by Phone Link



For routing to work, router Alpha needs to know how to get to network 12ab and needs to know about file server Frank, and router Bravo needs to know how to get to network 1. This information can either be sent via RIP and SAP across the phone link or configured statically on Alpha and Bravo.

NOTE: *See Routing Table on page 6-3 for information on static routes.*

Assuming that Alpha and Bravo know the necessary information, the following sequence of events will occur:

1. When Wally wants to connect to Frank, it will send a SAP request for a file server.
2. Alpha will send a SAP response with information about Frank, which is connected to network 12ab.
3. Wally receives this response and sends a RIP request for network 12ab.
4. Alpha sends a response to this since it has a route to 12ab.
5. Wally sends an **establish connection** packet to Alpha destined for network 12ab.
6. Alpha sends this packet to Bravo, which sends it to Frank.
7. File server Frank sends the reply destined for network 1 to Bravo.
8. Bravo sends the reply to Alpha, which in turn sends it to Wally.

6.3.1 Configuration

To display the current IPX configuration, use the **Show IPX** command. This will display the state of the IPX routing and the Ethernet port configuration. The default IPX configuration is as follows:

- IPX routing is disabled
- All frame types have a network number of 0 and are disabled
- RIP listen and send are enabled
- SAP listen and send are enabled

6.3.1.1 Ethernet Interface

The first step in setting up IPX routing is to enable IPX routing on the LRS. Use the following command:

Figure 6-8: Enabling IPX Routing

```
Local>> DEFINE IPX ROUTING ENABLED
```

Next, the Ethernet interface must be configured to match the IPX network configuration. Two pieces of information are required: the **frame type** and the **network number**.

IPX can run on any of four different Ethernet frame types: **ETHERNET_II**, **802.3**, **802.2**, or **SNAP**. Typically all file servers and workstations on a network are configured to use one frame type. Check the configuration of the Novell file servers and workstations on your network to see which frame type(s) they are using.

Novell file servers also have an IPX network number associated with their Ethernet interfaces. **This is not the internal network number.** This is a common network number that all IPX nodes share for a given network; all file servers on the network will have the same number.

To display the frame type and network number, type **CONFIG** on a file server console screen. Using the displayed type and number, configure the Ethernet interface:

Figure 6-9: Configuring the Ethernet Interface

```
Local>> DEFINE IPX FRAME 802.2 NETWORK abcd
Local>> DEFINE IPX FRAME 802.2 ENABLED
```

In the example above, the frame type is **802.2** and the network number is **abcd**.

Once a frame type is enabled, the IPX router process will send RIP and SAP requests to that interface to get all available routes and services. To confirm that the frame type and number are correct, use the **Show IPX Interface** command.

Figure 6-10: Confirming the Ethernet Interface Configuration

```
Local>> SHOW IPX INTERFACE 802.2
```

The active IPX routing interfaces will be displayed, along with counts for packets received and sent on that interface. If the frame type and network number are correct, these values should be non-zero.

When routing between different frame types, it is possible that the router will send a packet that is larger than the maximum Ethernet packet length. This happens, for example, when one node is using 802.3 or Ethernet v2 and the other is using 802.2 or SNAP. In this case, the node on the 802.3/Ethernet v2 side sends out a packet that is the maximum size for that frame type: 1500 bytes of data plus 14 bytes of header, a total of 1514 bytes. The router then sends the packet to the 802.2/SNAP side. Because the 802.2/SNAP side uses a header of greater than 14 bytes, the packet is now longer than the 1514 byte maximum. To alleviate this problem, add the following command to the NetWare client's **net.cfg** file.

Figure 6-11: Managing Packet Size

```
large internet packets = off
```

The command in Figure 6-11 causes the client to renegotiate with the file server to deliver 576-byte packets. Although this is not an optimal packet size, it is the only way to alleviate the problem.

6.3.1.2 Static Routing

The IPX router can be configured to use only static routes and services. This limits the router to only routing data among the configured static routes.

6.3.1.3 Sample LAN to LAN Configuration

The following section details a sample LAN to LAN configuration, displayed in Figure 6-7 on page 6-5.

6.3.1.3.1 Configuring LRS “Alpha”

LRS Alpha must have IPX routing enabled, and it must have an IPX network number configured for the Ethernet:

Figure 6-12: Enabling IPX Routing and Configuring the Ethernet Interface

```
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX FRAME 802.3 NETWORK 1
```

The range of network numbers for Alpha is defined using the **Define IPX Netrange** command:

Figure 6-13: Defining Range of Network Numbers

```
Local>> DEFINE IPX NETRANGE 10
```

Next, RIP and SAP listening are disabled.

Figure 6-14: Disabling RIP / SAP Listening

```
Local>> DEFINE IPX FRAME 802.3 RIP LISTEN DISABLED
Local>> DEFINE IPX FRAME 802.3 SAP LISTEN DISABLED
```

IPX routing is enabled on the 802.3 frame type using the following command:

Figure 6-15: Enabling IPX Routing on 802.3

```
Local>> DEFINE IPX FRAME 802.3 ENABLED
```

The route to file server Frank’s internal network is statically configured to point to site **idaho**, which handles all connections to Frank.

Figure 6-16: Configuring Static Route to Network 12ab

```
Local>> DEFINE IPX ROUTE 12ab SITE idaho
```

A service named **frank** is configured using the **Set/Define IPX Service** command:

Figure 6-17: Creating Service

```
Local>> DEFINE IPX SERVICE frank 4 12ab 00-00-00-00-00-01 451
```

Note in the above example that the static service **frank** does not reference site **idaho**. It is only specified that frank is on IPX network 12ab; the Define Route command used in Figure 6-16 specified that the static route to network 12ab points to site idaho.

NOTE: *In Figure 6-17, the numbers 4 and 451 correspond to the service type and socket, respectively. See Services and Sockets on page 6-11 for more information.*

6.3.1.3.2 Configuring LRS "Bravo"

LRS Bravo must also have IPX routing enabled and an IPX network number configured for its Ethernet interface. The following commands are used:

Figure 6-18: Enabling IPX Routing and Configuring the Ethernet Interface

```
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX FRAME SNAP NETWORK 2
```

The range of network numbers for Bravo is defined using the **Define IPX Netrange** command:

Figure 6-19: Defining Range of Network Numbers

```
Local>> DEFINE IPX NETRANGE 20
```

RIP and SAP listening are disabled using the following command:

Figure 6-20: Disabling RIP / SAP Listening

```
Local>> DEFINE IPX FRAME SNAP RIP LISTEN DISABLED
Local>> DEFINE IPX FRAME SNAP SAP LISTEN DISABLED
```

IPX routing is enabled on the SNAP frame type:

Figure 6-21: Enabling IPX Routing on SNAP

```
Local>> DEFINE IPX FRAME SNAP ENABLED
```

The route to network 1 is statically configured to point to site **nevada**, which handles all connections to network 1.

Figure 6-22: Configuring Static Route to Network 1

```
Local>> DEFINE IPX ROUTE 1 SITE nevada
```

When the client shell on Wally is loaded the following sequence of events will occur:

1. Wally requests the nearest file server.
2. LRS Alpha has a static route to a file server, so it will respond with information about Frank.
3. Wally will then ask for a route to Frank's IPX network, 12ab.
4. LRS Alpha has a static route to 12ab, so it will respond with that information.
5. Wally will then send an **establish connection** packet to IPX network 12ab.
6. LRS Alpha receives this packet and will route the packet to site idaho. If the link between Alpha and Bravo isn't currently up, Alpha will establish the connection.
7. When LRS Bravo receives the packet, it will route it out the Ethernet interface to Frank.

8. Frank will send a reply to IPX network 1.
9. LRS Bravo consults its routing table, and routes this packet to site nevada.

Imagine that there is another file server on network 2, **Delta**, which has internal network number **74fca132** and hardware address (node number) **00-00-12-00-12-34**. The following commands entered on LRS Alpha will allow workstations to connect to Delta:

Figure 6-23: Enabling Connections to File Server Delta

```
Local>> DEFINE IPX ROUTE 74fca132 SITE idaho
Local>> DEFINE IPX SERVICE delta 4 74fca132 00-00-12-00-12-34 451
```

The commands in Figure 6-23 tell LRS Alpha that file server Delta is on network **74fca132** and that network is reachable through site **idaho**.

NOTE: *In Figure 6-23, the numbers 4 and 451 correspond to the service type and socket, respectively. See Services and Sockets on page 6-11 for more information.*

6.4 Remote Node Routing

Three things must be configured in order to support IPX remote node routing functionality:

- IPX Routing must be enabled
- The frame type(s) must be set and enabled, see *Ethernet Interface* on page 6-6
- A netrange must be defined, see *IPX Address Assignment* on page 6-2

6.5 Spoofing

Spoofing enables an LRS to send keepalive packets and responses to and from a file server and workstation. This permits the connection between the workstation and file server (or between two LRS units) to remain idle when there is no interactive packet traffic; while spoofing is enabled, connections will not be initiated simply for keepalive packets.

Spoofing is discussed in detail in Chapter 4, *Additional Remote Networking*.

6.6 Services and Sockets

A static service includes a service type and a socket number. For example, a static service for a file server would use service type 4 and socket 451 (see Figure 6-24). Table 6-1 list some of the more well-known service types.

Table 6-1: Common Service Types

Type	Purpose	Type	Purpose
0000	Unknown	0024	Remote Bridge Server
0003	Print Queue	0027	TCP/IP Gateway
0004	File Server	002D	Time Synch Server
0005	Job Server	0047	Advertising Print Server
0007	Print Server	0098	NetWare Access Server
0009	Archive Server	009E	Portable NetWare
000B	Administration	FFFF	Wildcard
0021	NAS SNA Gateway		

Sockets are part of the IPX network address and need to be specified when configuring a static service. For example, you would use the NCP socket (socket 451) to set up a static service for a file server (service type 4). The service would be configured as follows:

Figure 6-24: Sockets as Part of a Static Service

```
Local>> DEFINE IPX SERVICE doc_server 4 2c15e830 00-00-00-00-00-01 451 3
```

NOTE: *For an explanation of the above command, see Set/Define IPX Service on page 13-94.*

Some of the more common IPX sockets are listed in Table 6-2. Leading zeroes can be omitted from the command.

Table 6-2: Common IPX Sockets

Socket	Purpose
0451	NetWare Core Protocol (NCP)
0452	Service Advertising Protocol (SAP)
0453	Routing Information Protocol (RIP)
0455	Novell NetBIOS
0456	Diagnostics

6.7 Examples

6.7.1 LAN to LAN

In this example, there are two different LANs, one in Los Angeles and one in San Diego. The LANs are connected via two LRS units and a leased line.

This LAN to LAN connection must meet the following criteria:

- Users in San Diego occasionally connect to a NetWare file server in Los Angeles.
- Users in Los Angeles occasionally connect to a NetWare file server in San Diego.
- IPX traffic must be transferred.

6.7.1.1 LRS in San Diego

This LAN is running NetWare on frame type **802.2**. The network number is **1234ABCD**. The leased line is connected to port 2 of the LRS.

Figure 6-25: San Diego LRS Configuration

```
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX FRAME 802.2 NETWORK 1234ABCD
Local>> DEFINE IPX FRAME 802.2 ENABLED
Local>> DEFINE IPX NETRANGE 100
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> INITIALIZE DELAY 0
```

6.7.1.2 LRS in Los Angeles

This LAN is running NetWare on frame type **802.2**. The network number is **FED**. The leased line is connected to port 2 of the LRS.

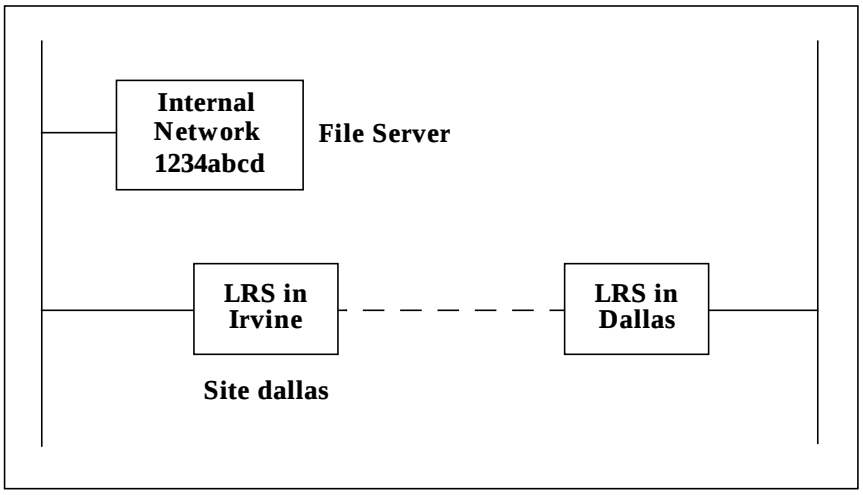
Figure 6-26: Los Angeles LRS Configuration

```
Local>> DEFINE IPX ROUTING ENABLED
Local>> DEFINE IPX FRAME 802.2 NETWORK FED
Local>> DEFINE IPX FRAME 802.2 ENABLED
Local>> DEFINE IPX NETRANGE 200
Local>> DEFINE PORT 2 AUTOSTART ENABLED
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> INITIALIZE DELAY 0
```

6.7.2 Packet Filters

An LRS in Irvine uses site **dallas** to manage connections to an LRS in Dallas. A filter list must be configured for this site to forward only 3 types of packets: IPX RIP, IPX SAP, and packets from a file server with internal network number **0x1234abcd.**

Figure 6-27: LAN to LAN Connection Between Irvine and Dallas



The following commands must be used to create the filter list:

Figure 6-28: Creating the Filter List

```
Local>> DEFINE FILTER texasfilt CREATE
Local>> DEFINE FILTER texasfilt ADD ALLOW IPX SNET 0xffffffff 0x1234abcd
Local>> DEFINE FILTER texasfilt ADD ALLOW IPX DSOCK EQ RIP
Local>> DEFINE FILTER texasfilt ADD ALLOW IPX DSOCK EQ SAP
Local>> DEFINE FILTER texasfilt ADD ALLOW IPX TYPE RIP
Local>> DEFINE FILTER texasfilt ADD ALLOW IPX TYPE SAP
Local>> SAVE FILTER texasfilt
```

To associate filter list **texasfilt** with site **dallas**, the Define Site Filter command is used.

Figure 6-29: Associating the Site with the Filter List

```
Local>> DEFINE SITE dallas FILTER OUTGOING texasfilt
```

Site dallas will use texasfilt as an outgoing filter list. When dallas is used for a connection, outgoing packets will be compared to the filters in this list before they are forwarded.

For complete filter list configuration instructions, see *Packet Filters and Firewalls* on page 12-22. The complete syntax of Set / Define Filter is listed on page 13-74. Define Site Filter is discussed on page 13-37.

6.8 Troubleshooting

If you experience problems using your LRS for IPX networking, there are two main troubleshooting areas to check:

- Ensure that the LRS is connected properly to a power source and to the Ethernet. See your **Installation Guide** for more information.
- Ensure that the LRS is configured properly for your network. IPX configuration items are listed in Table 6-3.
- Examine the error codes (if any) by entering the **Show/Monitor/List NetWare** command.

Table 6-3: IPX Settings to Check

Area To Check	Desired Configuration
Display the IPX configuration.	Use the **Show IPX** command (page 13-151) to display the IPX configuration. If the LRS is configured properly, the command should show the following: 1. IPX routing is enabled 2. The Netrange is non-zero 3. The correct frame type(s) for your network is / are enabled. 4. The LRS has the correct network number These items are explained further below.
Check the IPX network number(s).	The LRS must have a unique internal network number. If there is a duplicate, change the LRS's network number.
Check the IPX Netrange.	Ensure that a netrange has been set. See the **Set/Define IPX Netrange** command on page 13-92 for more information.
Check the enabled frame types.	If packets are transferred between some but not all nodes on the network, it is possible that they are not using the same frame type(s). Ensure that the frame type(s) of both the origination node and destination node are enabled. Re-enable any frame types necessary.
Check the internal routing setting.	If more than one frame type is enabled, internal routing should also be enabled.
Display the IPX counters.	Use the **Show IPX Interface** or **Show IPX Interface <name>** command (page 13-151) to display the counters for active IPX interfaces. These counters should be non-zero.

Table 6-3: IPX Settings to Check, cont.

Area To Check	Desired Configuration
Display the IPX routes.	Use the **Show/Monitor/List IPX Routes** command (page 13-151). If the LRS is configured properly, a routing table should be displayed showing all known routes. If no routes are displayed, type **Show IPX Interface** to determine if RIP listening is enabled for your frame type and if any RIP responses have been received. If no RIP responses have been received, make sure that the frame type and network number displayed match your network.
Display the IPX services.	Use the **Show IPX Services** command (page 13-151). If the LRS is configured properly, a service table should be displayed which shows all known services. If no services are displayed, type **Show IPX** to determine if SAP listening is enabled for your frame type. Use the Show IPX Interface or Show IPX Interface <frame type> commands to determine if the LRS is receiving SAP responses. If no SAP responses have been received, make sure the frame type and network number match your network. In addition, check the network cabling.
Ensure that IPX is enabled on all sites.	Use the **Show Site IPX** command (page 13-161) to display the IPX information for all sites that need to forward IPX traffic.
Log IPX activity.	Logging displays real-time information to the user by displaying events as they are happening. To log IPX activity, become the privileged user (page 13-124) and enter the following commands: **Set/Define Logging Destination Memory** (page 13-96). **Set/Define Logging IPX 7** (page 13-96). **Monitor Logging Memory** (page 13-152). If you attempt to establish a dial connection at this point, all IPX debugging information about link establishment will be displayed.

6.8.1 NetWare Error Codes

When the LRS detects NetWare problems, it will record the problem in the form of an error code. To display these error codes, use the **Show/Monitor/List NetWare** command. The **Error Reasons** field may display a hexadecimal value.

To translate the hexadecimal value into a bit number and find out what error it represents, see the Show / Monitor / List NetWare command entry on page 13-153 of the *Command Reference*.

6.9 Quick Reference

IPX Address Assignment			
To	**Use This Command**	**Example(s)**	**What Example Does**
Specify the Base Number of the IPX Netrange	Set / Define IPX Netrange, page 13-92.	`DEFINE IPX NETRANGE 0x100`	Defines 0x100 as the base number of the LRS netrange. Each LRS port will be assigned an IPX network number equal to the sum of 0x100 and the port number. For more information, see *IPX Address Assignment* on page 6-2.
Routing			
To	**Use This Command**	**Example(s)**	**What Example Does**
Display the Current IPX Configuration	Show / Monitor / List IPX, page 13-151.	`SHOW IPX`	Displays information about IPX RIP, SAP, frame types, and whether IPX routing is enabled or disabled. For more information, see *Ethernet Interface* on page 6-6.
Enable IPX Routing	Set / Define IPX Routing, page 13-94.	`DEFINE IPX ROUTING ENABLED`	Enables the LRS to route IPX packet traffic. For more information, see *Ethernet Interface* on page 6-6.

Configure the Ethernet Frame Type and Network Number	Set / Define IPX Ethernet Frame, page 13-90.	`DEFINE IPX ETHERNET FRAME 802.2 NETWORK abcd`
		
		`DEFINE IPX ETHERNET FRAME 802.2 ENABLED`
			Enables frame type 802.2 on Ethernet abcd.
			
			For more information, see *Ethernet Interface* on page 6-6.

Routing, cont.

To	Use This Command	Example(s)	What Example Does
Verify the Current IPX Frame Type and Network Number	Show / Monitor / List IPX Interface, page 13-151.	`SHOW IPX INTERFACE 802.2`	Displays the active IPX routing interfaces. For more information, see *Ethernet Interface* on page 6-6.
Define a Static Route	Set / Define IPX Route, page 13-93.	`DEFINE IPX ROUTE 1234 NEXTROUTER 45af-00-00-ab-12-e2-38`	Specifies that the route to network 1234 is through router 45af-00-00-ab-12-e2-38. For more information, see *Routing Table* on page 6-3.
		`DEFINE IPX ROUTE 1234 SITE dallas 2 50`	Specifies that the route to network 1234 is through site “dallas”.
Define a Static Service	Set / Define IPX Service, page 13-94.	`DEFINE IPX SERVICE frank 4 12ab 00-00-00-00-00-01 451`	Creates a static service named “frank”. This service is on network 12ab, node 00-00-00-00-00-01, socket 451. It is a type 4 service. For more information, see *Routing Table* on page 6-3.
Disable RIP or SAP	See *RIP and SAP* on page 4-5.		
Configure Keepalive Spoofing	See *Spoofing* on page 4-5.		

7 AppleTalk

7 - AppleTalk

This chapter explains the important concepts of AppleTalk addressing, routing, and networking. This information is only necessary for those using the AppleTalk protocol.

7.1 Concepts

The LRS supports AppleTalk Phase 1 and Phase 2 networking. The main features of AppleTalk networks are discussed in the following sections.

7.1.1 Node Names and Addresses

AppleTalk devices have two main types of identifiers: node names and node addresses. Nodes are usually named for the physical device's primary owner or primary purpose. For example, a file server sitting in a company's accounting department may be named "MoneyMac."

Node addresses are more complex. Each node address is made up of a 16-bit network number portion and an 8-bit node number portion, expressed together in decimal format as **network.node**. The network number portion is provided by a router and is taken from the network number range of the connected network segment. Each node chooses a node number portion whenever it is connected to the AppleTalk network. Node addresses, not node names, function as the unique identifier for each networked node.

NOTE: *Node numbers are not permanent; nodes may choose a different node number if they are disconnected from and reconnected to the network.*

7.1.2 Zones

A zone is a logical grouping of networked AppleTalk nodes. Every node on the network is associated with one and only one zone. When a node is first added to an AppleTalk network, it will appear in the default zone. Nodes can be moved to different zones if desired.

NOTE: *It is strongly recommended that zone names be kept unique on the local network.* *See the How Sites Work section on page 7-5 for more information.*

7.1.3 Name Binding Protocol (NBP)

The Name Binding Protocol is used by nodes and applications to learn the addresses of other nodes on the network. NBP maps the node's name to its address so that it is easier for users to locate; it is easier to remember a descriptive name for a node than to remember its precise network address.

To understand how NBP works, examine the Apple Chooser application. When a user opens the Chooser, he is presented with a list of zones, one of which is highlighted, and a list of device types. If he selects LaserWriter as the device type, he will see a list of all LaserWriter devices in the selected zone. At this point, he can choose a particular LaserWriter to connect to without ever having to know the printer's network address.

NBP is more complex than that, however. While the user selects a zone and device type, NBP looks up the appropriate zone and asks for devices of the chosen device type to respond. The responses include each device's name and network address. NBP then sends a list of responding

devices back to the Chooser where the user can select one of the devices. The exchange takes place almost instantly.

NOTE: *If there are two or more networks with the same zone name, an NBP query will search both networks.*

7.1.4 AppleTalk Routing

7.1.4.1 Routers

There are two types of routers on AppleTalk networks: seed routers and learning routers. Seed routers propagate information about their attached networks to other routers on the network. Learning routers do not propagate information, but merely learn it from the seed routers. Each AppleTalk network must have at least one seed router.

Seed routers may allow their own routing table information to be "overruled" by another seed on the network. The philosophy is that other seeds may have more accurate information because they were on the network first.

In order to route packets successfully, all routers on a network segment must know the network number range and zone list to use for that segment. The network range is a contiguous range of valid network numbers. The size of the network range determines the maximum number of nodes allowed on that network. The zone list for each segment can contain up to 255 zone names, one of which is designated as the default zone.

NOTE: *For optimal performance, use the smallest network range that meets your needs.*

All routers on the network must agree on the network range and the contents of the zone list. They must also agree which zone from the zone list is the default zone for that network.

7.1.4.2 Routing Tables

When an AppleTalk router is added to the network or brought back on-line after a shutdown, it propagates a list of its associated zones and network numbers. It also receives information from all adjacent routers on the network. This information is stored by each router in a **routing table**.

The routing table includes information about all of the networks it can see, including their network number ranges, associated **hop-counts** (the number of routers it takes to get to the network), the identifier of the next router needed to get to that network, and an **entry state** that tells whether the route is more likely to be reliable or outdated. This information can change as networks and routers are brought on-line and off-line.

A simplified example of a routing table appears below:

Network	Next Router	Metric	State	Zone Name
3-5	0	0	Good	Doc_Zone
11	3.41	1	Good	Accounting
27	3.208	3	Good	Dallas

A router must include an entry in its routing table for every zone that it is willing to route to, and it must advertise the zones to other AppleTalk routers. **RTMP** (the Routing Table Maintenance Protocol) governs updates to the routing table.

7.1.5 AppleTalk on the LRS

Before the LRS can be used on an AppleTalk network, it must have both a name and an AppleTalk network address, and it must be placed in a valid AppleTalk zone. If you would like the LRS to function as a seed router on the network, you must also configure seed information. See the following section, *Configuring the LRS*, for specific configuration options.

Once on the network, the LRS uses sites to administer both LAN to LAN and remote node connections. For LAN to LAN connections, the remote LAN's zone name and network number(s) are associated with the site. For remote node dial-ins, a single zone and network number pair is configured on the LRS for all users. Sites are then used to control authentication, filters, time to dial, and other connection options.

NOTE: *For general information about LAN to LAN and remote node networking, see Connection Types on page 3-1. For more information about sites, see Managing Connections With Sites on page 3-2.*

NOTE: *AppleTalk sites can use RADIUS for authentication. For more information about RADIUS, see page 12-12.*

For LAN to LAN connections, the LRS advertises all of its configured LAN to LAN zones to other nodes on the Ethernet. When another node on the network tries to connect to one of these zones, the LRS will attempt to bring up a link to the remote site. For remote node connections, a remote client dials into the LRS and the LRS gives it a node number from the configured remote node network number. The remote client can then access the attached Ethernet, with the LRS acting as a router between the Ethernet network numbers and the remote node network number. LAN to LAN and remote node configurations are detailed in *AppleTalk Networking* on page 7-5.

7.2 Configuring the LRS

Address information may be changed at any time. However, AppleTalk routing must be turned off to configure any seed, routing, or networking settings. This is not a limitation of the LRS, but a peculiarity of the AppleTalk protocol itself. If parameters are changed while the LRS is on-line and actively routing packets, the changes will not be propagated accurately to the other routers.

The LRS can be configured in one of two ways:

1. Ensure that AppleTalk routing is disabled (the default), configure all AppleTalk parameters using Set commands, then re-enable AppleTalk routing.
2. Configure all AppleTalk parameters using Define commands, ensure that AppleTalk routing is enabled, then reboot the LRS.

The following configurations assume that the second option was chosen.

7.2.1 Address Information

The LRS comes pre-configured with a server name, and this name will be used to identify it on the AppleTalk network. To change the LRS server name, see **Set/Define Server Name** on page 13-130.

When it is first connected to the AppleTalk network, the LRS will acquire a temporary network number from a predetermined range of startup numbers, then find an unused node number on that network. Using these numbers as a temporary network address, the LRS can communicate with another router and obtain a valid network number from the network's pre-configured network number range.

AppleTalk nodes must also be assigned to a valid existing zone. Initially, the LRS will appear in the network's **default zone**. To reassign the LRS to a different zone, use the **Set/Define AppleTalk Ethernet Zone** command:

Figure 7-1: Assigning the LRS to a Zone

```
Local> DEFINE APPLETALK ETHERNET ZONE "Doc Zone"
```

The LRS can be part of any zone that is being advertised by another router on the Ethernet.

7.2.2 Seed Router Information

The LRS can be configured as a learning router, or as a seed router if there are no other seed routers on the network. If there is at least one other seed router, the LRS will function as a learning router regardless of its configuration, allowing the existing seed router's information to override its own settings.

Before the LRS can be used as a seed router for the Ethernet, seed information must be configured using the **Set/Define AppleTalk Ethernet Seed** command. Give the LRS a valid network number range to use for the Ethernet, and a list of zones on the network. If the default zone is not explicitly specified, the first zone entered becomes the default. Also, the unit must have AppleTalk routing enabled via the **Set/Define AppleTalk Routing** command.

Figure 7-2: Configuring LRS Seed Information

```
Local>> DEFINE PROTOCOLS APPLETALK ETHERNET SEED 18 22
Local>> DEFINE PROTOCOLS APPLETALK ETHERNET SEED ZONE "Doc Zone" DEFAULT
Local>> DEFINE PROTOCOLS APPLETALK ETHERNET SEED ZONE "Accounting"
Local>> DEFINE PROTOCOLS APPLETALK ROUTING ENABLED
Local>> LIST APPLETALK ZONES
```

In the example above, the valid network number range is 18 to 22. Two zones have been named as part of the network, and the default zone has been designated. Routing was enabled so that the LRS would come on-line as a router after the reboot. In addition, the **List AppleTalk Zones** command was entered to double-check the zone name configuration before rebooting the unit.

Up to 255 zones can be specified with repeated **Set/Define AppleTalk Ethernet Seed Zone** commands. However, zones cannot be removed individually— seed information must be removed entirely before new seed information can be entered. To remove seed information, enter the **Clear/Purge AppleTalk Ethernet Seed** command:

Figure 7-3: Removing Seed Information

```
Local>> PURGE APPLETALK ETHERNET SEED
```

7.3 AppleTalk Networking

7.3.1 How Sites Work

When a user opens the Macintosh Chooser and selects a zone that must be accessed via the LRS, the LRS brings up a site to query the specified zone for its attached devices and the information needed to connect to them. The user then selects a particular device by name, and is connected to that device via the site that was started for the look-up.

If there are multiple sites associated with the same zone name, the LRS will bring up all connections to all of the sites. It is therefore recommended that zone names be kept unique on a network.

NOTE: *AppleTalk sites can use RADIUS for statistics logging. For more information about RADIUS, see page 12-12.*

7.3.2 LAN to LAN Connections

During LAN to LAN remote networking, the LRS functions as a half-router, meaning that it is one of two routers connecting geographically-separate AppleTalk networks via a long-distance communication link. The link can be a simple modem connection, or it can include several devices across several networks.

7.3.2.1 Creating the Site

A LAN to LAN site must be created on the LRS before users can connect, and AppleTalk routing must be enabled for a LAN to LAN site.

Figure 7-4: Creating a LAN to LAN AppleTalk Site

```
Local>> DEFINE SITE “conn1” APPLETALK ENABLED APPLETALK ROUTING ENABLED
```

If you also want the site to accept packets that update the routing table, enable the RTMP characteristic for the site.

Figure 7-5: Enabling RTMP

```
Local>> DEFINE SITE “conn1” APPLETALK RTMP ENABLED
```

The LRS will still receive updates from other routers regardless of the RTMP setting.

7.3.2.2 Creating a Route to the Site

In order to make an outgoing LAN to LAN connection from the LRS, there must be a zone name, site name, metric, and network number range configured on the LRS to use for the connection. Together, this information constitutes a route to the site, and is specified with the **Set/Define AppleTalk Route** command.

Figure 7-6: Configuring a Route to an AppleTalk Site

```
Local>> DEFINE PROTOCOLS APPLETALK ROUTE “Marketing” “conn1” 3 18 22
```

NOTE: *Remember, AppleTalk Routing must be turned off while routing configurations are being made.*

In the previous example, the route allows LAN to LAN users to connect to site *conn1* of zone *Marketing*. The number 3 is a metric, which means that the route goes through three routers before connecting to the site. The last two numbers identify the network number range of 18 to 22.

To view configured routes to sites, use one of the following **Show/Monitor/List AppleTalk** commands. The first shows the RTMP routing table organized by network number range, and the second shows the routes organized by zone.

Figure 7-7: Viewing Configured Routes

```
Local>> LIST PROTOCOL APPLETALK ROUTES
OR
Local>> LIST PROTOCOL APPLETALK ZONES
```

Configured routes can be removed individually or in groups. Use the **Clear/Purge AppleTalk** command to remove routes to LRS sites on a particular network, or all routes to LRS sites. The following example removes the route configured in Figure 7-6, and all other routes to sites on that network segment.

Figure 7-8: Removing a Route

```
Local>> PURGE APPLETALK ROUTE NET 18
```

7.3.3 Remote Node Connections

Before dial-in users can connect to the LRS, a site must be configured for incoming remote node connections. Remote node connections do not involve routing, so AppleTalk routing must be disabled for a remote node site.

Figure 7-9: Creating a Remote Node AppleTalk Site

```
Local>> DEFINE SITE “incoming” APPLETALK ENABLED APPLETALK ROUTING DIS-
ABLED
```

The LRS assigns a zone name and network number to all dial-in users. If the remote node does not want to use the assigned zone and network number, the connection will be denied.

The zone name and network number for remote node users can be configured with the **Set/Define AppleTalk Remote** command.

Figure 7-10: Configuring Incoming Remote Node Connections

```
Local>> DEFINE PROTOCOLS APPLETALK REMOTE “Accounting” 54
```

NOTE: *Remember, AppleTalk Routing must be turned off while remote node configurations are being made.*

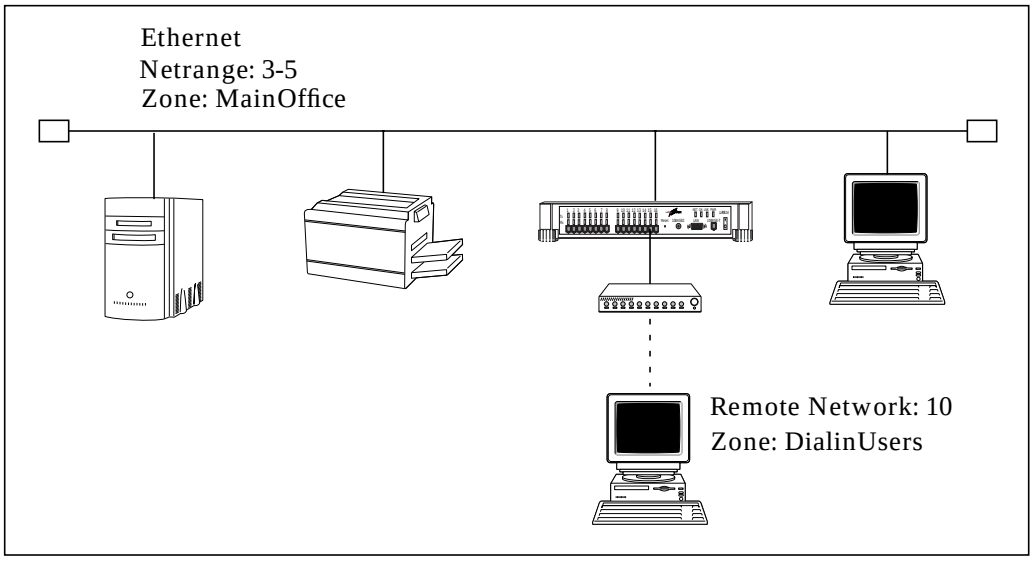
In the example above, remote node users dialing into the LRS will use the zone named *Accounting*, on a network whose network number is 54.

7.4 Examples

7.4.1 Basic Remote Node

The main office of a company wants its employees to be able to dial in and connect to the network. The company has an LRS on their network, and a modem attached to the LRS for the dial-in connections. The basic topology is shown in the following figure:

Figure 7-11: Basic Remote Node Example



For this type of connection, remote node parameters need to be configured, and a site must be created for remote node users. The configuration needed for the LRS is as follows:

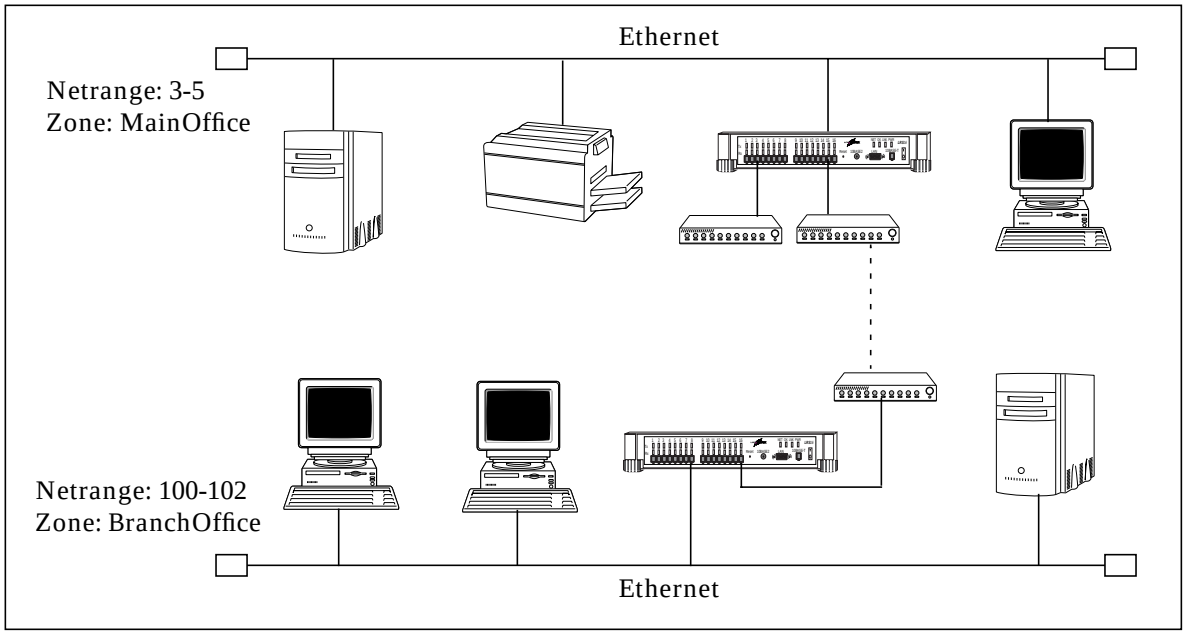
Figure 7-12: Main Office Remote Node Configuration

```
Local>> DEFINE APPLETALK REMOTE “DialinUsers” 10
Local>> DEFINE SITE “dialin” APPLETALK ENABLED
Local>> DEFINE SITE “dialin” APPLETALK ROUTING DISABLED
```

7.4.2 LAN to LAN

Suppose the main office in the previous example has a branch office, and it wants employees at the branch office to be able to access networked devices at the main office. The offices are connected by a modem link between two LRSs. The network topology is shown below:

Figure 7-13: LAN to LAN Example



The LRS at the branch office is going to be used as a seed router for its small LAN, so seed information must be configured. In addition, a LAN to LAN site must be created for main office connection, which will be called **mainsite**, as well as a route to the site. The following commands would be needed:

Figure 7-14: Branch Office Configuration

```
Local>> DEFINE APPLETALK SEED 100 102
Local>> DEFINE APPLETALK SEED ZONE “BranchOffice” DEFAULT
Local>> DEFINE SITE “mainsite” APPETALK ENABLED
Local>> DEFINE SITE “mainsite” APPLETALK ROUTING ENABLED
Local>> DEFINE SITE “mainsite” APPLETALK RTMP ENABLED
Local>> DEFINE APPLETALK ROUTE “MainOffice” “mainsite” 1 3 5
Local>> DEFINE APPLETALK ROUTING ENABLED
```

The main office LRS only accepts incoming LAN to LAN connections, therefore, the only configuration needed is the site to use for the connection. The site will be called **remotesite**.

Figure 7-15: Main Office Configuration

```
Local>> DEFINE SITE “remotesite” APPLETALK ENABLED
Local>> DEFINE SITE “remotesite” APPLETALK ROUTING ENABLED
Local>> DEFINE SITE “remotesite” APPLETALK RTMP ENABLED
```

7.5 Quick Reference

Address Information			
To	**Use This Command**	**Example(s)**	**What Example Does**
Configure the LRS's Name	See *Changing the LRS Server Name* on page 2-4.		
Add the LRS to an AppleTalk Zone	Set / Define AppleTalk Ethernet Zone, page 13-60.	`DFINE APPLETALK ETHERNET ZONE "Marketing"`	Places the LRS in the specified zone. See *Address Information* on page 7-3 for more information.
Seed Router Configuration			
To	**Use This Command**	**Example(s)**	**What Example Does**
Specify the Network Number Range for the Network	Set / Define AppleTalk Ethernet Seed *number*, page 13-59.	`DEFINE APPLETALK ETHERNET SEED 52 55`	Configures a network number range of 52 to 55. See *Seed Router Information* on page 7-4 for more information.
Specify the Zones Associated with the Network	Set / Define AppleTalk Ethernet Seed Zone, page 13-59.	`DEFINE APPLETALK ETHERNET SEED ZONE "Internal"`	Adds this zone to the network zone list. See *Seed Router Information* on page 7-4 for more information.
Specify the Default Zone	Set / Define AppleTalk Ethernet Seed Zone, page 13-59.	`DEFINE APPLETALK ETHERNET SEED ZONE "Public" DEFAULT`	Adds this zone to the network zone list, and specifies it as the default zone for the network. See *Seed Router Information* on page 7-4 for more information.
View the Zone List	Show / Monitor / List AppleTalk, page 13-147.	`SHOW APPLETALK ZONES`	Displays the network's currently configured zones. See *Seed Router Information* on page 7-4 for more information.

Seed Router Configuration, cont.

To	Use This Command	Example(s)	What Example Does
Remove LRS Seed Configuration	Clear / Purge AppleTalk, page 13-4.	`PURGE APPLETALK ETHERNET SEED`	Specifies the removal of **all** configured LRS seed information when the unit is rebooted. See *Seed Router Information* on page 7-4 for more information.

LAN to LAN Networking

To	Use This Command	Example(s)	What Example Does
Create a LAN to LAN AppleTalk Site	Define Site AppleTalk, page 13-31.	`DEFINE SITE "applelan" APPLETALK ENABLED`	Creates a site called *applelan* which is to be used for AppleTalk connections. See *LAN to LAN Connections* on page 7-5 for more information.
Enable Routing on the Site	Define Site AppleTalk, page 13-31.	`DEFINE SITE "applelan" APPLETALK ROUTING ENABLED`	Enables AppleTalk routing on site *applelan*. See *LAN to LAN Connections* on page 7-5 for more information.
Enable Routing Table Updates for the Site	Define Site AppleTalk, page 13-31.	`DEFINE SITE "applelan" APPLETALK RTMP ENABLED`	Enables incoming routing table update packets on site *applelan*. See *LAN to LAN Connections* on page 7-5 for more information.
Create a Route to an AppleTalk Site	Set / Define AppleTalk Route, page 13-61.	`DEFINE PROTOCOLS APPLETALK ROUTE "Doc Zone" "applelan" 4 155 162`	Creates a four-hop route to site *applelan* of zone *Doc Zone*, which has a network range of 155 to 162. See *LAN to LAN Connections* on page 7-5 for more information.

LAN to LAN Networking, cont.

To	Use This Command	Example(s)	What Example Does
View Configured Routes to AppleTalk Sites	Show / Monitor / List AppleTalk Routes, page 13-147.	`LIST APPLETALK ROUTES`	Displays the configured routes to AppleTalk sites that will be in effect after the next reboot. See *LAN to LAN Connections* on page 7-5 for more information.
Remove an AppleTalk Route	Clear / Purge AppleTalk Routes, page 13-4.	`CLEAR APPLETALK ROUTE ALL`	Removes all configured LRS routes to AppleTalk sites.
		`CLEAR APPLETALK ROUTE NET 155`	Removes all configured LRS routes to sites associated with this network (the network that has 155 as the low network number in its network number range). See *LAN to LAN Connections* on page 7-5 for more information.

Remote Node Networking

To	Use This Command	Example(s)	What Example Does
Create a Remote Node AppleTalk Site	Define Site AppleTalk, page 13-31.	`DEFINE SITE "incoming" APPLETALK ENABLED APPLETALK ROUTING DISABLED`	Creates a site called *incoming*, and disables AppleTalk routing to make the site remote node only. See *Remote Node Connections* on page 7-6 for more information.
Specify Connection Information for Dial-in Users	Set / Define AppleTalk Remote, page 13-60.	`DEFINE PROTOCOLS APPLETALK REMOTE "Public" 45`	Specifies that dial-in users will connect to a zone named *Public*, which has been allocated network number 45. See *Remote Node Connections* on page 7-6 for more information.

8 PPP

8 - PPP

PPP is the Point-to-Point Protocol. It is primarily used to transmit high layer protocols over a serial link, ISDN connection, or other point-to-point based connection. PPP supports authentication, escape sequences for flow control characters, loopback detection, and per-packet checksums.

8.1 LCP

The Link Control Protocol (LCP) is used to negotiate basic characteristics of the connection. These characteristics include packet size, header compression, control character escaping, and authentication mechanisms.

NOTE: *LCP is documented in RFCs 1661 and 1662.*

8.1.1 Packet Sizes

Both sides negotiate the size of packets each can receive. Packet size is also known as *Maximum Receive Unit* (MRU). The MRU need not be the same in each direction. The LRS MRU is 1522 bytes.

8.1.2 Header Compression

PPP frames each packet with certain data fields, some of which may be omitted or compressed (see **Define Ports PPP** on page 13-29 for details). PPP header compression is enabled by default on all LRS ports. To disable header compression, use the following command:

Figure 8-1: Disabling PPP Header Compression

```
Local>> DEFINE PORT 2 PPP HEADERCOMPRESSION DISABLED
```

8.1.3 Character Escaping

PPP can be configured to substitute a two byte sequence of characters for specific characters. The substituted characters are sent instead and the recipient translates them back into the original characters. This substitution is called **character escaping**.

Escaping characters is often used with XON / XOFF flow control. This method of flow control (used with many modems) involves treating two characters (hex 0x11 and hex 0x13) in a special manner.

Applications that use these characters (for example, certain text editors) may incorrectly trigger XON / XOFF flow control. If a user enters a Ctrl-S (hex 0x13) or Ctrl-Q (hex 0x11), these characters won't be transmitted; they'll be interpreted as flow control characters and removed from the data stream.

PPP can escape values between 0x00 and 0x1f (inclusive). To do this, PPP uses a 32-bit Asynchronous Character Control Map (ACCM). For each character to be escaped, that bit is set in hexadecimal format in the ACCM. For XON / XOFF flow control, the ACCM would be 0x000A0000.

NOTE: *The values 0x7d and 0x7e are always escaped.*

To escape a particular character, use the **Define Ports PPP ACCM** command. To automatically escape the XON / XOFF flow control characters, use the **XONXOFF** parameter. To escape all control characters, enter **0xffffffff** as the ACCM value. These options are all shown in Figure 8-2.

Figure 8-2: Escaping Characters

```
Local>> DEFINE PORT 2 PPP ACCM 0x000a0000
Local>> DEFINE PORT 2 PPP ACCM XONXOFF
Local>> DEFINE PORT 2 PPP ACCM 0xffffffff
```

If the port is set for XON / XOFF flow control, the XON / XOFF characters are automatically added to any configured ACCM.

8.1.4 Authentication

PPP supports two authentication methods, the Challenge Handshake Authentication Protocol (CHAP) and the Password Authentication Protocol (PAP). Both protocols involve a pre-assigned password.

8.1.4.1 CHAP

CHAP authentication begins with a challenge message from the unit trying to verify its peer. The peer receives the challenge, uses its password to encrypt the challenge, and responds. The authenticating unit then checks the response against what is expected, and either accepts or rejects the authentication attempt. At no time is the password transmitted over the link.

8.1.4.2 PAP

PAP, a simpler protocol, involves transmitting the username and password over the link in plain text. If the unit is authenticating to an unauthorized peer, the password could be compromised.

8.1.4.3 How CHAP and PAP Work

The LRS may be configured for authentication in one of three ways:

- Remote hosts must authenticate themselves
- The LRS authenticates itself to remote hosts
- Remote hosts and the LRS authenticate each other

PAP and CHAP may be enabled or disabled on each port and each site. If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the peer does not support CHAP, PAP will be attempted instead.

On incoming connections, the **port's** CHAP or PAP configuration will be used to determine the authentication required for the connection. For example, imagine that a remote node was logging into port 2 on the LRS. If port 2 was configured to use PAP to authenticate remote hosts, the remote node would be prompted to authenticate itself.

Outgoing connections use the **site's** CHAP or PAP configuration. For example, imagine that site **irvine** was initiating an outgoing connection to a remote router. If the remote site required the LRS to authenticate itself using CHAP and CHAP was enabled on site irvine, the LRS would offer its username and password to the remote site.

Care should be taken when using CHAP / PAP authentication because configuring both a local and a remote password on the same site could compromise security. If a site has both local and remote passwords defined and receives an incoming call, it will say during the LCP negotiation process that it is willing to transmit both passwords. It won't automatically transmit the passwords, but it will let the user know it is willing to do so if required. If the user requires the LRS to authenticate itself, the LRS will transmit the remote password over the link, and thereby give the user a password to access to the server.

NOTE: *For a complete description of authentication, refer to Chapter 12, Security.*

8.1.5 CBCP

The LRS supports the Microsoft Callback Control Protocol (CBCP) for dial-in PPP clients that request it. In conjunction with CBCP, the LRS may be configured to allow the PPP client to choose a dialback telephone number to reverse phone charges.

For more information, see *Dialback Using Callback Control Protocol (CBCP)* on page 12-6.

8.2 NCP

A Network Control Protocol (NCP) governs use of a specific network protocol over the PPP link. On the LRS, PPP can use three protocols over the link: IP, IPX, and AppleTalk.

8.2.1 IP Over PPP

PPP uses the IP Control Protocol (IPCP) to negotiate the use of IP over a link. IPCP allows for dynamic address assignment and Van Jacobson TCP header compression.

NOTE: *IP over PPP is described in RFC 1332. Van Jacobson TCP compression is covered in RFC 1144.*

During the negotiation process, if the LRS receives a request for more IP compression slots than are configured on the site (using the Define Site IP Slots command), the LRS will NAK (negative acknowledge), and request the number of slots configured on the site.

8.2.2 IPX Over PPP

PPP uses the IPX Control Protocol (IPXCP) to negotiate the use of IPX over a link. IPXCP allows for dynamic address assignment, compressed IPX (CIPX), and negotiation of a routing protocol.

NOTE: *IPX over PPP is described in RFC 1552. CIPX is described in RFC 1553.*

During the negotiation process, if the LRS receives a request for more IPX compression slots than are configured on the site (using the Define Site IPX Slots command), the LRS will NAK (negative acknowledge), and request the number of slots configured on the site.

8.2.3 AppleTalk over PPP

PPP uses the AppleTalk Control Protocol (ATCP) to negotiate the use of AppleTalk over a link.

NOTE: *AppleTalk over PPP is described in RFC 1378.*

8.3 Starting PPP

PPP can be started in a number of ways. For a detailed discussion of the PPP startup sequence, see *Incoming LAN to LAN and Remote Node* on page 3-9 and *Outgoing LAN to LAN Connections* on page 3-9.

8.3.1 User-initiated PPP

If PPP is enabled for a port, a user can start a PPP session from Local> mode using the **Set PPP** command on page 13-124. The user can specify a site to connect to by appending the site name to the command.

8.3.2 Automatic Detection of PPP

A port may be configured to automatically detect a PPP packet and, if PPP is enabled on the port, run PPP when the packet is received. This eliminates the need for callers to explicitly start PPP.

To enable this PPP autodetection feature, use the **Define Ports PPPdetect** command.

Figure 8-3: Enabling Automatic Protocol Detection

```
Local>> DEFINE PORT 2 PPPDETECT ENABLED
```

8.3.3 Dedicated PPP

If a port is dedicated to PPP (see *Preferred/Dedicated Services and Protocols* on page 9-7), the protocol runs automatically when the port is started. The autodetection setting is ignored.

8.3.4 Multilink PPP

When a port that is enabled for multilink PPP receives a multilink call and more bandwidth is needed for the connection, the LRS will add other ports, if available, to reach the necessary bandwidth.

For more information about Multilink connections, see *Configuring Multilink PPP*, next, and *Bandwidth On Demand* on page 4-9.

8.4 Configuring Multilink PPP

When an incoming PPP connection requires additional bandwidth, the LRS can add ports to the connection and combine the two or more physical streams of PPP data into one logical stream. This is called multilink PPP.

Two servers are needed for multilink PPP connections, one to initiate the call and one to receive it. All multilink packets for a given connection must originate from the LRS that brought up the link and be received by another single LRS. The following sections explain how to configure a calling LRS and a receiving LRS for a one-way multilink connection.

NOTE: *Multilink PPP is described in RFC 1990.*

8.4.1 Configuring the Calling LRS

1. Enable Multilink PPP on all ports that may be used for a multilink connection.

Figure 8-4: Enabling Multilink PPP

```
Local>> DEFINE PORT 1-4 PPP MULTILINK ENABLED
```

NOTE: *Ensure that other port parameters (such as speed, parity, and flow control) are properly configured for the connection.*

2. Create a site for the outgoing multilink PPP connection.

Figure 8-5: Creating the Calling Site

```
Local>> DEFINE SITE irvine
```

NOTE: *All other desired site parameters should be set up, and a static route should be defined for the site, before the site is used for connections.*

3. Configure the ports associated with the multilink site.

   A. Associate the site with two or more ports, giving each port a priority. Higher priority ports will be used first.

Figure 8-6: Configuring Port Priority

```
Local>> DEFINE SITE irvine PORT 1 PRIORITY 1
Local>> DEFINE SITE irvine PORT 2 PRIORITY 2
Local>> DEFINE SITE irvine PORT 3 PRIORITY 3
Local>> DEFINE SITE irvine PORT 4 PRIORITY 4
```

   B. Estimate the bandwidth of each port associated with the site.

      The estimate should be based on the fastest data transfer rate that the attached modem can support, adjusted for expected compression.

The following example assumes a 28.8 kbps modem attached to port 2 with about a 2:1 compression rate (28800 x 2 = 57600 bps = 5760 bytes per second, rounded to 5800 bytes per second).

Figure 8-7: Estimating Port Bandwidth

```
Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 5800
```

See *Estimating Each Port's Bandwidth* on page 4-10 for in-depth instructions on calculating bandwidth amounts.

C. Specify a telephone number for each port.

When the site is brought up, the LRS will attempt a connection by dialing the telephone number associated with the highest priority port (in this case, 555-1001).

Figure 8-8: Configuring Port Telephone Numbers

```
Local>> DEFINE SITE irvine PORT 1 TELEPHONE 555-1001
Local>> DEFINE SITE irvine PORT 2 TELEPHONE 555-1002
Local>> DEFINE SITE irvine PORT 3 TELEPHONE 555-1003
Local>> DEFINE SITE irvine PORT 4 TELEPHONE 555-1004
```

4. Configure the site bandwidth parameters.

NOTE: *The LRS will only modify bandwidth if it initiated the connection.*

A. Specify the initial and maximum bandwidths.

The maximum bandwidth should not exceed the sum of the bandwidths for all of the ports.

Figure 8-9: Configuring Initial and Maximum Bandwidths

```
Local>> DEFINE SITE irvine BANDWIDTH INITIAL 2800
Local>> DEFINE SITE irvine BANDWIDTH MAXIMUM 11500
```

For more information about site bandwidth settings and how to fine-tune them, see *Configuring Bandwidth Allocated to Sites* on page 4-10.

B. Specify when to add and remove bandwidth from a connection.

In the following example, the bandwidth should remain between 40% and 90% of the maximum value, 11500 bytes per second. The bandwidth will be measured every 60 seconds and compared to the add and remove values to see if an adjustment is necessary.

Figure 8-10: Configuring Site Bandwidth Settings

```
Local>> DEFINE SITE irvine BANDWIDTH ADD 90
Local>> DEFINE SITE irvine BANDWIDTH REMOVE 40
Local>> DEFINE SITE irvine BANDWIDTH PERIOD 60
```

5. Configure site authentication.

   All of the ports raised for a multilink connection should be added to the connection and authenticated together. A username and remote authentication password will be needed, and CHAP and / or PAP authentication should be enabled.

Figure 8-11: Configuring Site Authentication

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME “sidney”
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE “k0ala”
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE irvine AUTHENTICATION PAP ENABLED
```

8.4.2 Configuring the Receiving LRS

1. Configure the ports that will be used for the multilink connection.

   A. Enable Multilink PPP on all ports that will be used.

Figure 8-12: Enabling Multilink PPP

```
Local>> DEFINE PORT 1-4 PPP MULTILINK ENABLED
```

   B. Ensure that the telephone numbers of the modems attached to the receiving ports match those configured in the calling site.

   C. Enable PPP CHAP and / or PAP authentication on the ports.

Figure 8-13: Enabling PPP Authentication

```
Local>> DEFINE PORT 1-4 PPP CHAP REMOTE
Local>> DEFINE PORT 1-4 PPP PAP REMOTE
```

2. Create a site to receive the multilink traffic.

   The site’s name must match that of the incoming multilink user (see Figure 8-11).

Figure 8-14: Creating the Receiving Site

```
Local>> DEFINE SITE “sidney”
```

3. Configure site authentication.

   A local authentication password will be needed (it should match the incoming site’s remote password, see Figure 8-11), and CHAP and / or PAP authentication should be enabled.

Figure 8-15: Configuring Site Authentication

```
Local>> DEFINE SITE sidney AUTHENTICATION LOCAL “k0ala”
```

NOTE: *Be sure to use the same authentication protocol on the receiving LRS as on the calling LRS.*

8.5 Restoring Default PPP Settings

To restore a port to its default PPP settings, enter the **Purge Port PPP** command:

Figure 8-16: Restoring Default PPP Settings

```
Local>> PURGE PORT 2 PPP
```

8.6 Troubleshooting

The LRS event logging feature enables you to monitor network and user activity and troubleshoot problems. Configure a destination for logging information using the **Set/Define Logging Destination** command, described on page 13-96.

To view PPP LCP and NCP negotiations with the remote host, use logging level 4 or 6. Level 4 logs PPP negotiation activity, and is adequate for most PPP troubleshooting. Level 6 logs all PPP events; this is generally only required to troubleshoot faulty PPP implementations.

Figure 8-17: Enabling PPP Event Logging

```
Local>> DEFINE LOGGING PPP 4
```

Once a connection is made, problems may be monitored using the **Show Port Counters** command. The following table explains the counters useful for PPP troubleshooting:

Table 8-1: Port Counters

Counter(s)	Information Displayed
Packets Input	Packets from the remote host to the LRS.
Packets Output	Packets from the LRS to the remote host.
Packet Too-Longs	Number of packets longer than the Maximum Receive Unit (MRU) negotiated with LCP. In most situations, this counter will be 0. To correct this error, the remote node should configure a smaller Maximum Transmission Unit (MTU).
Bad FCS (Frame Checksum)	Number of corrupted packets. This problem may be due to line noise, flow control problems, and so on. This number should be less than 1% of the Packets Input counter; if it is not, performance is suffering greatly.

8.7 Quick Reference

Authentication			
To	**Use This Command**	**Example(s)**	**What Example Does**
Configure PAP / CHAP Authentication	See *Incoming Authentication* on page 12-1 and *Outgoing LAN to LAN Authentication* on page 12-17.		
Character Escaping			
To	**Use This Command**	**Example(s)**	**What Example Does**
Configure Character Escaping for XON / XOFF Flow Control	Define Ports PPP ACCM, page 13-28.	`DEFINE PORT 2 PPP ACCM XONXOFF`	When PPP is run on port 2, the XON / XOFF flow control characters will be escaped. See *Character Escaping* on page 8-1 for more information.
Header Compression			
To	**Use This Command**	**Example(s)**	**What Example Does**
Enable / Disable PPP Header Compression	Define Ports PPP HeaderCompression, page 13-29.	`DEFINE PORT 2 PPP HEADERCOMPRESSION DISABLED`	Disables compression of PPP headers on port 2. See *Header Compression* on page 8-1 for more information.

Starting PPP

To	Use This Command	Example(s)	What Example Does
Configure the PPP Startup Sequence	See *Incoming LAN to LAN and Remote Node* on page 3-9 or *Outgoing LAN to LAN Connections* on page 3-13.		
Configure a Port to Detect and / or Run PPP Automatically	See *Automatic Protocol Detection* and *Preferred/Dedicated Services and Protocols* on page 9-7 for more information.		

Restoring Default Settings

To	Use This Command	Example(s)	What Example Does
Restore the Default PPP Settings for a Port	Purge Port PPP, page 13-54.	`PURGE PORT 2 PPP`	Removes any user-configured PPP settings from port 2.

9 Ports

9 - Ports

Each LRS port can be configured in a number of ways. Configuration options include a port's start method, available sessions, services, access, serial parameters, and flow control.

9.1 Using Port Commands

Most port commands require you to be the privileged user. To become the privileged user, use the **Set Privileged/Noprivileged** command. This command is discussed in detail on page 13-124.

Many port commands require that Define commands be used instead of Set commands. Set commands take effect immediately for the current session. Define commands do not take effect until the port is logged out (with the Logout Port command) or the server is rebooted.

NOTE: *For a more detailed explanation of the difference between Set and Define commands, see Set and Define on page 2-3.*

If you're entering a number of commands at once, you may wish to enable the Command Completion characteristic. When Command Completion is enabled, the LRS will complete partially-typed commands when the Space or Tab keys are pressed. This can save time and reduce errors if you're entering a number of commands.

Command Completion is disabled by default. To enable it, use the following command:

Figure 9-1: Enabling Command Completion

```
Local>> DEFINE PORT COMMAND COMPLETION ENABLED
```

9.2 Accessing a Port

A port's access may be set to one of the following: dynamic, local, remote, or none. **Dynamic** (the default) permits both local and remote logins, **local** permits only local logins, and **remote** permits only remote logins. **None** prevents all incoming and outgoing connections, rendering the port unusable.

Before a user can Telnet from the network to an LRS port and dial out using an attached modem, the port must have dynamic or remote access. Before a user can log into a port locally and Telnet to a remote host, the port must have local or dynamic access.

To configure access to a port, use the **Set/Define Ports Access** command.

Figure 9-2: Configuring Connection Type

```
Local>> DEFINE PORT 2 ACCESS LOCAL
```

9.3 Starting a Port

When the LRS is booted, the ports can start up in one of two ways: they can automatically start, or wait for character input. Each port can be individually configured; for example, one port may wait for character input before starting, while another may automatically start when the LRS is booted.

A port's start-up procedure may involve a combination of factors. For example, if modem control is enabled, the port will wait until the modem asserts the DSR signal, then it could either automatically start, or wait for character input before starting (depending on the port configuration).

9.3.1 Automatic Start-up

A port can be configured to automatically start up when the LRS is booted. This is controlled by the **Autostart** setting; when Autostart is enabled, the port will start up and execute any configured commands or connections. (No user input or serial data is necessary for the port to start up; it will occur automatically.)

To enable **Autostart**, use the following command.

Figure 9-3: Enabling Autostart

```
Local>> DEFINE PORT 2 AUTOSTART ENABLED
```

Once Autostart is enabled, the port will start up automatically without waiting for character input. The port will then perform any operations that it's configured to run at start-up. For example, the port may connect to a particular host or service, run an authentication sequence, or run a particular protocol.

NOTE: *To dedicate a port to a host or service, see Preferred/Dedicated Services and Protocols on page 9-7.*

If PPP is enabled on the port, it will start when a PPP packet is received. See *PPP Mode* on page 9-3 for details. If both Autostart and modem control are enabled, the port will start as soon as the DCD signal is raised.

9.3.2 Waiting For Character Input Before Starting

By default, each LRS port will be idle until character input is received (for example, a Return key pressed at the remote node). If the LRS detects that the packet is a PPP or SLIP character and automatic protocol detection and the protocol are enabled (see *Automatic Protocol Detection* on page 9-4), the appropriate protocol will run.

In order for a port to wait for character input before starting, Autostart must be disabled. If Autostart is enabled, disable it using the **Set/Define Ports Autostart** command.

Figure 9-4: Disabling Autostart

```
Local>> DEFINE PORT 2 AUTOSTART DISABLED
```

9.4 Port Modes

An LRS port can be used in one of three **modes**: character mode, PPP mode, or SLIP mode. By default, the LRS will wait for character input before starting ports, then when the Return or Line Feed key is pressed, the ports will be in character mode. To configure a port to run PPP or SLIP, see the corresponding sections below.

NOTE: *Enabling PPP or SLIP on the LRS serial console port is not recommended.*

9.4.1 Character Mode

By default, the LRS ports will start character mode when the Return or Line Feed key is pressed at startup. When a port is in character mode, the Username> prompt is displayed. Once it is entered, users will see the Local> prompt. LRS commands can be entered at this prompt to configure the unit, control logins, Telnet or Rlogin to remote hosts, start PPP or SLIP, or display information.

NOTE: *For information on Telnet or Rlogin, see Sessions on page 9-4.*

9.4.2 PPP Mode

When a port is in PPP mode, it is running the Point-to-Point Protocol. A port can be configured to run PPP in a number of ways; for example, users can be authenticated, headers can be compressed, and negotiation can take place. Because PPP isn't designed for user interaction (the user isn't entering LRS commands), the Local> prompt will not be displayed.

When PPP and PPPdetect (see *Automatic Protocol Detection* on page 9-4) are enabled on a port, PPP will automatically run once a port's startup procedure (for example, waiting for character input) is complete and a PPP packet is received. Running PPP in this manner bypasses a port's usual authentication (using a login password or username / password combination); therefore CHAP or PAP authentication should be used.

To enable a port to run PPP, use the **Define Ports PPP** command.

Figure 9-5: Enabling PPP

```
Local>> DEFINE PORT 2 PPP ENABLED
```

NOTE: *For more information on PPP, refer to Chapter 8, PPP.*

9.4.3 SLIP Mode

When SLIP (Serial Line Internet Protocol) and SLIPdetect (see *Automatic Protocol Detection*, next) are enabled on a port, SLIP will run once a port's start-up procedure is complete.

Running SLIP in this manner bypasses a port's usual authentication process (login password, etc). As SLIP doesn't support authentication, no authentication will occur in this situation. To use authentication with SLIP, see Chapter 12, *Security*.

To enable a port to run SLIP, use the following commands:

Figure 9-6: Enabling SLIP

```
Local>> DEFINE PORT 2 SLIP ENABLED
```

9.5 Automatic Protocol Detection

An LRS port may be configured to automatically detect a PPP or SLIP packet and (if PPP or SLIP is enabled on the port) run the appropriate protocol when the packet is received. This eliminates the need for callers to explicitly start PPP or SLIP.

In some situations, autodetection should be disabled. For example, SLIP doesn't support authentication. To authenticate users, autodetection of SLIP could be disabled; incoming callers would be presented with the Local> prompt and could be forced to enter the login password. Once authenticated, they could manually start SLIP by entering the **Set SLIP** command.

NOTE: *To configure SLIP authentication, see Chapter 12, Security*

To enable PPP autodetection, use the **Define Ports PPPdetect** command. Automatic detection of SLIP is configured with the **Set/Define Ports SLIPdetect** command.

Figure 9-7: Enabling Automatic Protocol Detection

```
Local>> DEFINE PORT 2 PPPDETECT ENABLED
Local>> DEFINE PORT 3 SLIPDETECT ENABLED
```

If a port is dedicated to PPP or SLIP (see *Preferred/Dedicated Services and Protocols* on page 9-7), the protocol will run automatically when the port is started. The autodetection setting will be ignored.

9.6 Sessions

When you log into an LRS port to connect to a network service, your connection is referred to as a **session**. A network service may be an interactive login to a TCP/IP host, a connection to a modem on the LRS, another server, etc. (Sessions describe interactive connections; PPP or SLIP connections are not referred to as sessions.)

Session configuration may apply only to the current session, or to all sessions run on a particular port. Session-specific configuration meets needs that apply only to an active session; for example, if binary files were being transferred, interpretation of the switch characters, XON/XOFF flow control characters, and messages could be disabled.

NOTE: *Only one session at a time will be displayed.*

Port-specific session configuration includes the number of sessions permitted on a port, the keys used to switch between sessions, and the key used to exit from a session to character mode. The commands used to configure these options are discussed in the following sections.

9.6.1 Multiple Sessions

Each port may have a number of sessions running at once. By default, each port is configured to permit up to 4 simultaneous sessions. The maximum number of simultaneous sessions, called the **session limit**, may be changed; up to 8 sessions may be run on each port.

To change the session limit, use the **Set/Define Ports Session Limit** command.

Figure 9-8: Changing Session Limit

```
Local>> DEFINE PORT 2 SESSION LIMIT 6
```

9.6.2 Switching Between Sessions

Sessions are organized in the order that they were created. Commands or keyboard equivalents are used to switch back and forth between active sessions. Switching to a session with an earlier creation date is called switching backward; conversely, switching to a later session is called switching forward. Sessions are arranged in a circular list; switching forward from the last session created will switch to the first session in the list, and vice-versa.

The command used to switch to the previous session is **Backwards**. Its keyboard equivalent is called the **backward switch**. To define a backward switch, use the following command:

Figure 9-9: Defining Backward Switch

```
Local>> DEFINE PORT 2 BACKWARD SWITCH ^O
```

The **Forwards** command is used to switch to the next session. Its keyboard equivalent, the **forward switch**, is specified as follows:

Figure 9-10: Specifying Forward Switch

```
Local>> DEFINE PORT 2 FORWARD SWITCH ^N
```

The backward switch and forward switch characters should not conflict with each other or with characters used for editing commands (see *Entering and Editing Commands* on page 2-2). In addition, the characters should not conflict with characters used on the host.

9.6.3 Exiting Sessions

The Break key is used to suspend a session. When a session is suspended or exited, the Local> prompt will be displayed. LRS commands can be entered at this prompt to configure the unit, start a new session, or display information.

9.6.3.1 Break Key Equivalent

If your keyboard doesn't have a Break key, an equivalent can be specified with the **Set/Define Ports Local Switch** command.

Figure 9-11: Specifying Local Switch

```
Local>> DEFINE PORT 2 LOCAL SWITCH ‘
```

When the Break key is pressed, the port will do one of three things: suspend the session and display the Local> prompt, pass the character to the remote service, or ignore it all together (pressing the key will have no result).

To configure the processing of the Break key, use the **Set/Define Ports Break** command. Break can be set to one of the following: Local, Remote, or Disabled.

Figure 9-12: Configuring Break Key Processing

```
Local>> DEFINE PORT 3 BREAK LOCAL
```

9.6.3.2 Disconnecting Sessions

To disconnect the current session, use the **Disconnect** command. To disconnect a particular session, specify the session number; to disconnect all sessions, use the All parameter.

Figure 9-13: Disconnecting Sessions

```
Local>> DISCONNECT
Local>> DISCONNECT SESSION 2
Local>> DISCONNECT ALL
```

9.6.4 Monitoring Session Activity

When the **Verification** characteristic is enabled, messages will be issued whenever a session on that port is connected, disconnected, or switched. Use the following command to enable this characteristic:

Figure 9-14: Enabling Verification

```
Local>> DEFINE PORT 3 VERIFICATION ENABLED
```

9.6.5 Setting Session Characteristics

There are two ways to configure sessions: when a connection is made, or from within the connection once it is running.

9.6.5.1 Configuring a Session When a Connection is Made

To configure a session when a connection is made, an **environment string** may be specified. This string may be used in conjunction with the Connect command, or saved as part of a preferred or dedicated hostname. The environment string consists of a series of key letters, some prefaced by a plus (+) or minus (-):

Table 9-1: Key Letter for Environment Strings

Letter	Environment(s)	
D	+D = Backspace mode	-D = Delete mode
E	+E = Local Echo mode	-E = Remote Echo mode
I	I = Interactive mode	
P	+P = Passall mode	-P = Passthru mode
C	+C = CR = CRLF,	-C = CR = LF
T	TCP mode (i.e. uninterpreted data stream)	
R	Rlogin protocol (sets port # to 513 if not already set)	
Q	Queued (i.e. RTEL) connection	
nnn	Optional port number	

NOTE: *Key letters are not case-sensitive, and white space is not permitted in environment strings.*

To use an environment string with the **Connect** command, specify the host, TCP port, or service to connect to, then specify the environment string prefaced by a colon. For example, to Telnet to host athena in Backspace and Passall mode, use the following command:

Figure 9-15: Using Environment String with Connect

```
Local>> CONNECT TELNET athena:+D+P
```

To set an environment string to use with a preferred or dedicated host/service, use the following syntax:

Figure 9-16: Using Environment String with Preferred/Dedicated Host

```
Local>> DEFINE PORT 2 DEDICATED RLOGIN athena:480+E
```

NOTE: *For more information on preferred and dedicated hosts/services, see Preferred/Dedicated Services and Protocols on page 9-7.*

9.6.5.2 Configuring a Session Once it's Running

The **Set Session** command enables users to configure a currently-running session. Areas that may be configured include:

- The character sent as the delete character
- Local echoing
- LRS interpretation of messages and server-specific keys
- The character sent to the remote device when the Return key is pressed
- LRS interpretation of switch characters, messages, and flow control

For the complete syntax of the Set Session command, see *Set Session* on page 13-144.

9.7 Preferred/Dedicated Services and Protocols

9.7.1 Preferred Services

A **preferred service** is the default service (Telnet or Rlogin) for a particular port. If you use the Connect command without specifying a service, you'll be connected to the preferred service. A port can be configured to automatically connect to the preferred service upon login; this option is called Autoconnect.

To specify a preferred service, use the **Set/Define Ports Preferred** command.

Figure 9-17: Specifying a Preferred Service

```
Local> DEFINE PORT 2 PREFERRED SERVICE lrs_modem
```

The preferred service will be used with the Connect command whenever a service isn't specified.

To automatically connect to the preferred service upon login to the port, the Autoconnect characteristic must be enabled. Use the following command:

Figure 9-18: Enabling Autoconnect

```
Local>> DEFINE PORT 3 AUTOCONNECT ENABLED
```

9.7.2 Dedicated Services

A **dedicated service** is a service to which a port will always connect. When a port is associated with a dedicated service (referred to as "dedicating a port"), the port cannot be used to connect to any other service. A connection to the dedicated service will automatically be started upon login to the port; when the user logs out of the service, he will be logged out of the LRS.

To specify a dedicated service, use the **Define Ports Dedicated** command.

Figure 9-19: Specifying a Dedicated Service

```
Local>> DEFINE PORT 2 DEDICATED lrs_modem
```

The dedicated service will be connected upon login to the port. When the user logs out of the service (or the service cannot be reached for some reason), the user will be logged out of the LRS.

9.7.3 Dedicated Protocols

A **dedicated protocol** is a protocol (PPP or SLIP) that will automatically run when a port is started. No other protocol can be run on the port; it will continue to run PPP or SLIP until it is logged out.

To dedicate a port to PPP or SLIP, use the following command:

Figure 9-20: Dedicating a Port to PPP / SLIP

```
Local>> DEFINE PORT 2 PPP DEDICATED
Local>> DEFINE PORT 3 SLIP DEDICATED
```

When a port is dedicated, the local prompt cannot be accessed, therefore, commands can't be entered to disable the Dedicated characteristic. Caution should be used when dedicating ports; if you're going to dedicate all LRS ports, be sure that you have another way to log into the server (for example, a Telnet login).

NOTE: *If you cannot log into the LRS, you'll need to restore the server to its factory default settings. See Initialize Server on page 13-50.*

9.7.4 Preferred/Dedicated Telnet Hosts

A preferred or dedicated Telnet host can be specified using the **Set/Define Ports Preferred Telnet** and **Define Ports Dedicated Telnet** commands.

Figure 9-21: Specifying a Preferred / Dedicated Telnet Host

```
Local>> DEFINE PORT 2 PREFERRED TELNET 192.75.1.0
Local>> DEFINE PORT 3 DEDICATED TELNET 192.0.1.221
```

By entering a sequence of key letters after the Telnet parameter, **Set/Define Ports Preferred** can be used to configure the connection environment before a session is started. TCP, Rlogin, RTEL, or a port number can be specified.

9.8 Port Restrictions

Ports may be restricted in a number of ways. These methods include locking a port, username / password protection, restriction of connection type, automatic logouts, control of session interruption, restriction of commands, and receipt of broadcast messages.

9.8.1 Locking a Port

The **Lock** command may be used to secure a port without disconnecting sessions. When Lock is entered, the user will be prompted to enter a password. The port will then be locked until this password is used to unlock it.

Figure 9-22 displays an example.

Figure 9-22: Locking and Unlocking a Port

```
Local> LOCK
Password> donut (not echoed)
Verification> donut (not echoed)
Unlock password> donut (not echoed)
Local>
```

NOTE: *Secure ports (set using the Set/Define Ports Security command) cannot be locked.*

To unlock a port without the Lock password, a privileged user must use the **Unlock Port** command or log out the port using the **Logout** command. Logout will disconnect all sessions.

NOTE: *Unlock Port is discussed on page 13-166. Logout is discussed on page 13-51.*

The **Set/Define Server Lock** command controls whether or not local users are permitted to lock ports. For information on this command, see page 13-129.

9.8.2 Preventing Access Until DSR is Asserted

The Signal Check characteristic can be used to prevent remote connections to a port unless DSR is asserted. This is often used to prevent Telnet logins to a port until the device attached to the port (for example, a terminal) asserts the DSR signal, indicating that it is connected and powered on.

To enable Signal Check, use the following command:

Figure 9-23: Enabling Signal Check

```
Local>> DEFINE PORT 3 SIGNAL CHECK ENABLED
```

9.8.3 Username/Password Protection

Before a login is permitted, ports can be configured to require either a login password or a username / password pair stored in an authentication database.

NOTE: *For detailed information on authentication, refer to Chapter 12, Security.*

9.8.3.1 Login Password

The **Set/Define Ports Password** command controls whether or not the login password is required to log into the specified port. To require the password, use the following command:

Figure 9-24: Requiring Login Password

```
Local>> DEFINE PORT 2 PASSWORD ENABLED
```

By default, incoming Telnet and Rlogin connections are not required to enter a login password. To require the login password, use the **Set/Define Server Incoming** command (see page 13-128). The login password is set with the **Set/Define Server Login Password** command (see page 13-129).

NOTE: *Set/Define Server Incoming can also be used to require passwords for virtual port logins.*

9.8.3.2 Username/Password Authentication

The **Set/Define Ports Authenticate** command is used to authenticate individual users. When this command is enabled, incoming logins will be prompted for a username / password pair. The username and password entered will be compared to authentication databases configured with the Set / Define Authentication command. If a match is found, the login will be permitted; otherwise, the login attempt will fail.

Figure 9-25: Set / Define Port Authentication Command

```
Local>> DEFINE PORT 3 AUTHENTICATE ENABLED
```

NOTE: *Set/Define Authentication is described in Chapter 12, Security.*

9.8.4 Automatic Logouts

When a device connected to the LRS is disconnected or powered off, the DSR signal is dropped. The LRS can be configured to automatically log out a port when this occurs to prevent users from accessing other sessions by physically switching terminal cables and using someone else's privileges. Ports can also be configured to automatically log out when they've been inactive for a specified period of time.

9.8.4.1 DSR Logouts

To configure a port to log out when the DSR signal is dropped, use the **Set/Define Ports Dsrlogout** command.

Figure 9-26: Enabling Dsrlogout

```
Local>> DEFINE PORT ALL DSRLOGOUT ENABLED
```

9.8.4.2 Inactivity Logouts

To configure a port to log out after a specified period of inactivity, use the **Set/Define Ports Inactivity Logout** command. This command works in conjunction with the **Set/Define Server Inactivity** command. The latter defines a particular number of minutes; after this period of time, a port with Inactivity Logout enabled will be considered inactive and automatically logged out.

NOTE: *Set/Define Server Inactivity is described on page 13-127.*

To enable Inactivity Logout, use the following command:

Figure 9-27: Enabling Inactivity Logout

```
Local>> DEFINE PORT 3 INACTIVITY LOGOUT ENABLED
```

The LRS will only perform an inactivity logout when a port is in character mode (not running PPP or SLIP). To configure idle time logouts for PPP and SLIP connections, you must configure an idle time for the site; after the site is idle for the specified time, the link will be shut down. Use the **Define Site Idle** command and specify the length of the idle time limit in seconds.

Figure 9-28: Enabling Idle Time Logouts for PPP / SLIP

```
Local>> DEFINE SITE irvine IDLE 60
```

9.8.5 Restriction of Commands

The Security characteristic may be used to limit a user's access to information about other ports. When Security is enabled, only a limited number of commands may be typed at the Local> prompt.

To enable Security on a particular port, use the **Set/Define Ports Security** command.

Figure 9-29: Enabling Security

```
Local>> DEFINE PORT 3 SECURITY ENABLED
```

9.8.6 Receipt of Broadcast Messages

The **Set/Define Ports Broadcast** command enables or disables a port's receipt of broadcast messages from other users, including the superuser. Figure 9-30 displays an example.

Figure 9-30: Enabling Broadcast Messages

```
Local>> DEFINE PORT 3 BROADCAST DISABLED
```

9.9 Serial Configuration

There are a number of configurations that apply specifically to serial transmission. These configurations are a port's parity, baud rate, and bits per character. The bits per character is set using the **Set/Define Ports Character Size** command, described on page 13-109. **Set/Define Ports Parity** (page 13-115) sets a port's parity, and **Set/Define Ports Speed** (page 13-120) sets the baud rate.

NOTE: *Use of these commands is relatively straightforward. Please refer to the designated page references for the appropriate syntax.*

9.10 Flow Control

Flow control enables two connected devices to control the amount of data transmitted between them. When flow control is enabled on an LRS port and a connected device (for example, a modem), flow control ensures that data sent from the sending device does not overflow the receiving device's buffers. Consider the following example.

An LRS port is connected to a modem. The LRS port transfers data to the modem at 115,200 bits per second, but the modem can only send data over the phone line at 15,000-30,000 bits per second. In a short period of time, the modem's buffer fills with data. The modem sends a signal to the LRS to stop sending data, and the LRS does not send data until it receives a signal from the modem that it can receive data again.

9.10.1 LRS Flow Control Support

The LRS supports hardware and software flow control. The hardware flow control option is RTS / CTS and the option for software flow control is XON / XOFF. Both flow control methods are described below.

NOTE: *When the LRS is communicating with a device, the LRS and the device must agree on the type of flow control used.*

9.10.1.1 Hardware Flow Control

When hardware flow control is used, the flow of data is controlled by two serial port signals (typically RTS and CTS). Two connected devices will assert and deassert RTS and CTS to indicate when they are ready to accept data.

For example, the LRS will assert RTS when it is ready to accept data. When it can no longer accept data (its buffers are full) it will deassert this signal. A connected modem will monitor the assertion and deassertion of this signal; it will only send data when RTS is asserted.

A modem will assert CTS when it is ready to accept data. When its buffers are full, it will deassert CTS to indicate to the LRS that it should stop sending data. The LRS will only send data when CTS is asserted.

RTS / CTS is the most reliable method of flow control, and is the recommended method for the LRS. In the event that RTS / CTS flow control cannot be used, XON / XOFF flow control is recommended.

9.10.1.2 Software Flow Control

XON / XOFF controls the flow of data by sending particular characters through the data stream. The characters sent to signify the ability or inability to accept data are Ctrl-Q (XON) and Ctrl-S (XOFF).

Applications that use the Ctrl-Q and Ctrl-S characters (for example, certain text editors) will conflict with XON / XOFF flow control. If a user enters a Ctrl-Q or Ctrl-S, these characters won't be transmitted; they'll be interpreted as flow control characters and removed from the data stream.

Protocols that require an 8-bit clean data path cannot use XON / XOFF flow control. Data passes through an 8-bit clean data path unchanged. SLIP and UUCP require an 8-bit clean data path; PPP may have the same requirements if the Asynchronous Character Control Map (ACCM) isn't set properly. To configure the ACCM, see Chapter 8, *PPP*.

9.10.2 Setting up Flow Control

To use flow control on an LRS port, complete the following steps.

1. Set Appropriate Line / Serial Speeds

   Consider the line speed and the serial speed of the modem; if data is being compressed, the serial speed should be set higher than the line speed. If you're connecting a terminal to the port, ensure that the speed of the terminal matches the port speed.

NOTE: *See Chapter 10, Modems, for a discussion of line speeds, serial speeds, and data compression. See your modem's documentation for information on configuring the modem's line and serial speeds.*

2. Disable Autobaud

   In order to ensure that the set speeds are always used, disable any automatic speed selection or autobaud options on your modem.

   In addition, disable autobaud on the LRS port you're configuring. To do this, use the **Set/Define Ports Autobaud** command. This command requires that you be a privileged user.

Figure 9-31: Disabling Autobaud

```
Local>> DEFINE PORT 2 AUTOBAUD DISABLED
```

NOTE: *If you aren't currently a privileged user, use the* **Set Privileged** *command.*

3. Determine the Appropriate Flow Control Method

   Refer to *Flow Control* on page 9-12 for a description of the different methods. Choose the method that's most compatible with the modem and applications you'll be using.

4. Configure Flow Control

   To configure your modem, refer to your modem's documentation.

   To configure flow control on the LRS, use the **Set/Define Ports Flow Control** command. Figure 9-32 displays an example.

Figure 9-32: Configuring RTS / CTS Flow Control

```
Local>> DEFINE PORT 2 FLOW CONTROL CTS
```

NOTE: *For the complete syntax of Set/Define Ports Flow Control, refer to page 13-111.*

9.11 Serial Signals

Two of the modem signals (DSR and DCD) can be used to control when the LRS ports are active. By monitoring when these signals are asserted or deasserted (dropped), LRS ports can be logged out or kept from starting. The LRS uses DTR to control attached devices.

All LRS DB25 and RJ45 signals are displayed in the following figures.

Figure 9-33: LRS DB25 Serial Signals

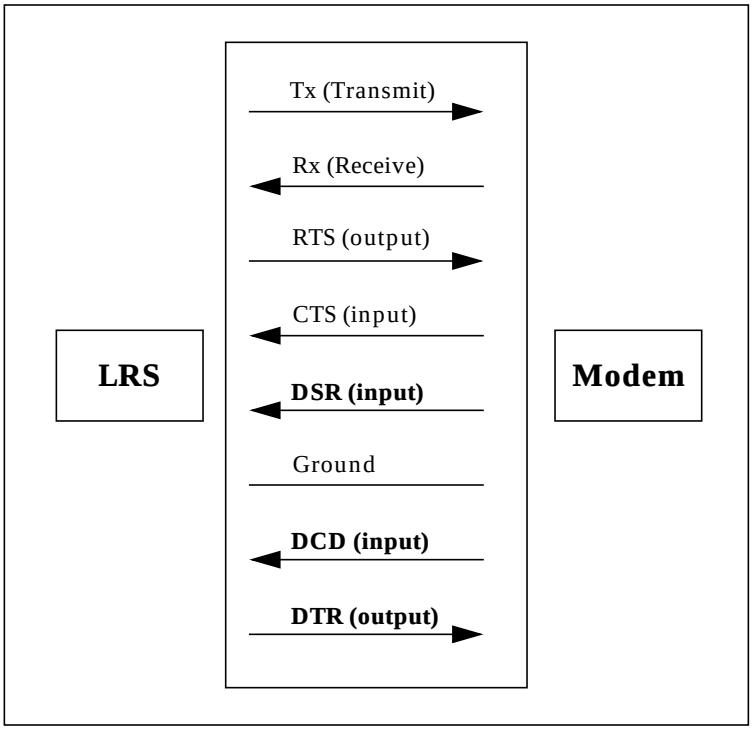
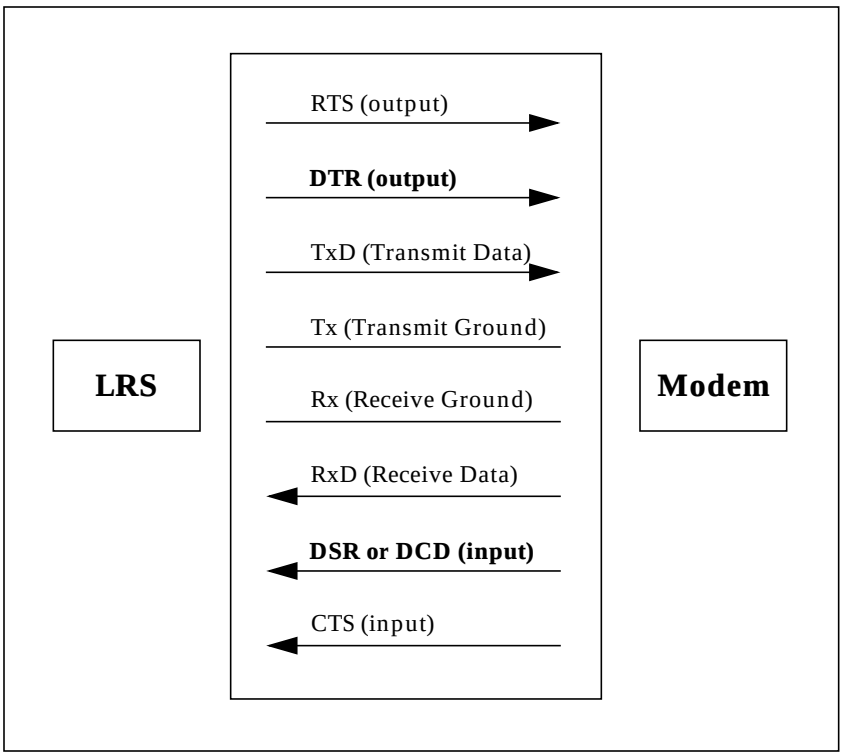


Figure 9-34: LRS RJ45 Serial Signals



9.11.1 DSR (Data Set Ready)

9.11.1.1 DSR for Automatic Logouts

An LRS port can be configured to automatically log itself out when DSR is no longer asserted; in other words, the port will log out when the modem is disconnected. This can help ensure port security; users will be prevented from unplugging terminal lines and using sessions that are still active. See *Automatic Logouts* on page 9-11 for more information.

9.11.1.2 DSR for Controlling Remote Logins

The DSR signal can also be used to determine whether or not a remote login to a port will be permitted. When enabled, the Signal Check characteristic will require the assertion of the DSR signal before a remote login is permitted on a particular port.

Signal Check is generally enabled for use with printers; if the printer doesn't assert the DSR signal, it's assumed to be disconnected or powered off. In this case, the remote login isn't permitted, and print jobs are not sent from the LRS to the printer.

To enable Signal Check, use the following command:

Figure 9-35: Enabling Signal Check

```
Local>> DEFINE PORT 3 SIGNAL CHECK ENABLED
```

9.11.2 DCD (Data Carrier Detect)

The DCD signal is asserted by the local modem when it detects a connection from a remote modem. If you're using a DB25 port, no wiring is required in order to use the DCD signal.

RJ45 ports have one pin that can be used for either DSR or DCD. If you are using modems, this pin must be wired to the modem's DCD pin. If you are using another type of device (such as a terminal or printer), this pin should be wired to the device's DSR pin. Refer to the *Pinouts* appendix of your Installation Guide for instructions.

9.11.3 DTR (Data Terminal Ready)

The LRS asserts DTR when it is ready to accept incoming data or connections. It also uses DTR to cycle the modem when modem control is enabled by temporarily dropping the signal.

LRS ports can be configured to assert DTR only when a user logs into the port by enabling the **Dtrwait** characteristic. See **Set/Define Ports Dtrwait** on page 13-111 for details.

9.12 Device Types

Communication devices (modems, printers, servers, etc.) are divided into two types: DTE (Data Terminal Equipment) and DCE (Data Communications Equipment). DTE and DCE are designed to work together, much as a male connector works with a female connector.

The LRS is a DTE device. Modems are DCE devices. This means that they use opposite signals; the LRS uses a particular signal to send data, and the modem uses that same signal to receive data.

Some devices that the LRS will connect to (such as printers) are DTE devices. Transmitting data between two DTE devices requires the use of a null modem cable to swap the signals; for complete wiring instructions, refer to the *Pinouts* appendix of your **Installation Guide**.

9.13 Controlling Modems

A number of Define Port commands are designed to control modems (for example, **Define Port Modem Answer**). These commands are covered in Chapter 10, *Modems*.

9.14 Restoring Default Port Settings

To restore all ports to their default settings, use the **Purge Port** command. Use caution with this command; any changes that you've made with Set and Define commands will be erased.

Figure 9-36: Restoring Default Port Settings

```
Local>> PURGE PORT 2
```

If the Purge Port command cannot be used (for example, authentication has been defined on all ports), the settings can only be restored by using the the Boot Configuration Program. See your **Installation Guide** for details.

9.15 Virtual Ports

Incoming Telnet and Rlogin connections are not associated with a physical port. Instead, they are associated with a **virtual port** which serves for the duration of the connection. Virtual port connections can be made only if incoming connections are enabled on the LRS.

Figure 9-37: Enabling Incoming Connections

```
Local>> DEFINE SERVER INCOMING TELNET
```

NOTE: *An incoming login password can also be configured with the Set/Define Server Incoming command. See page 13-128.*

Each virtual port is created with a default set of characteristics. The Set Port commands (beginning on page 13-104) can be used by the user to customize a virtual port during the Telnet / Rlogin session, but these customizations cannot be saved.

To make configurations that apply to all virtual ports (all future Telnet / Rlogin connections), use Define Port commands, specifying **port 0** as the port number. When the command in Figure 9-38 is used, all future network logins will be required to enter a username and password.

Figure 9-38: Configuring Virtual Ports

```
Local>> DEFINE PORT 0 AUTHENTICATION ENABLED
```

NOTE: *Port 0 cannot be configured using Set commands, only Define commands.*

Define Port 0 commands are often used to provide local switches to network logins, as they typically do not have a Break key to use after the connection is made. NCP and Telnet remote console sessions are considered virtual logins; configurations made with Define Port 0 commands will apply to these connections.

To display the characteristics used for virtual ports, enter the following command:

Figure 9-39: Displaying Virtual Port Characteristics

```
Local>> LIST PORT 0
```

9.15.1 Remote Console Port

The remote console port is a virtual port, designated as port 7000. This port is typically used when there isn't another way to telnet to the LRS (for example, Telnet logins are disabled), or when a consistent prompt is required. To Telnet to this port, use the **telnet** command, specifying the LRS IP address and 7000 as the port number.

NOTE: *For more information on the remote console port, see Remote Console Connections on page 5-9.*

The LRS will display the remote console port prompt (#). The login password must be entered at this prompt to successfully log into the port. The default login password is **access**. To change this password, see **Set/Define Server Login Password** on page 13-129.

9.16 Additional Port Settings

9.16.1 Autodetection of Port Characteristics

The **Autobaud** characteristic enables a port to detect an incoming baud rate, character size, and parity and configure its characteristics to match. This characteristic cannot be enabled if Access is set to Remote or Dynamic (page 9-1), or if the specified port offers a service.

9.16.2 Dialback

The Dialback feature allows a system manager to set up a dialback list of authorized users for incoming modem connections. When a username matching one in the list is entered, the port is logged out and the phone number will be sent out the serial port using the port's modem profile.

For a complete description of dialback, see *Dialback from Local Mode* on page 12-5.

9.16.3 Menu Mode

The **Set/Define Ports Menu** command controls whether the Local> prompt or a menu will be displayed upon login. To enable Menu mode, use the following command:

Figure 9-40: Enabling Menu Mode

```
Local>> DEFINE PORT 3 MENU ENABLED
```

When Menu mode is enabled, the Local> prompt cannot be accessed. Be sure that you have another way to log into the LRS before enabling Menu mode on all ports.

NOTE: *For a complete discussion of menu mode, see Menu Mode on page 12-20.*

9.16.4 Naming a Port

To assign a particular name to a port, use the **Set/Define Ports Name** command:

Figure 9-41: Assigning a Port Name

```
Local>> DEFINE PORT 3 PORT NAME “highspeed_modem”
```

The default name for each port is Port_*n*, where *n* denotes the port number (for example, Port_2).

9.16.5 Specifying a Username

A username can be specified for a port using the **Set/Define Ports Username** command. When the username is specified with the Define Port Username command, users will not be prompted for a username upon login. Figure 9-42 displays an example.

Figure 9-42: Specifying a Username

```
Local>> DEFINE PORT 3 USERNAME fred
```

9.16.6 Notification of Character Loss

When the **Loss Notification** characteristic is enabled, a bell character (Ctrl-G) will be sent when data error or overrun causes the loss of a character. Figure 9-43 displays an example.

Figure 9-43: Enabling Loss Notification

```
Local>> DEFINE PORT 2 LOSS NOTIFICATION ENABLED
```

9.16.7 Padding Return Characters

By default, the LRS will pad Carriage Returns entered in Telnet sessions with null characters. To disable this characteristic, use the **Set/Define Ports Telnet Pad** command.

Figure 9-44: Disabling Telnet Pad

```
Local>> DEFINE PORT 3 TELNET PAD DISABLED
```

9.16.8 PPP Commands

A number of Set / Define Port commands apply specifically to configuration of PPP (Point-to-Point Protocol). For information about these commands, refer to Chapter 8, *PPP*.

9.16.9 Setting the Device Type

The **Type** characteristic is used to specify the device types compatible with the port. Type must be one of the following device types: ANSI, Hardcopy, or Softcopy. To set a Type, use the following command:

Figure 9-45: Configuring the Device Type

```
Local>> DEFINE PORT 3 TYPE ANSI
```

NOTE: *For more information about Type options, refer to Set/Define Ports Type on page 13-122.*

9.16.10 Specifying a Terminal Type

A terminal type, to be sent to the remote host for Telnet and Rlogin sessions, can be specified for a port using the Set / Define Ports Telnet Pad command. The terminal type should be entered as a string, for example, VT100.

Figure 9-46: Specifying a Terminal Type

```
Local>> DEFINE PORT ALL TERMTYPE IBM1000
```

NOTE: *By default, no specific terminal type is specified.*

Termtype information is used for outbound sessions; the LRS doesn't use this information. For example, a remote host might use the terminal type to configure your terminal to run a particular application.

9.17 Quick Reference

Port Access			
To	**Use This Command**	**Example(s)**	**What Example Does**
Change a Port's Access	Set / Define Ports Access, page 13-104.	`DEFINE PORT 2 ACCESS DYNAMIC`	Permits incoming and outgoing connections on port 2. See *Accessing a Port* on page 9-1 for more information.
		`DEFINE PORT 2 ACCESS LOCAL`	Permits only local logins on port 2.
		`DEFINE PORT 2 ACCESS REMOTE`	Permits only remote logins on port 2.
		`DEFINE PORT 2 ACCESS NONE`	Prevents all incoming and outgoing connections on port 2.
Port Startup Procedure			
To	**Use This Command**	**Example(s)**	**What Example Does**
Configure a Port to Start Automatically When the LRS is Booted	Set / Define Ports Autostart, page 13-106.	`DEFINE PORT 2 AUTOSTART ENABLED`	Configures port 2 to automatically start when the unit is booted. See *Automatic Start-up* on page 9-2 for more information.
Configure a Port to Wait for Character Input Before Starting	Set / Define Ports Autostart, page 13-106.	`DEFINE PORT 2 AUTOSTART DISABLED`	Delays port 2's startup procedure until the port receives a character. See *Waiting For Character Input Before Starting* on page 9-2 for more information.

Running PPP/SLIP

To	Use This Command	Example(s)	What Example Does
Enable a Port to Run PPP / SLIP	Set Ports PPP, page 13-116.	`DEFINE PORT 2 PPP ENABLED`	Enables use of the Set PPP command on port 2. See *PPP Mode* on page 9-3 for more information.
	Set Ports SLIP, page 13-120.	`DEFINE PORT 2 SLIP ENABLED`	Enables use of the Set SLIP command on port 2. See *SLIP Mode* on page 9-3 for more information.
Automatically Run PPP / SLIP When a PPP / SLIP Packet is Received	Define Ports PPPdetect Enabled, page 13-30.	`DEFINE PORT 2 PPPDETECT ENABLED`	Port 2 will automatically run PPP when it receives a PPP packet. See *Automatic Protocol Detection* on page 9-4 for more information.
	Set / Define Ports SLIPdetect Enabled, page 13-120.	`DEFINE PORT 2 SLIPDETECT ENABLED`	Port 2 will automatically run SLIP when it receives a SLIP packet. See *Automatic Protocol Detection* on page 9-4 for more information.

Sessions

To	Use This Command	Example(s)	What Example Does
Set the Maximum Number of Simultaneous Sessions on a Port	Set / Define Ports Session Limit, page 13-119.	`DEFINE PORT 2 SESSION LIMIT 6`	Up to 6 sessions may be simultaneously run on port 2. See *Multiple Sessions* on page 9-4 for more information.
Set the Key Used to Switch to the Previous Session	Set / Define Ports Backward Switch, page 13-107.	`DEFINE PORT 2 BACKWARD SWITCH ^B`	On port 2, pressing Ctrl-B will switch to the previous session. See *Switching Between Sessions* on page 9-5 for more information.
Set the Key Used to Switch to the Next Session	Set / Define Ports Forward Switch, page 13-112.	`DEFINE PORT 2 FORWARD SWITCH ^F`	On port 2, pressing Ctrl-F will switch to the next session. See page 9-5 for more information.
Specify a Break Key Equivalent	Set / Define Ports Local Switch, page 13-113.	`DEFINE PORT 2 LOCAL SWITCH ‘`	On port 2, pressing the apostrophe (‘) key will exit the current session. See *Break Key Equivalent* on page 9-5 for more information.
Control What the Break Key Does	Set / Define Ports Break, page 13-108.	`DEFINE PORT 2 BREAK LOCAL`	On port 2, pressing the Break key will suspend the current session and display the Local> prompt. See *Break Key Equivalent* on *page 9-5* for more information.
		`DEFINE PORT 2 BREAK REMOTE`	On port 2, when the Break key is pressed, the character will be passed to the remote service.
		`DEFINE PORT 2 BREAK DISABLED`	Pressing the Break key on port 2 will have no effect (the key is ignored).

Sessions, cont.

To	Use This Command	Example(s)	What Example Does
Issue Messages When a Session is Connected, Disconnected, or Switched	Set / Define Ports Verification, page 13-123.	`DEFINE PORT 2 VERIFICATION ENABLED`	When sessions on port 2 are connected, disconnected, or switched, a message will be issued. See *Monitoring Session Activity* on page 9-6 for more information.
Set Session Characteristics Before a Session is Started	See *Setting Session Characteristics* on page 9-6.		
Configure a Session Once it's Running	Set Session, page 13-144.	`SET SESSION DELETE BACKSPACE`	Sends a backspace character (ASCII 0x8, or Ctrl-H) when the Delete key is pressed. See *Configuring a Session Once it's Running* on page 9-7 for more information.

Preferred/Dedicated Services and Protocols

To	Use This Command	Example(s)	What Example Does
Specify a Preferred Service	Set / Define Ports Preferred, page 13-117.	`DEFINE PORT 2 PREFERRED SERVICE lrs_modem`	Specifies "lrs_modem" as port 2's default service. If the Connect command is used on port 2 and a service is not specified, the user will be connected to "lrs_modem". See *Preferred Services* on page 9-7 for more information.
Specify a Preferred Telnet Host	Set / Define Ports Preferred Telnet, page 13-117.	`DEFINE PORT 2 PREFERRED TELNET 192.75.1.0`	Specifies host 192.75.1.0 as port 2's default Telnet host. If the Connect command is used on port 2 and a service is not specified, the user will be telnetted to 192.75.1.0. See *Preferred/Dedicated Telnet Hosts* on page 9-9 for more information.

Preferred/Dedicated Services and Protocols, cont.

To	Use This Command	Example(s)	What Example Does
Automatically Connect to the Preferred Service / Host at Login	Set / Define Ports Autoconnect Enabled, page 13-106.	`DEFINE PORT 2 AUTOCONNECT ENABLED`	When users log into port 2, they will automatically be connected to the preferred service. See page 9-8 for more information.
Specify a Dedicated Service	Define Ports Dedicated, page 13-14.	`DEFINE PORT 2 DEDICATED lrs_modem`	When users log into port 2, they will automatically be connected to the "lrs_modem" service. If they log out of the service, they will be logged out of the LRS. See *Dedicated Services* on page 9-8 for more information.
Specify a Dedicated Protocol (PPP or SLIP)	Define Ports PPP Dedicated, page 13-28. or Define Ports SLIP Dedicated, page 13-31.	`DEFINE PORT 2 PPP DEDICATED`	When port 2 is started, it will automatically run PPP. Users will not be able to run SLIP or access the Local> prompt. See *Dedicated Protocols* on page 9-8 for more information.
Specify a Dedicated Telnet Host	Define Ports Dedicated Telnet, page 13-14.	`DEFINE PORT 5 DEDICATED TELNET hermes`	When users log into port 2, they will automatically be connected to host "hermes". If they log out of the host, they will be logged out of the LRS. See *Dedicated Protocols* on page 9-8 for more information.

Port Restrictions

To	Use This Command	Example(s)	What Example Does
Prevent Remote Connections to a Port Until the DSR Signal is Asserted	Set / Define Ports Signal Check, page -119.	`DEFINE PORT 2 SIGNAL CHECK ENABLED`	Remote connections may not be made to port 2 until the DSR signal is asserted. See *Preventing Access Until DSR is Asserted* on page 9-10 for more information.
Lock a Port	Set / Define Server Lock, page 13-129.	`LOCK`	Prompts for a "locking" password; when one is entered and confirmed, the port is locked. To unlock the port, this password must be entered. See *Locking a Port* on page 9-9 for more information.
Force Users to Enter a Login Password	1. Set / Define Server Login Password, page 13-129.	`DEFINE SERVER LOGIN PASSWORD "badger"`	Defines "badger" as the login password. See *Login Password* on page 9-10 or Chapter 12, *Security*, for more information.
	2. Set / Define Ports Password Enabled, page 13-116.	`DEFINE PORT 3 PASSWORD ENABLED`	Incoming callers on port 3 will be forced to enter the login password, "badger".
Force Telnet / Rlogin Users to Enter the Login Password	Set / Define Server Incoming Password, page 13-128.	`DEFINE SERVER INCOMING PASSWORD`	Incoming Telnet / Rlogin users will be required to enter the login password, "badger". See *Login Password* on page 9-10 for more information.

Port Restrictions, cont.

To	Use This Command	Example(s)	What Example Does

Force Users to Enter a Username / Password Pair Before PPP / SLIP Runs	1. Define Ports PPPdetect Disabled, page 13-30.
	
	or Set / Define Ports SLIPdetect Disabled, page 13-120.
		`DEFINE PORT 3 PPPDETECT DISABLED`
		
		`DEFINE PORT 3 SLIPDETECT DISABLED`
			Disables autodetection of PPP / SLIP on port 3.
			
			See *Automatic Protocol Detection* on page 9-4 for more information.

	2. Set / Define Ports Authenticate, page 13-104.	`DEFINE PORT 3 AUTHENTICATE ENABLED`	Incoming callers on port 3 will be forced to enter a username / password pair. This pair will be checked against any configured authentication databases. See *Username/Password Authentication* on page 9-10 or Chapter 12, *Security*, for more information.
Automatically Log Out a Port When the DSR Signal is Dropped	Set / Define Ports Dsrlogout Enabled, page 13-110.	`DEFINE PORT 2 DSRLOGOUT ENABLED`	When the DSR signal is dropped (deasserted), port 2 will be logged out. See *Automatic Logouts* on page 9-11 for more information.
Configure Port Inactivity Logouts	1. Set / Define Server Inactivity, page 13-127.	`DEFINE SERVER INACTIVITY LIMIT 15`	Sets a server-wide inactivity limit of 15 minutes. See *Inactivity Logouts* on page 9-11 for more information.
	2. Set / Define Ports Inactivity Logout, page 13-112.	`DEFINE PORT 2 INACTIVITY LOGOUT ENABLED`	Enables inactivity logouts on port 2. When port 2 is inactive for 15 minutes, the port will be logged out. Any active connections will be disconnected.
Permit Local Logins While a Network Connection is Running	1. Set / Define Ports Access Dynamic, page 13-104.	`DEFINE PORT 2 ACCESS DYNAMIC`	Permits incoming and outgoing connections on port 2. See *Accessing a Port* on page 9-1 for more information.

Port Restrictions, cont.

To	Use This Command	Example(s)	What Example Does
Restrict a User's Use of Commands	Set / Define Ports Security Enabled, page 13-118.	`DEFINE PORT 2 SECURITY ENABLED`	Users on port 2 will only be able to enter a limited number of commands at the Local> prompt. See *Restriction of Commands* on page 9-11 for more information.
Enable / Disable a Port's Receipt of Broadcast Messages	Set / Define Ports Broadcast Enabled / Disabled, page 13-108.	`SET PORT 2 BROADCAST DISABLED`	Blocks port 2's reception of broadcast messages. See *Receipt of Broadcast Messages* on page 9-12 for more information.

Flow Control

To	Use This Command	Example(s)	What Example Does
Set the Appropriate Line and Serial Speeds	See your modem's documentation or Chapter 10, *Modems*.		
Disable Autobaud	Set / Define Ports Autobaud Disabled, page 13-105.	`DEFINE PORT 2 AUTOBAUD DISABLED`	Disables Autobaud on port 2. See *Flow Control* on page 9-12 for more information.
Enable XON / XOFF or RTS / CTS Flow Control	Set / Define Ports Flow Control, page 13-111.	`DEFINE PORT 2 FLOW CONTROL CTS`	Enables RTS / CTS flow control on port 2.

Modem Signals

To	Use This Command	Example(s)	What Example Does
Automatically Log Out a Port When the DSR Signal is Dropped	Set / Define Ports Dsrlogout Enabled, page 13-111.	`DEFINE PORT 2 DSRLOGOUT ENABLED`	When the DSR signal is dropped (deasserted), port 2 will be logged out. See *Automatic Logouts* on page 9-11 for more information.
Require the Assertion of the DSR Signal for Remote Logins	Set / Define Ports Signal Check Enabled, page 13-119.	`DEFINE PORT 2 SIGNAL CHECK ENABLED`	Before remote connections to port 2 will be permitted, the DSR signal must be asserted. See *DSR (Data Set Ready)* on page 9-15 for more information.
Assert the DTR Signal Only When a User Logs Into a Port	Set / Define Ports Dtrwait, page 13-111.	`DEFINE PORT 2 DTRWAIT ENABLED`	On port 2, the DTR signal will not be asserted until a user logs into the port. See *DTR (Data Terminal Ready)* on page 9-16 for more information.
Control Modem Operation	See Chapter 10, *Modems*.		

Restoring Default Port Settings

To	Use This Command	Example(s)	What Example Does
Restore Default Port Settings	Purge Port, page 13-54.	`PURGE PORT 2`	Restores port 2's default settings. See *Restoring Default Port Settings* on page 9-16 for more information.
	Initialize Server Factory, page 13-50.	`INIT SERVER FACTORY DELAY 3`	Reboots the LRS and restores all of its default settings, including the port settings, after a delay of three minutes.

Miscellaneous Port Settings

To	Use This Command	Example(s)	What Example Does
Logout Current User / Make Port Commands Take Effect	Logout Port, page 13-51.	`LOGOUT PORT 2`	Stops the current session, logs out the current user, reloads configured settings from NVR (including any newly-defined commands), and readies the port for the next connection attempt.
Automatically Detect and Match the Incoming Baud Rate, Parity, and Character Size	1. Set / Define Ports Access Local, page 13-104.	`DEFINE PORT 2 ACCESS LOCAL`	Sets port 2's access to local. This is required in order to enable Autobaud.
	2. Set / Define Ports Autobaud Enabled, page 13-105.	`DEFINE PORT 2 AUTOBAUD ENABLED`	Port 2 will automatically detect and match the incoming baud rate, parity, and character size. See *Autodetection of Port Characteristics* on page 9-18 for more information.
Secure Ports Using Automatic Dialback	See *Dialback from Local Mode* on page 12-5.		
Display a Menu (Instead of the Local> Prompt) Upon Login	Set / Define Ports Menu Enabled, page 13-114.	`DEFINE PORT 2 MENU ENABLED`	When users log into port 2, a menu will be displayed (rather than the Local> prompt). See *Menu Mode* on page 9-18, *Menu Mode* on page 12-20, or Set / Define Menu on page 13-100 for more information.
Assign a Name to a Port	Set / Define Ports Name, page 13-115.	`DEFINE PORT 2 PORT NAME "highspeed_modem"`	Assigns the name "highspeed_modem" to port 2. See *Naming a Port* on page 9-18 for more information.

Miscellaneous Port Settings, cont.

To	Use This Command	Example(s)	What Example Does
Send a Character When an Error or Data Overrun Causes the Loss of a Character	Set / Define Ports Loss Notification Enabled, page 13-114.	`DEFINE PORT 2 LOSS NOTIFICATION ENABLED`	When a character is lost during a connection to port 2, a Ctrl-G character will be sent. See *Notification of Character Loss* on page 9-19 for more information.
Disable the Padding of Carriage Returns During Telnet Sessions	Set / Define Ports Telnet Pad Disabled, page 13-121.	`DEFINE PORT 2 TELNET PAD DISABLED`	Disables the padding of Carriage Returns on port 2. See *Padding Return Characters* on page 9-19 for more information.
Configure the Device Types Compatible With a Port	Set / Define Ports Type, page 13-122.	`DEFINE PORT 2 TYPE ANSI`	Specifies that port 2 is compatible with ANSI devices. See *Setting the Device Type* on page 9-19 for more information.
Specify a Default Username for a Port	Set / Define Ports Username, page 13-123.	`DEFINE PORT 2 USERNAME fred`	Defines “fred” as port 2’s default username. When users log into port 2, they will not be prompted to enter a username. See *Specifying a Username* on page 9-18 for more information.

10 Modems

10 - Modems

This chapter discusses how to configure your modem and the LRS to work together.

10.1 Modem Speeds

The modem's serial speed, measured in bits per second (bps), is the rate at which the modem sends data to a host computer or other device (such as the LRS) over its serial port. The modem's line speed, also measured in bits per second, is the rate at which the modem sends data through a telephone line to another modem or communications server. Although the two are related, they are not the same thing.

10.1.1 Serial Speed

The modem and the LRS must agree on the serial speed used for the connection to avoid corrupted data. However, the LRS may speak to a remote modem at a different speed due to error correction and flow control techniques used for the connection. In general, the serial speed should be set higher than the line speed, and higher still if compression is used.

Commonly used serial speeds include 1200, 2400, 9600, 19200, 38400, 57600, and 115200 bps. The LRS's default serial speed is 9600 bps, but can be changed with the **Set/Define Ports Speed** command. When a modem profile is defined, the LRS will automatically select the highest possible serial speed.

NOTE: *See your modem's documentation for more information about supported serial speeds and configuration options.*

10.1.2 Line Speed

Common line speeds include 9600, 14400, 28800, and 33600 bps. 9600 and 14400 are sometimes referred to by the names of the modem standards that define them (v.32 and v.32bis, respectively).

Notice that the faster line speeds do not have corresponding serial speeds. If there is no matching serial speed, the next highest serial speed should be used because faster serial speeds make the most efficient use of the given line speed. For example, a v.32bis modem (14400 bps) should use at least a 19200 bps serial speed.

To configure the proper serial and line speeds for a connection, see the *Examples* section.

NOTE: *Flow control must be used when the line speed and serial speed do not match. For more information on flow control setup, see Flow Control on page 9-12.*

10.2 Modem Profiles

The LRS interacts with a modem by sending commands to and expecting responses from the modem. This communication consists of strings or of simple commands to enable or disable modem features.

In order to communicate appropriately with a particular modem (this varies from modem to modem), the LRS consults a list of appropriate commands and responses for that modem. This compilation is called a **modem profile**.

10.2.1 Using a Profile

Preconfigured profiles are available for a number of modem types. Each profile contains all settings necessary to appropriately configure that type of modem. To display the list of profiles, use the **Show Modem** command. If your modem is listed, copy it to the port using the **Define Ports Modem Type** command.

Figure 10-1: Associating Modem Profile With a Port

```
Local>> DEFINE PORT 3 MODEM TYPE 5
```

All configurations in the modem profile will be applied to the specified port. The port's flow control will be changed to RTS/CTS, Autobaud will be disabled if it's enabled, and the port's serial rate will be changed to the highest rate the modem can support.

If your modem isn't in the list of profiles, use a modem profile for a modem that is similar to your modem type (for example, a modem from the same manufacturer). If there isn't a similar modem listed, use the Generic profile.

NOTE: *Be sure to verify the provisions mentioned in Security on page 10-10.*

New modem profiles will be added to the list as they become available from users and our engineering staff. If your modem isn't included in the list of profiles, contact Lantronix to see if it will be added in a later version of the software.

NOTE: *If you configure a modem profile that is not available on the list, please mail it to support@lantronix.com.*

To view the modem profile, or verify that changes have been successfully made to the profile, use the **List Port Modem** command:

Figure 10-2: Verifying Modem Configuration

```
Local>> LIST PORT 3 MODEM
```

10.2.2 Editing a Profile

If a profile isn't available for your modem, editing a profile for a similar modem is recommended (for example, a modem from the same manufacturer). However, if a similar modem profile isn't available, you can edit a preconfigured "generic" modem profile. This is explained in detail in *Profile Settings* on page 10-4.

NOTE: *Very few modems can use all commands in the generic modem profile. This is only a starting point.*

Profiles can also be edited to "fine-tune" your modem's performance. For example, dialing performance can be increased by adjusting the DMTF (touch tone) duration and spacing. To edit a modem profile, complete the following steps.

10.2.2.1 Examine the Profile

Display the modem profile by entering the **List Port Modem** command:

Figure 10-3: Displaying Modem Configuration

```
Local>> LIST PORT 3 MODEM
```

A series of settings will be displayed. For example, the Attention string may currently be set to **at**, and Error Correction may be enabled. Read through the configuration options discussed in *Profile Settings* on page 10-4 and determine which options you'll need to enable or disable to meet your needs. Consult your modem's documentation for the appropriate strings.

10.2.2.2 If Necessary, Edit the Init String

The Init string configures your modem at initialization. This string should do the following:

Table 10-1: Commands in Initialization String

Command Should	Example String
Set the modem to factory defaults.	&f
Set the modem to ignore any character that may force it to return to command mode (for example, +++).	s2=128
Set carrier detect (DCD) to "follow carrier."	&c1
Set the modem to hang up phone and return to command mode when the DTR signal is dropped.	&d2
Set the modem to use hardware flow control.	&k3
Set the modem to determine its serial speed from the Attention command (rather than using a constant serial speed).	s20=0
Set the modem to return as many result codes as possible (known as "all progress"). Result codes will be returned in text rather than numbers.	w1
If desired, set the modem to pass Caller-ID information to the LRS.	%ccid=1

NOTE: *The example strings given in Table 10-1 are not for all modems: consult your documentation for appropriate commands.*

If the Init string in your profile needs to be edited, use the **Define Ports Modem Init** command. The following example uses the example strings from Table 10-1:

Figure 10-4: Sending Initialization String

```
Local>> DEFINE PORT 3 MODEM INIT "&fs2=128&c1&d2&k3s20=0w1"
```

Often, initialization commands are sent individually, prefaced by the modem's Command Prefix string (commonly "at"). In order for the LRS to correctly send the information to your modem, all commands must be sent in one string. Do not include the Command Prefix string in the init string.

NOTE: *DSR should always be on.*

10.2.2.3 Edit Other Settings

All settings in a modem profile can be edited with the **Define Ports Modem Control** commands. For example, to configure the Dial string, use the **Define Ports Modem Dial** command.

Figure 10-5: Configuring a String

```
Local>> DEFINE PORT 3 MODEM DIAL "DT"
```

10.2.2.4 Enable Modem Control

Before a port can control a modem, modem control must be enabled. Use the following command:

Figure 10-6: Enabling Modem Control

```
Local>> DEFINE PORT 3 MODEM CONTROL ENABLED
```

10.2.2.5 Initialize the Modem

Log out the port to which the modem is connected. The modem will be initialized, incorporating any changes that you've made to the modem's profile.

Figure 10-7: Initializing the Modem

```
Local>> LOGOUT PORT 2
```

10.2.3 Profile Settings

These settings can be configured with the Define Port Modem commands.

10.2.3.1 Answer Enabled/Disabled

This setting configures whether or not the modem will automatically answer the telephone line.

10.2.3.2 Answer Command string

This string causes the modem to answer upon ring or to never answer. It is directly preceded by the Commandprefix string and is commonly set to "A".

10.2.3.3 Attention string

The attention string is sent to the modem each time the port is logged out or when the server first boots. The Modem must return the OK String. Otherwise it is assumed that the modem is disconnected or unavailable. It is commonly set to "at".

10.2.3.4 Busy string

The modem should respond with this string if the remote telephone line is busy. It is commonly set to “BUSY”.

10.2.3.5 Carrierwait string

This setting determines the amount of time (in seconds) that the modem will wait for a carrier. If a carrier isn’t received within this period of time, the call will fail. By default, Carrierwait is set to 60 seconds.

10.2.3.6 Commandprefix string

This string is placed before all commands sent to the modem except for the Attention String. In the unlikely event that your modem doesn’t use a common command prefix for all commands, this string should be left blank; include the appropriate command prefix in every string sent to the modem. It is commonly set to “at”.

10.2.3.7 Compression Enabled/Disabled

This setting enables or disables the modem’s data compression.

NOTE: *See Compression on page 10-8 for a complete description of compression.*

10.2.3.8 Compression Command disablestring enablestring

These strings cause the modem to compress data or to let data pass uncompressed. Note that compression often causes higher latency on a line in return for higher throughput.

10.2.3.9 Connected string

The modem must respond with this string after it connects with a remote modem. The modem may respond with other strings as well, but they will be ignored. It is commonly set to “CONNECT”.

10.2.3.10 Dial string

This string is sent after the Command Prefix but before the telephone number to be dialed. Commonly, touch tone dialing is activated with “dt” and pulse dialing is activated with “dp”.

10.2.3.11 Error string

The modem should respond with this string when it detects an error. It is commonly set to “ERROR”.

10.2.3.12 Errorcorrection Enabled/Disabled

This setting enables or disables the modem’s error detection and error correction.

NOTE: *See Error Correction on page 10-9 for a complete description of error correction.*

10.2.3.13 Errorcorrection Command disablestring enablestring

These strings cause the modem to use error correction or to let data pass uncorrected. Note that correction often causes higher latency on a line in return for data integrity.

10.2.3.14 Getsetup string

This string displays the modem’s current configuration. The LRS uses this information to determine if the modem’s configuration has changed. It is commonly set to “&v”.

When most modems receive the Get Setup string, they'll return one page that lists their configuration. The LRS will not function properly if more than one page of configuration information is sent (prompting the user to press a key to continue to the next page); if your modem is configured in this manner, the Get Setup string will need to be set to "". When Get Setup is set to "", the modem will not be queried for its configuration; instead, the LRS will write the modem's NVR each time the LRS is booted.

NOTE: *The AT&T Paradyne Comsphere and AT&T Dataport pose this problem.*

Use caution when configuring Get Setup in this manner. A modem's NVR can only be written a particular number of times; if the LRS is rebooted too often, setting Get Setup to "" could wear out the modem's NVR.

10.2.3.15 Init string

The Initialization (Init) string must be configured in a specific manner in order for your modem to work with the LRS. See *If Necessary, Edit the Init String* on page 10-3 for instructions.

10.2.3.16 Nocarrier string

The modem should respond with this string if the remote modem doesn't present a carrier. It is commonly set to "NO CARRIER".

10.2.3.17 Nodialtone string

The modem should respond with this string if no dial tone is present and the modem cannot dial. It is commonly set to "NO DIAL".

10.2.3.18 OK string

The modem must respond with this string after receiving the Attention String. It is commonly set to "OK".

10.2.3.19 Reset string

This string resets the modem and reloads its setup from nonvolatile memory (NVR). It is commonly set to "Z".

10.2.3.20 Ring string

The LRS will expect this string when the modem is ringing. If set to "", any characters from an idle modem will be interpreted as a ring. It is commonly set to "RING".

10.2.3.21 Save string

When the modem receives the Save string, it will save its configuration to nonvolatile memory (NVR). It is commonly set to "&w".

10.2.3.22 Speaker Enabled/Disabled

This setting enables or disables the modem's speaker.

10.2.3.23 Speaker Command disablestring enablestring

These strings turn the modem's speaker on or off. The speaker on switch may also set the speaker volume. It is commonly set to "m1l1" and "m0".

10.2.3.24 Statistics string

This string is sent to the modem after each call to gather statistics on that call. The resulting information from the modem is sent to the server's logging system for later analysis.

10.2.4 Modems with External Switches

Some modems, such as the USRobotics Sportster and Courier, have external switches that control the modem's behavior. Modems that have external switches but do not have predefined modem profiles on the LRS should be set not to autoanswer. The LRS answers the phone; the modem should never pick up the phone on it's own.

Sometimes the switch settings can be overridden by command strings, but sometimes they cannot. If your modem has switches, the LRS will tell you how to set the switches when you define the modem profile, as seen in Figure 10-8.

Figure 10-8: Enabling Modem Compression

```
Local>> DEFINE PORT 3 MODEM TYPE 30
%Info: Switch settings 1-8: UUDU DUUD
%Info: Port speed changed to 115200.
%Info: Port flow control changed to CTS.
```

In the example, "U" stands for up and "D" stands for down. Duplicate these settings on your modem, then power cycle the modem before logging out of the port or rebooting the LRS.

10.3 How the LRS Interacts with the Modem

10.3.1 Initialization

When the LRS is booted, the DTR signal will be held low so that the modem will reset and will not answer incoming calls. All LRS ports with Modem Control enabled will be checked to see if a modem is connected and powered up. To determine this, the LRS will send the Attention string to the modem and wait for the OK string to be sent in response.

The modem will then be asked for its current configuration. The Init string will be sent followed by a request for the modem's configuration. If the current modem profile on that port does not match the configuration sent from the modem, it will be assumed that the modem's setup has changed. The Save string will be sent, and the setup contained in the profile will be saved in the modem's permanent memory (NVR).

NOTE: *The NVR on some modems will wear out with repeated use. This limitation is avoided by only writing the setup to the modem if it has changed.*

The LRS will raise DTR so that the modem can answer incoming calls. The port then waits to start an outgoing call and waits to receive the Ring string from the modem to start an incoming call.

10.3.2 Outgoing Calls

On outgoing calls, the LRS will send the Attention string until the modem responds with the OK string (up to three times). If the modem does not send the OK string, the attempt will fail and the modem will be reset. If the OK string is received, the LRS will send the Command Prefix, the Dial String and the telephone number to the modem.

NOTE: *To set the telephone number, refer to Assign A Telephone Number to the Port or Site on page 3-16.*

If the modem responds with the Connect String, the call will succeed. If the modem responds with the No Carrier, Error, No Dial Tone or Busy strings, or if no response is received in 60 seconds, the call will fail and the modem will be reset. (60 seconds is the default wait period; this can be configured using the **Define Ports Modem Carrierwait** command).

NOTE: *Define Ports Modem Carrierwait is discussed on page 13-18.*

10.3.3 Incoming Calls

The LRS will detect an incoming call when a port receives the Ring string. The port will then be in a "ringing" state; outgoing calls cannot be made from this port during this period. The LRS will send the Command string followed by the Answer string forcing the modem to answer the call.

When the modem asserts the DCD signal, the incoming call will be permitted. If more than 60 seconds pass between ring signals or before the assertion of DCD, the LRS will assume that the caller hung up or that the connection attempt failed. (60 seconds is the default wait period; this can be configured using the **Define Ports Modem Carrierwait** command). The port will then be available for outgoing calls.

10.3.4 When a Port is Logged Out

Each time a port is logged out (for example, when a user hangs up), the LRS will send the Attention string to the modem. The OK string is expected in return. When this string is received, the LRS will send the Command Prefix string and the Reset string.

When the modem receives the Reset string, it will read its configuration from NVR. Any temporary configuration (for example, changes that an outbound modem user made) will be cleared at this point.

NOTE: *If a user made changes during an outbound call and saved them to the modem's NVR, the modem will be returned to that state.*

10.3.5 Compression

The compression setting in a modem profile enables or disables **data compression** in the modem.

Data compression enables a modem to transfer a larger amount of data in the same amount of time. When compression is used, uncompressed data arrives on the modem's serial port and the modem compresses the data before sending it over the phone line. The advantage of compression is increased **throughput**. For example, a modem might compress data to 1/2 its original size, doubling the modem's throughput; twice the data could be sent in the same amount of time required to send uncompressed data.

The disadvantage of compression is increased **latency**. Latency is the delay before data transfer occurs, caused by the additional time the modem requires to compress the data before it is sent. In situations where the delay is undesirable (for example, during interactive use over a long distance line), compression should not be used.

The "compressibility" of data depends on what is being compressed. Some data can be compressed to less than half its original size, while other data cannot be compressed at all. As the type of data to be sent changes, the modem's throughput will change.

Before compression can be enabled, flow control must be enabled (See *Flow Control* on page 9-12). In addition, the modem's serial speed must be set higher than the line speed. This enables the LRS to keep the modem's internal data buffer filled with data to compress. As lower compression ratios decrease the effective line speed, the modem will flow control the LRS more often. When compression ratios and the effective line speed rise, the modem will flow control the LRS less often.

NOTE: *On some modems, error compression must be enabled for data compression to work properly. See Error Correction on page 10-9.*

To enable modem compression, use the following command:

Figure 10-9: Enabling Modem Compression

```
Local>> DEFINE PORT 2 MODEM COMPRESSION ENABLED
```

NOTE: *For the complete syntax of Define Ports Modem Compression, see page 13-19.*

When modem compression is enabled on a port, the LRS will send a string to the modem to instruct it to enable modem compression. When compression should be disabled, a disable string may be sent. The default enable and disable strings vary, depending upon the modem profile used. To display the default strings for a particular modem profile, use the List Modem command:

To modify these strings, use the **Define Ports Modem Compression** command. The first string specified is the disable string; the second is the enable string.

Figure 10-10: Changing the Disable and Enable Strings

```
Local>> DEFINE PORT 2 MODEM COMPRESSION “s46=136” “q5”
```

The compression mode used varies from modem to modem, however, the most common mode is **V.42bis**. This is the recommended method of data compression.

V.42bis encoding offers an automatic 20% savings on all data sent, regardless of how compressible it is. Some text files can be compressed down to 1/4 or less of their original size. In addition, V.42bis will enable or disable compression according to whether or not it's required.

Other compression modes, such as MNP, may not give the same results as V.42bis. To obtain the best results, experiment with different modes of compression.

NOTE: *On many modems, error correction must be enabled in order to use data compression.*

10.3.6 Error Correction

A modem profile's **Error Correction** setting enables or disables the modem's error correction mode.

Error correction modes enable modems to ensure data integrity in the presence of telephone line noise. These modes work by checking the data for errors at the receiving modem. If an error is detected, the receiving modem requests that the sending modem retransmit the data.

When errors are not detected, data flows through the modem at a normal rate. When an error occurs, the sending modem must retransmit the data and not send any new data. The sending modem must be able to flow control the LRS during the retransmission. Ensure that flow control is enabled on the LRS before enabling error correction.

NOTE: *To configure flow control, see Flow Control on page 9-12.*

To enable error correction, use the following command:

Figure 10-11: Enabling Error Correction

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION ENABLED
```

NOTE: *For the complete syntax of Define Ports Modem Errorcorrection, see page 13-22.*

When error correction is enabled on a port, the LRS will send a string to the modem to instruct it to enable error correction. When error correction should be disabled, a disable string may be sent. The default enable and disable strings vary, dependent upon the modem profile used. To display the default strings for a particular modem profile, use the List Modem command.

To modify these strings, use the **Define Ports Modem Errorcorrection** command. The first string specified is the disable string; the second is the enable string.

Figure 10-12: Changing the Disable and Enable Strings

```
Local>> DEFINE PORT 2 ERROR CORRECTION “&q5” “q0”
```

10.3.7 Security

If security measures aren’t taken, unauthorized callers may be able to gain access regardless of the port’s security measures. In order to prevent this, the following must be true:

- If a remote user hangs up without logging out, the modem will sense the loss of carrier, and deassert the DCD signal. The server will then log the port out.
- If the remote user logs out, the server will force the modem to hang up immediately and reset.

These items should be carefully verified for each port that a modem is attached to, even if a pre-configured modem profile is used.

Dialback security, discussed below, can be used in conjunction with these techniques on modem ports for an additional layer of security.

The Ports and Security chapters cover security features in detail. The best tools for securing modem ports are username and password pairs, server passwords, and idle timeouts.

10.3.8 Autostart

A port with Autostart and modem control enabled will not run the specified mode (for example, PPP) until the modem asserts the DCD signal. This prevents the port from sending data to the local modem before a remote modem is connected.

NOTE: *For information on Autostart or the DCD signal, see Chapter 9, Ports*

10.3.9 Dialback

Dialback allows a system manager to set up a dialback list of authorized users for incoming modem connections. When a username matching one in the list is entered, the port will be logged out and the user will be called back at the predefined number.

For a complete discussion of dialback, see *Dialback* on page 12-4.

10.4 Terminal Adapters

ISDN Terminal adapters (TA's) are similar to modems. Modems convert asynchronous serial signals to a form that can be transmitted via regular phone lines, and terminal adapters (TA's) convert asynchronous serial signals to a form that can be transmitted by ISDN phone lines. The main difference between using these devices with the LRS is the complexity of TA setup, which varies by telephone service provider.

For the most part, the LRS interacts with a TA in the same way that it interacts with a modem. However, two things must be taken into account when using a TA with the LRS:

- Although some TAs can autodetect certain settings, it is not always possible to auto-configure information needed for the connection, such as the caller's own phone number. Therefore, no TA profiles are preconfigured for the LRS itself. TA users must edit the generic modem profile so that it can be used with their specific TAs and ISDN service providers.

NOTE: *Lantronix provides Tech Tips that outline the configuration needed for certain specific terminal adapters. To find out if your TA's configuration is included in a Tech Tip, contact your dealer or Lantronix technical support.*

- B-channel ISDN connections are much faster than modem connections. Those who wish to use the LRS bandwidth-on-demand functionality should take this speed increase into consideration when configuring bandwidth settings.

10.5 Caller-ID

Three commands provide the LRS with basic Caller-ID functionality, provided that Caller-ID is available and the LRS is attached to a modem capable of decoding Caller-ID signals.

Define Ports Modem CallerID Enabled allows the LRS to parse Caller-ID information that it receives from the attached modem.

Figure 10-13: Turning on Caller-ID

```
Local>> DEFINE PORT 2 MODEM CALLERID ENABLED
```

NOTE: *The modem should be configured for either Single or Multiple Message Format; the LRS cannot parse information in raw data format (ASCII coded hexadecimal). See your modem's documentation for configuration.*

Define Ports Modem Answer Rings configures the number of rings, either 1 or 3, that the LRS will wait for before answering the line. The telephone company sends Caller-ID information between the first and second rings, so the LRS must be set to wait for 3 rings before answering in order for Caller-ID functionality to work.

Figure 10-14: Setting Modem Ring Value for Caller-ID

```
Local>> DEFINE PORT 2 MODEM ANSWER RINGS 3
```

NOTE: *The modem init string must be modified to tell the modem to pass Caller-ID information to the LRS. See If Necessary, Edit the Init String on page 10-3 for more information.*

Finally, **Show/Monitor/List Ports Modem Status** displays status information about modems connected to LRS ports, including the most recently collected Caller-ID information. A sample modem status display is shown in Figure 10-14.

Figure 10-15: Modem Status Display with Caller-ID Information

```
Local>> show port 2 modem status

Port 2: Username: Stephan    Physical Port 2 (Local Mode)

  Last Connect Speed: 28800/ARQ/V34/LAPM/V42BIS

  Last Caller ID Information:

    Date:    12-19 12:20

    Number:  7145551234

    Name:    (n/a)

Local>>
```

Caller-ID information is also recorded by modem logging level 2 (see Set / Define Logging on page 13-98) and sent to RADIUS servers (see Appendix E, *Supported RADIUS Attributes*).

10.6 Wiring

The LRS must be wired to the DCD pin on your modem. If you're using an LRS16, you'll need to wire the DB25 adapter from the LRS16 DSR/DCD pin to the DCD pin on the modem. See the *Pin-outs* appendix of the **Installation Guide** for complete wiring information.

NOTE: *For more information, see Serial Signals on page 9-14.*

10.7 Examples

10.7.1 Typical Modem Configuration

Figure 10-16 lists the commands required for a typical modem setup. In this example, an LRS modem profile exists for this brand of modem. All modem strings in this profile are acceptable; no special configuration is required.

Figure 10-16: Typical Modem Configuration

```
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 4
Local>> DEFINE PORT 2 MODEM SPEAKER DISABLED
Local>> LOGOUT PORT 2
```

10.7.2 Modem Configuration Using Generic Profile

In this example, a V.34 modem is attached to LRS port 2. A modem profile does not exist for this brand of modem; the generic modem profile must be used. This modem will support incoming and outgoing connections.

Port 2's speed must be set properly for the modem. To determine the appropriate port speed, examine the following table:

Table 10-2: Maximum Baud Rates

Modem	Typical Maximum Line Rate
V.32	19200
V.32bis	57600
V.fast	115200
V.34	115200

To determine the maximum baud rate supported by the modem, the port speed must be set and tested. Modem handling must be disabled on the port; if it is enabled, the LRS will attempt to initialize the modem when the port is logged out.

Figure 10-17: Configuring Port Speed

```
Local>> DEFINE PORT 2 MODEM DISABLED
Local>> DEFINE PORT 2 SPEED 115200
```

The port speed is tested by logging into the port and sending an attention ("at") command. The modem should respond with "OK". If it does not send "OK", the port speed should be set to a lower baud rate (see Table 10-2).

Figure 10-18: Testing the Port Speed

```
Local>> SET PORT 2 LOCAL SWITCH ^\
Local>> CONNECT LOCAL PORT_2
Local protocol emulation V2.2
at
OK

Local>>
```

After the appropriate port speed is determined, the port must be configured using the generic modem profile. In addition, modem operation must be enabled.

To determine which profile number is the generic profile (the number will change as new profiles are added), enter the List Modem command:

Figure 10-19: Displaying Modem Profiles

```
Local>> LIST MODEM
1- Modem 1
2- Modem 2
3- Modem 3
4- Generic
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 4
%Info: Port speed changed to 57600.
%Info: Port flow control changed to CTS.
```

The generic modem profile made a series of configurations to port 2. To determine the current configuration of port 2, use the List Port or List Port Modem command.

Figure 10-20: Current Port Configuration

```
Local>> list port 2

Port 2: Username:                       Physical Port 2 (Idle)

  Char Size/Stop Bits:         8/1      Input Speed:          57600
  Flow Ctrl:               Cts/Rts      Output Speed:         57600
  Parity:                     None      Modem Control:     Disabled

  Access:                    Local      Local Switch:          None
  Backward:                   None      Port Name:           Port_2
  Break Ctrl:                Local      Session Limit:            4
  Forward:                    None      Terminal Type:      Soft ()

  Preferred Services:     (Telnet)

  Characteristics:  Broadcast  Loss Notify  Telnet Pad  Verify
```

The speed for port 2 is now 57600. This speed must be set to the appropriate speed (determined earlier by setting and testing the speed), 115200.

Figure 10-21: Configuring Port Speed

```
Local>> DEFINE PORT 2 SPEED 115200
```

Port 2 will be used for incoming and outgoing connections, therefore, access must be set to Dynamic.

Figure 10-22: Configuring Local Switch and Port Access

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

After entering this command, log out the port to ensure that the changes will be in effect when the next user logs into port 2.

10.7.3 Editing Modem Strings

The current init string on port 2 is **&fw1&c1&d2&k3s2=128**. This string must be changed to work with a particular modem:

Figure 10-23: Changing Init String

```
Local>> DEFINE PORT 3 MODEM INIT “&fw1&c1&d2s2=128s38=0”
```

NOTE: *To see what the above modem initialization string is configured to do, refer to Table 10-1 on page 10-3.*

Consult your modem’s documentation for the exact items to include in the modem init string.

10.8 Troubleshooting

To help diagnose any difficulty with your modem setup, it is a good idea to do the following:

- Install a breakout box between the modem and the LRS. Set all modem switches to the "normal" position, and remove all jumpers. When the modem and LRS are powered on, the box's LEDs will display the state of the signals, enabling you to more easily diagnose the problem.
- Enable logging for modems. (See *Event Logging* on page 12-25)
- Use the **List Port** command to ensure that modem control is enabled on the port. Many of the port's characteristics will be displayed; modem control is the third item listed in the left column.
- Ensure that all modems have been reset by rebooting the LRS.
- Verify the cable connections.

The following table lists some common problems that occur with modem configuration and proposes solutions for them.

Table 10-3: Modem Troubleshooting

Problem	Possible Cause(s)	Remedy
The modem won't answer the phone.	The modem isn't configured to answer the phone.	Enable answering with the **Define Ports Modem Answer** command (page 13-16).
	The DTR signal isn't attached.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.
	The LRS isn't asserting the DTR signal.	Ensure that the **Dtrwait** characteristic (page 13-111) is disabled on the LRS port used.
	The modem has hung.	Cycle power on the modem.
The modem doesn't respond to the LRS's configuration requests.	The modem's flow control isn't set properly, or the modem's autobaud isn't functioning properly.	Reset the modem's NVR to the factory default state (the **at&f** string is commonly used). For further instructions, refer to your modem's documentation.
	The modem isn't wired correctly.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
The modem answers, but cannot connect to the LRS.	The **Access** characteristic on the LRS port is set to None or Remote.	Set Access (page 9-1) to **Local** or **Dynamic**.
	The modem's serial speed does not match the serial speed on the LRS port used.	Ensure that the serial speeds of the modem and LRS port match.
	A network user is connected to the modem.	Use the **Show Ports** command (page 13-155) to verify that the LRS port is idle. If it is not idle, log out the port using the **Logout Port** command (page 13-51).
	The modem has hung.	Cycle power on the modem.
	The LRS cannot detect the DCD signal.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.

Table 10-3: Modem Troubleshooting, cont.

Problem	Possible Cause(s)	Remedy
All data is corrupted.	The ground pins aren't wired correctly.	Verify the wiring. Ensure that the ground pins on the RJ45 ports are wired together.
	The modem's serial speed does not match the serial speed on the LRS port used.	Ensure that the serial speeds of the modem and LRS port match.
	Flow control isn't working properly.	Ensure that the modem and LRS port are configured to use the same flow control method.
	The modem is set to the wrong baud rate.	Cycle power on the modem.
The first few lines of data are transmitted properly, but the subsequent data is corrupted.	Flow control isn't working properly.	Ensure that the modem and LRS port are configured to use the same flow control method. Flow control is discussed in detail in *Flow Control* on page 9-12.
	The ground pins aren't wired correctly.	Verify the wiring. On RJ45 ports, ensure that the ground pins are wired together.
When the port is logged out, the modem doesn't hang up the phone line.	Modem Control isn't enabled on the LRS port used.	Ensure that Modem Control is enabled. See **Define Ports Modem Control** on page 13-20 for details.
	The DTR signal isn't attached.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
	The modem isn't configured to reset when the DTR signal is dropped.	Check the modem's configuration.
When the phone is hung up, the LRS doesn't log out the port.	Modem Control isn't enabled on the LRS port used.	Ensure that Modem Control is enabled. See **Define Ports Modem Control** on page 13-20 for details.
	The DCD signal isn't attached.	Verify the wiring. Ensure that the ground pins on RJ45 ports are wired together.
	The modem isn't configured to deassert DCD upon loss of carrier.	Check the modem's configuration.
The modem answers, but won't connect to the remote modem.	One or both modems are configured not to connect unless some feature is enabled (for example, error correction).	Check the documentation for both modems; verify their configuration.
	The two modems cannot be connected. (Some modems are incompatible with one another).	Replace one or both of the modems. Verify that the modem is using the correct and current version of its software.

10.9 Quick Reference

Modem Profiles			
To	**Use This Command**	**Example(s)**	**What Example Does**
Display the Available Modem Profiles	Show / Monitor / List Modem, page 13-153.	`SHOW MODEM`	Displays all LRS modem profiles. See *Modem Profiles* on page 10-2 for more information.
Copy a Modem Profile to a Port	Define Ports Modem Type, page 13-27.	`DEFINE PORT 2 MODEM TYPE 5`	Copies modem profile 5 to port 2. See *Using a Profile* on page 10-2 for more information.
Enable Modem Operation on a Port	Define Ports Modem Control Enabled, page 13-20.	`DEFINE PORT 2 MODEM ENABLED`	Tells the LRS to treat port 2 as if there is a modem attached.
Make a Modem Profile Take Effect (Once Copied to a Port)	Logout, page 13-51.	`LOGOUT PORT 2`	Port 2 will start using its defined profile. See *Using a Profile* on page 10-2 for more information.
Display a Port's Modem Configuration	Show / Monitor / List Modem, page 13-153.	`LIST PORT 2 MODEM`	Displays the modem configuration for port 2. See *Examine the Profile* on page 10-3 for more information.
Edit a Modem Profile	1. Display the port's modem configuration (see above).		
	2. Define Ports Modem Control <string>, beginning on page 13-20.	`DEFINE PORT 2 MODEM INIT "&f&c1s20=0"`	Configures port 2's initialization string. See *Profile Settings* on page 10-4 for more information.

Modem Profiles, cont.

To	Use This Command	Example(s)	What Example Does
Edit a Modem Profile, cont.	3. Define Ports Modem Control, page 13-20.	`DEFINE PORT 2 MODEM CONTROL ENABLED`	Enables modem operation on port 2. See *Enable Modem Control* on page 10-4 for more information.
	4. Logout Port, page 13-51.	`LOGOUT PORT 2`	Initializes the modem attached to port 2. Any changes made to the LRS modem configuration will be put into effect. See *Initialize the Modem* on page 10-4 for more information.

Compression

To	Use This Command	Example(s)	What Example Does
Enable / Disable the Modem's Data Compression	Define Ports Modem Compression, page 13-19.	`DEFINE PORT 2 MODEM COMPRESSION ENABLED`	The LRS will configure the modem to use data compression by sending the appropriate string when the modem is configured. See *Compression* on page 10-8 for more information.
Edit the Strings Sent to the Modem to Enable / Disable Compression	Define Ports Modem Compression, page 13-19.	`DEFINE PORT 2 MODEM COMPRESSION "s46=136" "q5"`	When modem compression is enabled on port 2, the LRS will send "s46=136" to the modem to disable compression and "q5" to enable compression. See *Compression* on page 10-8 for more information.

Error Correction

To	Use This Command	Example(s)	What Example Does
Enable the Modem's Error Correction	Define Ports Modem Errorcorrection, page 13-22.	`DEFINE PORT 2 MODEM ERRORCORRECTION ENABLED`	The LRS will configure the modem to use error correction by sending the appropriate string when the modem is configured. See *Error Correction* on page 10-9 for more information.
Edit the Strings Sent to the Modem to Enable / Disable Error Correction	Define Ports Modem Errorcorrection, page 13-22.	`DEFINE PORT 2 MODEM ERRORCORRECTION "&q5" "q0"`	When modem compression is enabled on port 2, the LRS will send "&q5" to the modem to disable error correction and "q0" to enable error correction. See *Error Correction* for more information.

Security

To	Use This Command	Example(s)	What Example Does
Secure Modem Ports	See Chapter 12, *Security*.		
Configure a List of Authorized Users for Dialback Modem Connections	See *Dialback from Local Mode* on page 12-5.		

Flow Control Configuration

To	Use This Command	Example(s)	What Example Does
Set the Appropriate Line and Serial Speeds	See *Modem Configuration Using Generic Profile* on page 10-13.		
Disable Autobaud	Set / Define Ports Autobaud, page 13-105.	`DEFINE PORT 2 AUTOBAUD DISABLED`	Disables Autobaud on port 2. See *Flow Control* on page 9-12 for more information.

Caller-ID

To	Use This Command	Example(s)	What Example Does
Use the LRS Caller-ID Functionality	1. Define Ports Modem CallerID, page 13-18.	`DEFINE PORT 2 MODEM CALLERID ENABLED`	Enables Caller-ID functionality. See *Caller-ID* on page 10-12 for more information.
	2. Define Ports Modem Answer Rings, page 13-16.	`DEFINE PORT 2 MODEM ANSWER RINGS 3`	Sets the attached modem to wait for three rings before answering the line. See *Caller-ID* on page 10-12 for more information.
	3. Define Ports Modem Init, page 13-23.	`DEFINE PORT 2 MODEM INIT #CID=1`	Tells the attached modem, in this case a US Robotics modem, to pass Caller-ID signals to the LRS. See *If Necessary, Edit the Init String* on page 10-3 for more information.
Display Caller-ID Information	Show / Monitor / List Ports Modem Status, page 13-155.	`SHOW PORT 2 MODEM STATUS`	Shows information about the modem attached to port 2, including the most recently gathered Caller-ID information. See *Caller-ID* on page 10-12 for more information.

11 Modem Sharing

11 - Modem Sharing

Modem sharing provides users with individual modem / phone line functionality at a reduced cost. When modems are shared, a group of IP or IPX users may use a modem pool to dial out of a LAN and connect to a remote host; for example, to connect to a bulletin board service (BBS). This eliminates the need for phone lines for each user's computer.

11.1 Services

A **service** represents a resource accessible to network users; for example, a modem or a pool of modems attached to the LRS.

Services provide links for TCP or SPX (Sequenced Packet Exchange) connections to LRS serial ports. They are employed in modem sharing to establish connections to the LRS modems.

11.1.1 Creating a Service

Each LRS service must have a unique name. To create a service, use the **Set/Define Service** command. An example is displayed below.

Figure 11-1: Creating a New Service

```
Local>> DEFINE SERVICE fastmodems
```

Service names are not case-sensitive, may be up to 16 alphanumeric characters long, and cannot include spaces.

11.1.2 Associating Ports with a Service

Each service must be associated with at least one port. To associate a port with a service, use the **Set/Define Service Ports** command:

Figure 11-2: Associating a Port with a Service

```
Local>> DEFINE SERVICE fastmodems PORTS 2
```

NOTE: *Set/Define Service Ports is discussed in detail on page 13-140.*

To use a service for modem sharing, the service should be associated with multiple ports; this permits multiple connections to the service. Connections will be made to the first available port.

Figure 11-3: Associating a Service with Multiple Ports

```
Local>> DEFINE SERVICE fastmodems PORTS 2-4
```

Ports associated with a service used for modem sharing must support outgoing connections. To support outgoing connections, the port access must be set to Dynamic or Remote.

Figure 11-4: Configuring a Port for Outgoing Connections

```
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

A port associated with a service used for modem sharing must also be configured to operate the modem attached to it. To configure modem operation on a port, use the following commands:

Figure 11-5: Configuring Modem Operation on a Port

```
Local>> DEFINE PORT 2 MODEM CONTROL ENABLED
Local>> LIST MODEM
Local>> DEFINE PORT 2 MODEM TYPE 5
```

To display a particular modem type's settings, use the **Show/Monitor/List Modem <type #>** command.

NOTE: *For more information on modem configuration, see Chapter 10, Modems. For more information on port configuration, see Chapter 9, Ports.*

11.1.3 Displaying Current Services

To display a list of the current services, use the **Show/Monitor/List Services** command.

To display specific information about a service, the following parameters may be used with the Show / Monitor / List Services command: Characteristics, Summary, and Status. For example, to display a service's characteristics (including the ports associated with it), use the following command:

Figure 11-6: Displaying a Service's Characteristics

```
Local> LIST SERVICES fastmodems CHARACTERISTICS
```

The command above shows the ports associated with the service **fastmodems**, the characteristics enabled for the service, and the **service rating**.

Generally, a service rating of 255 means that the service is available, and a rating of zero means that it is busy or otherwise unavailable. A rating between 255 and zero indicates that the service is partially available. For example, fastmodems may be a modem pool containing three high-speed modems, one of which is available. In this case, the service rating for fastmodems would be 85.

NOTE: *Show/Monitor/List Services is discussed in detail on page 13-160.*

11.2 IPX

11.2.1 Configuring an IPX Modem Pool Service

For services on an IPX network, the LRS uses the SPX protocol to manage the connection to a remote host. To enable SPX on a service, use the **Set/Define Service SPX** command:

Figure 11-7: Enabling SPX on a Service

```
Local>> DEFINE SERVICE fastmodems SPX ENABLED
```

NOTE: *The complete syntax of Set/Define Service SPX is listed on page 13-142.*

11.2.2 Using the COM Port Redirector

The Lantronix IPX Redirector is an application that allows PCs to share modems connected to the LRS using Microsoft Windows communication applications. With the Redirector, PC users can use their communication software to dial out, connect to a modem available as an LRS service, and connect to a remote host.

The Redirector software is shipped on the LRS CD-ROM. For installation and configuration instructions, see the *Redirector Quick Installation Template* that came with your LRS.

NOTE: *The Redirector must be installed on each PC that will share LRS modems.*

11.3 IP

To share LRS modems, IP users must do one of the following:

- Use the Lantronix COM Port Redirector application.
- Form a TCP connection to a TCP listener socket associated with a service.
- Form a TCP connection directly to an LRS serial port.
- Log into the LRS and connect to a local service or port.

These methods are discussed in the following sections.

11.3.1 Configuring an IP Modem Pool Service

Creating a service allows you to set up a modem pool on several LRS ports. To create an IP modem pool service, enter the **Set/Define Service** command.

Figure 11-8: Creating an IP Modem Pool Service

```
Local>> DEFINE SERVICE modempool PORT 8 TCPPORT 4008
```

NOTE: *The complete syntax of Set/Define Service TCPport is listed on page 13-143.*

11.3.2 Using the COM Port Redirector

Using the Redirector on an IP network is basically the same as using it on an IPX network, with one important exception. Instead of creating a modem pool service with SPX enabled, you must create a modem pool service that is associated with a TCP listener socket. Refer to Figure 11-9 (*Connecting to a TCP Listener Service*, next) for the necessary command.

For complete Redirector installation and configuration information, see the *Redirector Quick Installation Template* that came with your LRS.

11.3.3 Connecting to a TCP Listener Service

Each service may be associated with a TCP listener socket. TCP connections to the socket are connected to the service. Once a connection is established, a user may issue commands to the modem.

To associate a service with a TCP listener socket, use the **Set/Define Service TCPport** command. Socket numbers must be between 4000 and 4999.

Figure 11-9: Specifying a Raw TCP Listener Socket

```
Local>> DEFINE SERVICE highspeedmodem TCPPORT 4999
```

NOTE: *The complete syntax of Set/Define Service TCPport is listed on page 13-143.*

If the socket should perform Telnet IAC character-escaping negotiations on the data stream, use the **Set/Define Service Telnetport** command:

Figure 11-10: Specifying a Telnet TCP Listener Socket

```
Local>> DEFINE SERVICE highspeedmodem TELNETPORT 4500
```

NOTE: *Set/Define Service Telnetport is discussed in detail on page 13-143.*

Connecting to a TCP listener service is recommended if more than one modem is being used. The LRS will automatically connect the user to the next available modem, avoiding the trial and error process of finding an available port (see *Connecting to an LRS Serial Port* on page 11-4).

11.3.4 Connecting to an LRS Serial Port

To connect directly to an LRS serial port, specify a port number of **3000 + *n***, or **2000 + *n***. The *n* represents the number of the LRS serial port; for example, port 2002 represents LRS serial port 2.

If you're using Telnet to connect to the LRS, connect to port 2000 + *n*. The 2000 port is intended for Telnet connections; it performs Telnet IAC character-escaping negotiations on the data stream. In the example below, the Telnet command is used to connect to LRS serial port 3.

Figure 11-11: Telnetting Directly to Port 3

```
% TELNET server_name 2003
```

If you're connecting via a host application, connect to port 3000 + *n*. This port provides an 8-bit clean connection, required by most host applications.

11.3.5 Connecting to an LRS Service or Port

To connect to a local service or port from an LRS login, use the **Connect Local** command at the Local> prompt.

Figure 11-12: Connecting to a Local Service / Port

```
Local>> CONNECT LOCAL fastmodems
Local>> CONNECT LOCAL PORT_2
```

If a service name is specified, a connection is made to the first available port associated with the service. If a port name is specified, the connection is made to the port unless the port is in use.

Once the connection is established, commands may be issued to the modem attached to the serial port.

11.4 Examples

Users on an IPX network need to connect to both a BBS and a commercial online service. The following modems are available:

- Two 28,800 bps modems, reserved for connections to the online service
- Four 14,400 bps modems, available for connections to both services
- One 9,600 bps modem, reserved for connections to the BBS

The modems are connected to an LRS as follows:

Table 11-1: Modems Connected to the LRS

Speed	Connected to	LRS Modem Type
28,800 bps (2)	Ports 2 and 3	6
14,400 bps (4)	Ports 4 through 7	5
9,600 bps (1)	Port 8	4

Three services will be created for the modems: **fastmodems**, **slowmodems**, and **slowestmodem**. These will be used for the 28,800, 14,400, and 9,600 modems, respectively.

Figure 11-13: Configuring the LRS fastmodems Service

```
Local>> DEFINE SERVICE fastmodems PORTS 2-3 SPX ENABLED
Local>> DEFINE PORT 2-3 ACCESS REMOTE
Local>> DEFINE PORT 2-3 MODEM TYPE 6
Local>> DEFINE PORT 2-3 MODEM CONTROL ENABLED
```

Figure 11-14: Configuring the LRS slowmodems Service

```
Local>> DEFINE SERVICE slowmodems PORTS 4-7 SPX ENABLED
Local>> DEFINE PORT 4-7 ACCESS REMOTE
Local>> DEFINE PORT 4-7 MODEM TYPE 5
Local>> DEFINE PORT 4-7 MODEM CONTROL ENABLED
```

Figure 11-15: Configuring the LRS slowestmodem Service

```
Local>> DEFINE SERVICE slowestmodem PORT 8 SPX ENABLED
Local>> DEFINE PORT 8 ACCESS REMOTE
Local>> DEFINE PORT 8 MODEM TYPE 4
Local>> DEFINE PORT 8 MODEM CONTROL ENABLED
```

When all of the configurations have been entered, log the ports out and initialize the server.

11.4.1 Configuring the Redirector

The following table shows how the Redirector setup utility should be configured for this example. All three LRS services (fastmodems, slowmodems, and slowestmodem) should appear in the Service Selection window.

Table 11-2: Redirector Configuration

COM Port #	Redirect?	Selected Services (in order)
COM Port 1	Yes	fastmodems slowmodems
COM Port 2	Yes	slowmodems slowestmodem

11.4.2 Configuring the PC Communications Software

The communication software must be configured to connect to the online service by dialing out through COM Port 1 and to the BBS by dialing out through COM Port 2

11.5 Troubleshooting

If commands issued to a modem aren't displayed, the modem may not be configured to echo commands. To correct this problem, enable modem echoing on the modem.

If a connection attempt fails, check the port's access. The access must be set to dynamic or remote in order to support outgoing connections. Failed connections may also result if the port is currently in use.

11.6 Quick Reference

Using Services For Modem Sharing: Step by Step Configuration

To	Use This Command	Example(s)	What Example Does
Create a Service	Set / Define Service, page 13-138.	`DEFINE SERVICE fastmodems`	Creates a new service named "fastmodems". See *Creating a Service* on page 11-1 for more information.
Associate Ports with a Service	Set / Define Service Ports, page 13-138.	`DEFINE SERVICE fastmodems PORTS 2-4`	Associates the "fastmodems" service with ports 2, 3, and 4. See *Associating Ports with a Service* on page 11-1 for more information.
Configure a Port to Support Outgoing Connections	Set / Define Ports Access Remote / Dynamic, page 13-104.	`DEFINE PORT 2 ACCESS REMOTE`	See page 11-2 or *Accessing a Port* on page 9-1 for more information.
Configure a Port to Support Modem Operation	1. Define Ports Modem Control Enabled, page 13-20.	`DEFINE PORT 2 MODEM CONTROL ENABLED`	Enables modem operation on port 2.
	2. Define Ports Modem Type, page 13-27.	`DEFINE PORT 2 MODEM TYPE 5`	Associates port 2 with modem profile 5. The port will be configured in accordance with the modem profile. See *Modem Profiles* on page 10-2 for more information.
Display Existing Services	Show / Monitor / List Services, page 13-160.	`LIST SERVICES fastmodems CHARACTERISTICS`	Displays the characteristics of "fastmodems", including any associated ports. See *Displaying Current Services* on page 11-2 for more information.

IPX

To	Use This Command	Example(s)	What Example Does
Enable SPX on a Service	Set / Define Service SPX Enabled, page 13-142.	`DEFINE SERVICE fastmodems SPX ENABLED`	Enables SPX on the “fastmodems” service. See *Configuring an IPX Modem Pool Service* on page 11-3 for more information.

IP

To	Use This Command	Example(s)	What Example Does
Create a TCP Listener Socket	1. Set / Define Service TCPport, page 13-143.	`DEFINE SERVICE highspeedmodem TCPPORT 4999`	Associates the “highspeedmodem” service with TCP listener socket 4999. TCP connections to 4999 will be connected to “highspeedmodem”. See *Connecting to a TCP Listener Service* on page 11-4 for more information.
	2. Set / Define Service Telnetport, page 13-143.	`DEFINE SERVICE highspeedmodem TELNETPORT 4500`	Associates the “highspeedmodem” service with TCP listener socket 4500. TCP connections to 4500 will be connected to “highspeedmodem”, and Telnet IAC character-escaping will be performed.
Connect Directly to an LRS Serial Port	Connect Telnet 2000 + <serial port #>, page 13-12.	`TELNET` *`server_name`* `2003`	Connects user to LRS serial port 3 with Telnet IAC character-escaping. See *Connecting to an LRS Serial Port* on page 11-4 for more information.
	Connect Telnet 3000 + <serial port #>, page 13-12.	`TELNET` *`server_name`* `3003`	Connects user to LRS serial port 3 with an 8-bit clean connection.

12 Security

12 - Security

The LRS enables you to secure your network in a number of ways. Supported security features include:

- Authentication of incoming connections
- Authentication of outgoing LAN to LAN connections
- Dialback during incoming connection attempts
- Restriction of user access to commands and functions
- Event logging

12.1 Incoming Authentication

Authentication forces users to prove their identities when attempting to connect to the LRS. The connection type affects the authentication sequence and how the authentication information is transferred. Incoming connections may be one of the following types: character mode (Local> prompt) logins, PPP logins, SLIP logins, or virtual port logins.

12.1.1 Character Mode Logins

Each LRS serial port may be configured to support any combination of the following:

- A server-wide login password
- A username / password pair
- Dialback on serial ports with modems attached

This section will discuss the login password and the username / password pair. Dialback will be discussed in the following section.

NOTE: *To configure a port to support character mode, see Port Modes on page 9-3.*

12.1.1.1 Login Password

To set the login password, use the **Set/Define Server Login Password** command:

Figure 12-1: Defining Login Password

```
Local>> DEFINE SERVER LOGIN PASSWORD badger
```

NOTE: *The login password can be up to 6 characters long. The default password is "access."*

To require that users enter the login password when logging into a particular port, use the **Set/ Define Ports Password** command:

Figure 12-2: Requiring Login Password on a Port

```
Local>> DEFINE PORT 2 PASSWORD ENABLED
```

12.1.1.2 Username/Password Pairs

In addition to the login password, each port may be configured to prompt users for a personal username and password. When the user enters the username / password pair, the LRS scans the authentication databases (see *Comparing the Username/Password to Authentication Databases* on page 12-3) for a matching pair. If a match is not found, the login will not be permitted.

To enable username / password authentication, use the **Set/Define Ports Authenticate** command:

Figure 12-3: Enabling Username / Password Authentication

```
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED
```

12.1.1.3 Virtual Port Logins

Users can connect to a virtual port via a terminal connected to the serial console port or over the network using Telnet, Rlogin, or EZCon. For a complete discussion of virtual ports, see *Virtual Ports* on page 9-17.

By default, incoming Telnet and Rlogin connections are not required to enter the login password. To require the login password, use the **Set/Define Server Incoming Password** command:

Figure 12-4: Requiring a Login Password for Telnet / Rlogin Connections

```
Local>> DEFINE SERVER INCOMING PASSWORD
```

To require username / password authentication for virtual port logins, use the **Set/Define Ports Authenticate** command, specifying port 0 as the port number.

Figure 12-5: Virtual Port Username / Password Authentication

```
Local>> DEFINE PORT 0 AUTHENTICATE ENABLED
```

12.1.2 PPP Logins

This section covers authentication on ports dedicated to PPP or with PPPdetect enabled. If PPP will be started from character mode, see *Character Mode Logins* on page 12-1.

NOTE: *To dedicate a port to PPP or enable PPPdetect, see Chapter 9, Ports.*

12.1.2.1 How the Username/Password is Transmitted

The username and password may be transmitted using CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). Each protocol goes through a negotiation sequence to complete the authentication; see Chapter 3, *Basic Remote Networking*, for details.

To use CHAP or PAP to authenticate incoming callers, CHAP Remote or PAP Remote must be enabled on the port accepting the call. One or both may be enabled, however, CHAP is recommended.

Figure 12-6: Enabling CHAP and PAP for Incoming Connections

```
Local>> DEFINE PORT 2 PPP CHAP REMOTE
Local>> DEFINE PORT 2 PPP PAP REMOTE
```

If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the remote host does not understand CHAP, PAP will be attempted instead. If neither CHAP nor PAP successfully authenticates the caller, the connection is terminated.

12.1.2.2 Comparing the Username/Password to Authentication Databases

If the username sent by the caller matches a site name, that site will be checked to determine if it has a **local password** defined. The local password is the password expected from the incoming caller. To configure a local password for a site, use the Define Site Authentication Local command:

Figure 12-7: Defining a Site Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION LOCAL “wallaby”
```

If the password entered matches the site’s local password, that site will be started. If it does not match the local password, or the site does not have a local password defined, the LRS will check the next database (according to the order of database precedence). See *Database Configuration* on page 12-7 for details.

NOTE: *Some databases are case-sensitive, so the login information must be entered in the proper case in order for authentication to succeed. See the Database Configuration section for more information.*

A custom site will only be started if the username matches a site name and any password in an authentication database. If the username doesn’t match a site name, but matches a username/password pair in an authentication database, a temporary site will be used for the connection.

If a matching username/password pair is not found in any authentication database, the connection attempt will fail.

12.1.2.3 Offering Authentication Information to the Incoming Caller

If the incoming caller must authenticate the LRS, the port must have PAP Local or CHAP Local configured. Use the **Define Ports PPP CHAP Local** or **Define Ports PPP PAP Local** command:

Figure 12-8: Enabling CHAP and PAP Local

```
Local>> DEFINE PORT 2 PPP CHAP LOCAL
Local>> DEFINE PORT 2 PPP PAP LOCAL
```

During CHAP/PAP negotiation, the LRS will send the site’s username and remote password to the incoming caller. To set a site’s username and remote password, use the Define Site Authentication command:

Figure 12-9: Configuring the Site Username and Remote Password

```
Local>> DEFINE SITE irvine AUTHENTICATION USERNAME seattle
Local>> DEFINE SITE irvine AUTHENTICATION REMOTE gopher
```

Use caution when configuring a site to offer and accept authentication information (when the site has both a local and remote password). PAP does not offer complete security in this situation; if the site has PAP authentication enabled for incoming and outgoing connections, both passwords may be compromised during the LCP negotiation process.

When the LRS receives an incoming call, a site configured with a local and remote password may let the incoming caller know that it is willing to transmit these passwords. If the remote caller has PAP authentication enabled, it may persuade the LRS to transmit its passwords to the remote caller as part of the PAP authentication negotiation. At that point, the remote caller can hang up in possession of the LRS passwords. The caller may be able to use the LRS remote password to log into other networks, or to call the LRS and connect as an authorized user.

12.1.3 SLIP Logins

SLIP does not support authentication; authentication must take place before SLIP is started.

Ensure that the port will start in character mode by disabling SLIP autodetection and SLIP dedicated modes. SLIP Autodetection and dedicated SLIP are disabled by default.

Figure 12-10: Disabling SLIPdetect and SLIP Dedicated

```
Local>> DEFINE PORT 2 SLIPDETECT DISABLED
Local>> DEFINE PORT 2 SLIP DISABLED
Local>> DEFINE PORT 2 SLIP ENABLED
```

12.1.4 Starting PPP/SLIP From Character Mode

PPP or SLIP may be started when a port is in character mode using the **Set Ports PPP** or **Set Ports SLIP** commands. If an incoming user specifies a particular site to be started (for example, Set PPP irvine), the site may prompt the user for its local (site-specific) password.

To configure a site's local password, use the **Define Site Authentication Local** command.

Figure 12-11: Setting a Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION LOCAL "badger"
```

To prompt the user for the local password when attempting to start the site, use the **Define Site Authentication Prompt** command:

Figure 12-12: Requiring Site's Local Password

```
Local>> DEFINE SITE irvine AUTHENTICATION PROMPT ENABLED
```

12.1.5 Dialback

When dialback is used, the LRS will verify the identity of incoming users by logging the port out and dialing the user back at a specified number. Dialback may be configured to do any combination of the following:

- Log a port out and call the user back
- Permit users to bypass the dialback process and connect immediately
- Terminate the connection when unauthorized users attempt to connect

NOTE: *The port must be configured to use modems; for additional information, see Chapter 10, Modems.*

12.1.5.1 Dialback from Local Mode

To use dialback for character logins, configure a list of authorized users with the following steps:

1. Enable modem control using the **Define Ports Modem Control Enabled** command.
2. Assign a modem type to the port using the **Define Ports Modem Type** command.
3. Enable dialback using the **Define Ports Dialback Enabled** command:
4. Configure how Dialback treats users who are not in the dialback database.

   The Dialback Bypass setting controls what happens when a user that is not in the dialback database attempts to connect to the LRS. If Bypass is enabled, these users will be allowed to connect without dialback occurring. If Bypass is disabled, these users will not be able to connect.
5. Add users to the dialback database.

   To add a user to the dialback database, use the **Set/Define Dialback** command and specify a username and telephone number. If the user must bypass dialback (regardless of whether Dialback Bypass is enabled or disabled), specify the Bypass parameter:

Figure 12-13: Adding Users to the Dialback Database

```
Local>> DEFINE DIALBACK BYPASS ENABLED
Local>> DEFINE DIALBACK FRANK BYPASS
Local>> DEFINE DIALBACK BOB “555-1235”
```

In the example in Figure 12-13, user **frank** will bypass dialback. When user **bob** attempts to connect, the LRS will call him back at **555-1235**. Any other user attempting to connect will be subject to dialback; if he or she is not in the dialback database, the attempt will fail.

To view the Dialback database, use the **Show/Monitor/List Dialback** command.

Figure 12-14: Viewing the Dialback Database

```
Local>> Show Dialback
```

NOTE: *You must be the privileged user to view the Dialback database.*

12.1.5.2 What Happens During Dialback

1. When a username is entered on a dialback port, the LRS determines if it should allow the connection or dial the user back.
2. If the LRS must dial the user back, it hangs up the modem by cycling DTR.
3. The LRS sends a command to the applicable serial port. The command contains the modem command prefix, the dial string, and the configured telephone number from the dialback database.

   The dial string should perform any special configuration required for the call, then dial the remote modem number (in the example in Figure 12-13, 555-1234). It is not necessary to precede telephone numbers by strings such as “atdt.”
4. The LRS waits the length of the Carrier Wait setting for the DCD signal to go high, indicating that the modem has reconnected successfully. Otherwise, DTR is dropped for 3 seconds and the port is reset.

5. The LRS waits 30 seconds for the user to enter a username when in Dialback mode. After 30 seconds, the port is logged out to keep unauthorized users from denying other users access to that port.

NOTE: *Dialback only applies to incoming port logins. Dialback ports can be used normally for outgoing connections.*

12.1.5.3 Dialback From SLIP/PPP Mode

To authenticate incoming PPP and SLIP callers using dialback, the site managing the incoming connection must have dialback enabled. Use the **Define Site Authentication Dialback** command:

Figure 12-15: Enabling Dialback on a Site

```
Local>> DEFINE SITE irvine AUTHENTICATION DIALBACK ENABLED
```

Ensure that the correct ports and telephone numbers are defined; the site will use the defined site-specific or port-specific telephone number to dial the incoming caller. See *Telephone Numbers* on page 3-14 for more information.

12.1.5.4 Dialback Using Callback Control Protocol (CBCP)

The LRS supports the Microsoft Callback Control Protocol (CBCP) for dial-in PPP clients that request it. In conjunction with CBCP, the LRS may be configured to allow the PPP client to choose the dialback telephone number. This form of dialback is referred to as “insecure dialback” because it negates the usual security provided by dialback. It is primarily used to offer remote users a way to specify a dialback number to reverse telephone charges.

NOTE: *Insecure dialback may pose a security risk. Use it with caution.*

After the CBCP-aware client has connected to the LRS and has passed PPP authentication, and is optionally switched to a custom site, the LRS will negotiate CBCP (this happens regardless of site dialback settings). Three callback options are available:

- If dialback is disabled for the site, the connection will proceed without the dialback step.
- If normal dialback authentication is enabled for the site, the LRS will offer to call the PPP client back at the site-specific telephone number listed in the dialback database. If the client refuses, the connection will be terminated.
- If insecure dialback is enabled for the site, the PPP client can choose to use the site-specific telephone number or specify a different telephone number to use for the return call. If the client refuses to use the site’s telephone number and does not enter a valid alternate telephone number, the connection will be terminated.

NOTE: *The caller should have the alternate telephone number handy when connecting to the LRS to ensure that the connection does not time out before the number can be entered.*

To configure a site to allow insecure dialback, enter the following command on the LRS.

Figure 12-16: Configuring Insecure Dialback

```
Local>> DEFINE SITE irvine AUTHENTICATION DIALBACK INSECURE
```

NOTE: *Insecure dialback is only offered under CBCP for PPP clients. It does not apply to SLIP or Local mode dialback situations.*

12.1.5.5 Potential Dialback Drawbacks

The Dialback system does not absolutely guarantee security. Depending on the modem in use and its configuration, it may be possible for a determined attacker to penetrate the system. There are two windows of vulnerability where an attacker could gain unauthorized access to the LRS. The first window exists after the LRS hangs up the modem but before the modem dials the user back. The second is when a dialback attempt fails but before the server reaches the end of the configured carrier wait time-out period (the default setting is 60 seconds). Careful configuration and testing of the system during these short vulnerable periods is required to ensure a high level of security.

If a second call arrives in the few moments after the server hangs up the modem but before the server issues the dial command, security may be breached. Until the modem goes “off hook,” it may answer another incoming call and remain on-line, granting access to a possibly unauthorized user. This is highly unlikely, and the chances of unauthorized access can be reduced further by configuring the modem to answer only after the second or third ring. Also, the modem must not answer the phone unless DTR is asserted. If possible, the modem should be configured to only dial after detecting a dial tone, and hang up otherwise.

12.1.6 Database Configuration

Six types of databases can store authentication information. The databases can be used in any order or combination, but no more than one of each type may be used.

- Local authentication database stored in the LRS’s permanent memory (NVR)
- Kerberos V4 server
- NetWare bindery
- RADIUS server
- SecurID ACE/Server
- UNIX password file, via TFTP

The database search order is determined by each database or server’s **precedence**. When configuring database precedence, it makes sense to specify the location where the largest amount of username/password pairs is most likely to be found as the primary database.

NOTE: *See Database Search Order on page 12-28 for an example of database precedence configuration.*

Precedence settings should be configured carefully. If a database is configured for a precedence slot that has already been filled by another database, it will take over the precedence setting and return all of the previous database type’s settings to their factory defaults.To check the database information, use the **Show Authentication** command. Databases are listed according to their precedence numbers.

It is important to realize that the LRS does not check the reasons for authentication failures, and in some cases, the remote host will not tell the LRS. If the authentication method with precedence 1 fails, the LRS will try the remaining authentication methods in order of precedence until one of them succeeds or all of them have failed, in which case the user is denied access to the LRS.

12.1.6.1 Local (NVR) Database

The local database is stored in the LRS NVR. Storing authentication information locally offers the following advantages:

- A network server is not required.
- Local authentication functions even when the network is down.
- Local authentication can execute and restrict user commands.
- CHAP may be used for authentication.

Disadvantages include:

- The LRS cannot share its databases with other servers.
- The LRS cannot share existing databases.
- The local database is limited by the size of the server's NVR.

12.1.6.1.1 Specifying the Precedence

A precedence must be specified in order to use the Local database. To specify the precedence, use the **Set/Define Authentication Local** command:

Figure 12-17: Specifying the Precedence

```
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 1
```

12.1.6.1.2 Username/Password Pairs

To add a username/password pair to the local database, use the **Set/Define Authentication Local** command:

Figure 12-18: Adding User and Password to Local Database

```
Local>> DEFINE AUTHENTICATION USER "elmo" PASSWORD "badger"
```

NOTE: *All passwords are case sensitive. All usernames are case insensitive.*

12.1.6.1.3 Forcing Execution of Commands

A command or series of commands may be associated with a particular username; the commands will be run when the user is successfully authenticated. For example, when user **elmo** logs into the LRS, he will be automatically telnetted to host **192.0.1.67** and logged out of the LRS.

Figure 12-19: Forcing Commands

```
Local>> DEFINE AUTHENTICATION USER "elmo" COMMAND "telnet 192.0.1.67; logout"
```

Commands must be enclosed in quotes. If a series of commands is specified, they must be separated by semicolons.

12.1.6.1.4 Permitting Users to Change Their Passwords

By default, users are not permitted to change their passwords. To enable a user to change his or her password, use the **Set/Define Authentication User Alter** command:

Figure 12-20: Permitting User to Change Passwords

```
Local>> DEFINE AUTHENTICATION USER “elmo” ALTER ENABLED
```

12.1.6.1.5 Forcing Selection of a New Password

Users may be forced to select a new password during their next login. This is useful when the user has forgotten his or her password, or to ensure that passwords are changed on a regular basis.

Figure 12-21: Forcing a User’s Password to Expire

```
Local>> DEFINE AUTHENTICATION USER “elmo” EXPIRED
```

12.1.6.1.6 Displaying the Local Database

Local database entries can be checked with the **Show/Monitor/List Authentication User** command. All users, their passwords, and other parameters are listed.

NOTE: *See Show/Monitor/List Authentication on page 13-148.*

12.1.6.1.7 Purging the Local Database

To remove a particular user from the database, use the **Clear/Purge Authentication User** command. See page 13-5 for a complete description of this command.

12.1.6.2 Kerberos

12.1.6.2.1 Introduction

The Kerberos Authentication Service is a network-based authentication service. Passwords are always transmitted in encrypted form. The LRS supports Kerberos version 4.

Kerberos is available as public-domain software and from commercial vendors. Please refer to your Kerberos server documentation for detailed information about setting up a Kerberos server, registering Kerberos clients, and administering a network that uses Kerberos.

Kerberos advantages include the following:

- Passwords are always encrypted; it is not possible to obtain a user’s password by eavesdropping on a connection attempt.
- Kerberos is a widely-accepted standard, and is proven to be secure.
- The LRS may easily be added to an existing Kerberos network.
- A large number of users may be supported.

Disadvantages include:

- Configuring the Kerberos database can be complicated.
- Kerberos only runs over IP.
- Kerberos does not guard against guessing a user's password.
- If the caller attempts to use CHAP for authentication, Kerberos cannot be used.

NOTE: *Kerberos authentication is case-sensitive.*

12.1.6.2.2 Configuration

1. Ensure that the LRS clock is synchronized with the clock on the Kerberos server. The Kerberos authentication model attaches timestamps to the packets sent between the LRS and Kerberos server to prevent replay attacks. The LRS timestamp is only allowed to deviate 5 minutes from the Kerberos server clock before the packet is considered invalid, which would result in a failed authentication attempt.

   To synchronize the LRS and the Kerberos clocks, use the **Set/Define IP Timeserver** command:

   Figure 12-22: Synchronizing the Clocks

   ```
   Local>> DEFINE IP TIMESERVER 192.0.1.110
   ```

2. Designate a precedence number for the Kerberos server
3. Configure the primary and secondary Kerberos server locations by IP address:

   Figure 12-23: Configuring Kerberos Precedence

   ```
   Local>> DEFINE AUTHENTICATION KERBEROS PRECEDENCE 2
   Local>> DEFINE AUTHENTICATION KERBEROS PRIMARY 192.0.1.52
   Local>> DEFINE AUTHENTICATION KERBEROS SECONDARY 192.0.1.53
   ```

4. Configure the realm. The **realm** is the name of the Kerberos administrative region that defines the scope of client authentication data maintained by a Kerberos server. Most installations choose realm names that mirror their Internet domain name system. To specify the realm, use the **Set/Define Authentication Kerberos Realm** command:

   Figure 12-24: Configuring the Kerberos Realm

   ```
   Local>> DEFINE AUTHENTICATION KERBEROS REALM PHRED.COM
   ```

5. Configure The **principle**, **instance** and **authenticator** that enable the Kerberos server to identify the LRS. Principle, instance, and authenticator entries must be configured on the LRS to match the corresponding entries on the Kerberos server.

   The default setting for the LRS principle is **rcmd**; for the LRS instance, the default setting is **lrs**.

The **authenticator** is the password for the principle/instance pair. It must be defined on the LRS and the Kerberos server. A text string or an eight-byte hexadecimal value may be specified.

To specify the LRS principle, instance, and authenticator, use the **Set/Define Authentication Kerberos** command:

Figure 12-25: Configuring the Principle, Instance, and Authenticator

```
Local>> DEFINE AUTH KERBEROS PRINCIPLE “kerbauth”
Local>> DEFINE AUTH KERBEROS INSTANCE “lrsname”
Local>> DEFINE AUTH KERBEROS AUTHENTICATOR “passwd”
Local>> DEFINE AUTH KERBEROS AUTHENTICATOR 0x08FF6D3E97735421
```

6. Configure the **Key Version Number** (KVNO). The key version number ensures that the LRS and Kerberos server are using the correct authenticator for the defined principle/instance pair. A KVNO must be configured on the LRS to match the KVNO on the Kerberos server.

   To configure the LRS KVNO, use the **Set/Define Authentication Kerberos KVNO** command:

Figure 12-26: Configuring the LRS KVNO

```
Local>> DEFINE AUTHENTICATION KERBEROS KVNO 1
```

NOTE: *By default, the KVNO is set to 1.*

For additional Kerberos configuration instructions, see **Set/Define Authentication** on page 13-62.

12.1.6.3 NetWare Bindery

NetWare file servers use a database called the **bindery**. The NetWare bindery offers the following advantages:

- An existing NetWare database may be used.
- The bindery is easy to manage.
- A large number of users may be supported.

Disadvantages include:

- If the caller attempts to use CHAP for authentication, the bindery cannot be used.
- The bindery is not compatible with NDS unless bindery emulation mode is used.

To store username/password pairs in the NetWare bindery, use the **Set/Define Authentication NetWare** command:

Figure 12-27: Configuring the LRS to Search a NetWare Bindery

```
Local>> DEFINE AUTHENTICATION NETWARE PRECEDENCE 3
Local>> DEFINE AUTHENTICATION NETWARE PRIMARY doc_server
Local>> DEFINE AUTHENTICATION NETWARE SECONDARY spare_server
```

NOTE: *NetWare authentication is not case-sensitive.*

12.1.6.4 RADIUS

The LRS supports the Remote Authentication for Dial-In User Services (RADIUS) protocol. RADIUS is a centrally-located client-server security system.

NOTE: *The LRS supports RADIUS as described in the Internet Engineering Task Force (IETF) RADIUS draft #5, and will support future versions and the eventual IETF standard when they become available.*

RADIUS is geared toward large networks that have many communications servers, or many users for which explicit security measures must be enforced. Its advantages are:

- Authentication information for multiple users, in multiple forms, can be stored in a single RADIUS server.
- The RADIUS server can be part of a local or wide-area network.
- RADIUS can be used with Kerberos and CHAP / PAP security.
- Passwords are not transmitted across the network in readable form.

Disadvantages include:

- Keeping authentication information on one server can be dangerous; the server should be backed up regularly.
- Those wishing to use RADIUS must use one of the database types that RADIUS supports (currently local RADIUS databases, UNIX password files, NIS files, Kerberos databases, and TACACS).
- RADIUS servers are subject to security attacks from users already on the network. More information can be found in the IETF draft and your RADIUS server's documentation.

RADIUS consists of two parts: authentication and accounting. Authentication is handled by the RADIUS authentication server, which stores authentication information configured by the network administrator. Accounting is handled by the RADIUS accounting server, which stores various statistical information about authenticated connections. RADIUS accounting and authentication can be implemented independently of one another.

NOTE: *For more information about RADIUS server configuration and operation, refer to your RADIUS server documentation.*

NOTE: *RADIUS authentication is case-sensitive if the Authentication server wants it to be.*

12.1.6.4.1 RADIUS Authentication

The general process of LRS user authentication using a RADIUS server is explained below.

1. A user connects to the LRS. The LRS prompts the user for a username and password, or CHAP / PAP authentication information if CHAP or PAP is configured.
2. The LRS creates an Access-Request packet that includes the username / password pair, an identification string for the LRS, the port being used for the modem connection, the port type, and other information as needed (see *Authentication Attributes* in Appendix E for more information). The LRS then encrypts the password and sends the packet to the RADIUS authentication server.

NOTE: *CHAP responses sent from the user's PPP software to the LRS are not encrypted beyond what is inherent to the operation of CHAP.*

3. The RADIUS authentication server decrypts the Access-Request packet and routes it to the appropriate security checking mechanism, such as a UNIX password file or Kerberos database. Based on the information returned from the security check, the RADIUS server does one of three things:

   A. If authentication is successful, the server sends an authentication acknowledgment (Access-Accept) packet to the LRS. This packet may contain additional information about the user's network system and connection requirements, such as the type of connection required and filtering information. The user is connected to a site or destination node if appropriate.

NOTE: *See Appendix E, Supported RADIUS Attributes, for more information about using filters with RADIUS.*

   B. If authentication fails, the server sends an Access-Reject packet to the LRS. The LRS will move on to the authentication method at the next precedence level, or terminate the connection if all methods have been tried.

   C. The server may be configured to send a challenge to the user attempting to log in. If this is the case, the LRS will print the server's challenge and prompt the user to enter a response. The user must respond to the challenge, at which time step 3 is repeated using the response in place of the password in the Access-Request Packet.

NOTE: *In order to respond to the challenge, the user must be in character mode which precludes the use of PAP or CHAP for authenticating the user. See RADIUS and Sites on page 12-14.*

To configure the LRS for RADIUS authentication, use the **Set/Define Authentication RADIUS** commands.

Figure 12-28: Configuring the LRS to use RADIUS Authentication

```
Local>> DEFINE AUTHENTICATION RADIUS PRECEDENCE 5
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.77
Local>> DEFINE AUTHENTICATION RADIUS SECONDARY 192.0.1.78 PORT 1620
```

In the example above, the third command tells the LRS to use port 1620 on the secondary RADIUS authentication server rather than the default RADIUS authentication port (port 1645).

NOTE: *See Set/Define Authentication RADIUS on page 13-67 for complete syntax and information.*

The secret string configured for the LRS must match that of the RADIUS server being used for authentication.

Figure 12-29: Configuring the RADIUS Secret

```
Local>> DEFINE AUTHENTICATION RADIUS SECRET “ok829dsnva1843qx”
```

For security reasons, it is recommended that you choose a secret string of at least 16 characters containing no obvious or easily-guessable items (such as names, phone numbers, or words that can be found in a dictionary).

12.1.6.4.2 RADIUS and Sites

When a user logs in via PPP or SLIP, the LRS looks for a site that has the same name as the user. If it finds a matching site, it starts that site and modifies it with whatever additional setup information the RADIUS server sends in its Access-Accept packet (see step 3A under *RADIUS Authentication*). If it does not find a matching site, it starts and modifies a copy of the default site.

NOTE: *Unless RADIUS specifically overrules a setting, the site's settings apply.*

If a user logs in using local mode but the RADIUS server indicates that this user should be using PPP or SLIP, the **Set Site** *sitename*; **Logout** command will be executed where *sitename* is the name of the RADIUS site created for this user.

NOTE: *Setting up sites for specific users should be done sparingly, and only when a user has special connection requirements that can't be met otherwise.*

If, on the other hand, the RADIUS server detects that a user logging in via PPP should actually be a local mode user, the connection will be denied. The reason for this is two-fold: the user would not be able to return to the local prompt once in PPP mode, and allowing the connection may create a security hole.

12.1.6.4.3 RADIUS Accounting

A RADIUS accounting server creates an accounting log based on information it gets from its client, such as an LRS. The server also responds to the client so that the client knows its packets reached the accounting server intact.

The LRS sends four types of packets to the accounting server:

Accounting-On Sent each time accounting is enabled or re-enabled on the LRS, and when the LRS boots with accounting enabled.

Accounting-Start Sent when a user logs into the LRS. This type of packet includes the user's name, port number, and current configuration.

NOTE: *EZCon users are logged as admin users.*

Accounting-Stop Sent when a connection is logged out or otherwise terminated. This type of packet includes the user's name, reason for logout, length of connection, and the counts of bytes and packets sent and received.

Accounting-Off Sent when accounting is disabled on the LRS, and when the LRS is about to shut down or reboot.

Accounting-Start and Accounting-Stop packets contain session IDs that are used to match them together. In order to generate the proper session IDs, the LRS must know the current time. It can be told the correct time by a timeserver (configured with Set / Define IP Timeserver or Set / Define IPX Timeserver) or by its internal clock (configured with Set / Define Server Clock). If the current time is not set properly, accounting packets may carry non-unique session IDs and cause problems in the accounting log.

NOTE: *See the RADIUS Attributes appendix for more information on the types of information that is included in accounting packets.*

To configure the LRS to send accounting information to the RADIUS accounting server, enter the **Set/Define Authentication RADIUS Accounting** command.

Figure 12-30: Configuring the LRS to use RADIUS Accounting

```
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING ENABLED
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING PRIMARY 192.0.1.130
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING SECONDARY 192.0.1.131
```

The default RADIUS Accounting port is port 1646. A different port can be specified by adding the Port parameter to the command as shown in the third line of Figure 12-28.

12.1.6.5 SecurID

The LRS supports the ACE/Server security system manufactured by Security Dynamics Technologies Inc. ACE/Server is a system of UNIX-based client-server software and accompanying token cards.

NOTE: *Refer to your Security Dynamics documentation for ACE/Server installation instructions.*

The SecurID card generates single-use, unpredictable numerical codes. These "cardcodes," together with the user's PIN, form the basis of the SecurID authentication. The PIN and generated cardcodes are referred to collectively as SecurID **passcodes**. To gain access to a network protected by SecurID, both elements of the passcode must be entered correctly.

SecurID advantages include the following:

- Three items are required for authentication: the token card, PIN, and user ID.
- The card's cardcode is constantly changing, thus changing the passcode that the user enters.
- If someone eavesdrops on a connection attempt and obtains a passcode, the passcode will not be useful; a new passcode will be required in a few minutes. This enhances the security of Telnet connections.

Disadvantages include:

- If the caller attempts to use CHAP for authentication, SecurID cannot be used.
- Users are required to carry the token card.
- SecurID cannot be used for LAN to LAN connections; the LRS has no way to generate passcodes.
- The SecurID server must be configured.

NOTE: *Secur-ID authentication is case-sensitive.*

The Security Dynamics SecurID system requires certain communication between the ACE/Server and the end-user. For example, the user must enter a new PIN when a SecurID card is first used, and a second passcode when locked out.

PAP does not allow for these types of messages or additional user input. Therefore, it is strongly recommended that SecurID be run from character mode only. It is possible to use SecurID with PAP, provided that situations like those mentioned above are either prevented or handled in text mode on the next call.

12.1.6.5.1 Using SecurID

To log into the LRS, the user must enter a username at the username prompt, and the passcode at the password prompt.

To specify the Secur-ID ACE/Server for authentication of username/passcodes, use the **Set/Define Authentication SecurID** command:

Figure 12-31: Configuring the LRS to Use SecurID

```
Local>> DEFINE AUTHENTICATION SECURID PRECEDENCE 4
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.50
Local>> DEFINE AUTHENTICATION SECURID SECONDARY 192.0.1.51
```

After SecurID is configured on the LRS, the LRS will receive further configuration information from the ACE/Server. However, this only happens the first time that the LRS and ACE/Server communicate. If you purge the authentication information on the LRS or change the precedence of SecurID, this learned information will be lost. You will need to have your ACE/Server administrator reinitialize the LRS with ACE/Server for SecurID to function properly again.

If SecurID receives repeated authentication requests for an invalid username/password pair, it assumes that a login attack is taking place. SecurID will react by continually slowing its responses to the LRS. This problem can be avoided by ensuring that SecurID has the highest precedence number. For example, if you're using SecurID, Kerberos, and a UNIX password file, set SecurID's precedence to 3.

For additional SecurID configuration instructions, see **Set/Define Authentication SecurID** on page 13-69.

12.1.6.6 UNIX Password File

Trivial File Transfer Protocol (TFTP) can be used to retrieve files from remote systems. During authentication, the LRS can TFTP a UNIX password file and check the username and password fields for the pair provided by a user. The LRS cannot add, modify, or delete password file entries.

NOTE: *The TFTP file is stored in UNIX /etc/passwd format. It must be in a location reachable via TFTP.*

UNIX password files are advantageous because existing UNIX password files can be used. Their main disadvantage is that TFTP poses a security risk. If the LRS can retrieve the file, chances are that other hosts on the network can retrieve the file and potentially crack the passwords. If your network is not trusted, you may not want to use TFTP authentication.

NOTE: *UNIX password file authentication is case-sensitive.*

To use a UNIX password file to authenticate users, use the **Set/Define Authentication TFTP** command:

Figure 12-32: Configuring the LRS to Use a UNIX Password File

```
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 5
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.50
Local>> DEFINE AUTHENTICATION TFTP SECONDARY 192.0.1.51
```

Specify the full pathname of the password file using the **Set/Define Authentication TFTP Filename** command:

Figure 12-33: Specifying the Pathname of the Password File

```
Local>> DEFINE AUTHENTICATION TFTP FILENAME "/tftpboot/passwd"
```

12.2 Outgoing LAN to LAN Authentication

When the LRS attempts to connect to a remote host, the host may require that the LRS send a username and password. The method used to transmit this username/password pair depends upon the type of login: character, SLIP, or PPP.

12.2.1 Character Mode Logins

If the remote device is expecting the information in character mode, the username and password must be sent in a chat script. The chat script should expect the username prompt, send the appropriate username, expect the password prompt, and send the appropriate password. See Chapter 4, *Additional Remote Networking*, for information on configuring chat scripts.

12.2.2 PPP Logins

If the remote device supports PPP, the username and password may be transmitted using CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol). Each protocol goes through a negotiation sequence to complete the authentication; see Chapter 3, *Basic Remote Networking*, for details.

To enable CHAP and PAP authentication on outgoing connections, use the **Define Site Authentication CHAP** and **Define Site Authentication PAP** commands. One or both may be enabled, however, CHAP is recommended.

Figure 12-34: Enabling PAP/CHAP Outgoing Authentication

```
Local>> DEFINE SITE dallas AUTHENTICATION CHAP ENABLED
Local>> DEFINE SITE dallas AUTHENTICATION PAP ENABLED
```

If both CHAP and PAP are configured for authentication, CHAP authentication will be attempted first. If the remote host does not understand CHAP, PAP will be attempted instead. If both PAP and CHAP fail, the connection will be terminated.

To define the username that the LRS sends to the remote host, use the **Define Site Authentication Username** command:

Figure 12-35: Configuring Site Username

```
Local>> DEFINE SITE dallas AUTHENTICATION USER "seattle"
```

The password sent to the remote host is called the **remote password**. Configure this password with the **Define Site Authentication Remote** command.

Figure 12-36: Configuring Site Remote Password

```
Local>> DEFINE SITE dallas AUTHENTICATION REMOTE “badger”
```

12.2.3 SLIP Logins

All outgoing SLIP authentication must be done with chat scripts before SLIP starts. SLIP does not support any authentication. To configure chat scripts, see Chapter 4, *Additional Remote Networking.*

12.3 User Restrictions

LRS users may be restricted in a number of ways. They may be prevented from using particular commands, forced to use a certain configuration, or forced to use a particular IP address.

12.3.1 Privileged Commands

Many of the LRS commands require privileged user (superuser) status. To become the privileged user, use the **Set Privileged** command. The default privileged password is **system**.

Figure 12-37: Set Privileged Command

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>>
```

NOTE: *To change the privileged password, use the Set/Define Server Privileged Password command, described on page 13-132.*

Only one user may have privileged status at any time. If another user currently has privileged status, the **Set Privileged Override** command may be used to forcibly become the privileged user. To stop being the privileged user, use the **Set Noprivileged** command.

12.3.2 Controlling Use of the Set PPP/SLIP Commands

In order for incoming callers to start PPP or SLIP with the Set PPP / SLIP commands, PPP or SLIP must be enabled on the port receiving the call. By default, PPP and SLIP are disabled.

To enable or disable PPP or SLIP on a port, use the Set / Define PPP / SLIP command:

Figure 12-38: Disabling PPP and SLIP

```
Local>> DEFINE PORT 2 PPP DISABLED
Local>> DEFINE PORT 2 SLIP DISABLED
```

12.3.3 Securing a Port

When a port is **secure**, users on that port will be prevented from editing many of the port's settings. In addition, they will only be able to display a limited amount of information using Show / Monitor / List commands.

NOTE: *Users logged in on secure ports cannot become privileged users.*

It is recommended to secure ports used for public use; for example, ports used for public dial-in modem pools. To secure a port, use the **Set/Define Ports Security** command:

Figure 12-39: Securing a Ports

```
Local>> DEFINE PORT 2 SECURITY ENABLED
```

NOTE: *The complete syntax of Set/Define Ports Security is listed on page 13-118.*

12.3.4 Locking a Port

The Lock command may be used to secure a port without disconnecting sessions. When **Lock** is entered, the user will be prompted to enter a password. The port will then be locked until this password is used to unlock it. Figure 12-40 displays an example.

Figure 12-40: Locking and Unlocking a Port

```
Local> LOCK
Password> donut (not echoed)
Verification> donut (not echoed)
Unlock password> donut (not echoed)
Local>
```

NOTE: *Secure ports (set using the Set/Define Ports Security command) cannot be locked.*

To unlock a port without the Lock password, a privileged user must use the **Unlock Port** command (page 13-166) or log out the port using the **Logout** command (page 13-51). Logout will disconnect all sessions.

12.3.5 Forcing Execution of Commands

When a username is entered in the local authentication database (NVR), a series of commands may be associated with that user. These commands will be executed when the user is successfully authenticated.

To execute commands when a user logs into the LRS, first ensure that authentication databases have been configured; see *Database Configuration* on page 12-7 for instructions. Then associate commands with the username using the **Set/Define Authentication User Command** command. The commands you specify will be executed when the user is successfully authenticated.

Figure 12-41: Forcing User to Start a Particular Site

```
Local>> DEFINE AUTHENTICATION USER bob COMMAND “SET PPP dialin_users; logout”
```

In the previous example, when user **bob** logs into the LRS, he will automatically start PPP and run the site **dialin_users**.

NOTE: *Another example appears under Terminal User Forced to Execute Command on page 12-29.*

To ensure that the user is not left at the Local> prompt after the forced command finishes executing, the string ";logout" may be added.

12.3.6 Restricting Multiple Authenticated Logins

The **Set/Define Authentication Unique Enabled** command can be used to prevent a single PPP or Local mode user from making multiple authenticated connections to the LRS.

For example, imagine that ports 1 through 8 have authentication enabled, but ports 9 through 16 do not. If user **george** connects to port 2 and enters the correct password, he will be permitted to log in. If while george is connected to port 2, another user tries to log into port 3 using george as his username, he will be rejected.

Unique authentication applies only to ports that have authentication enabled. If user george connects to port 2 and then attempts a second connection to port 9, the second login will be allowed because port 9 does not have authentication enabled. Similarly, if george attempts an authenticated login to port 2 after another user has logged into port 9 with username george, he will succeed (provided that he enters the correct password) because he is the first user to log in as george on an authenticated port.

To enable unique authentication, enter the following command:

Figure 12-42: Preventing Multiple Authenticated Logins by Single Users

```
Local>> DEFINE AUTHENTICATION UNIQUE ENABLED
```

12.3.7 Menu Mode

For added security, ports may be configured to run **menu mode**. When a port is in menu mode, users that log into the port will be presented with a list of menu options. They will be limited to the choices listed on the menu, and will not be permitted to enter text commands.

To set up a menu, use the **Set/Define Menu** command. For each menu entry, specify the option's numbered position in the table, the option name that will be listed, and the actual command invoked when the user chooses that option. Option and command names must be enclosed in quotes.

Figure 12-43: Adding Command Entry to Menu Mode

```
Local>> DEFINE MENU 4 "Telnet irvine" "TELNET 192.0.1.53"
```

It is good idea to add a command to the menu that allows the user to log out of the server.

Figure 12-44: Adding Logout Command to Menu

```
Local>> DEFINE MENU 10 "Exit" "Logout Port"
```

To display the current menu, use the **Show/Monitor/List Menu** command.

To enable menu mode on a particular port, use the **Set/Define Ports Menu** command:

Figure 12-45: Configuring Port to Run Menu Mode

```
Local>> DEFINE PORT 2 MENU ENABLED
```

12.3.8 IP Address Restriction

To avoid routing problems and enhance security, the LRS can restrict incoming remote networking callers to a particular address or range of addresses.

Each site may specify a particular range of acceptable IP addresses. When an incoming caller requests to use a specific address, it will be compared to this range. If the address falls within the range, the connection will be permitted, if not, the connection attempt will fail.

To specify the beginning and end of the range, use the **Define Site IP Remoteaddress** command. Two addresses must be specified: the beginning of the range, and the end of the range.

Figure 12-46: Specifying Range of Addresses

```
Local>> DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.254
```

Callers will not be permitted to use IP addresses with the host part of the address set to all zeroes or all ones. These addresses are reserved to identify broadcast packets. If the range that you specify includes such an address (for example, 192.4.5.0 or 192.4.5.255) and a caller requests this address, the connection will not be permitted.

NOTE: *For more information on IP address assignment, see IP, IPX, and AppleTalk Addressing on page 3-6.*

12.4 Network Restrictions

12.4.1 Incoming Telnet/Rlogin Connections

Incoming Telnet and Rlogin connections can be permitted without restriction, password protected, or prevented entirely. By default, incoming Telnet and Rlogin connections are permitted without entering the login password; to change this configuration, use the **Set/Define Server Incoming** command:

Figure 12-47: Preventing Incoming Telnet / Rlogin Logins

```
Local>> DEFINE SERVER INCOMING NONE
Local>> DEFINE SERVER INCOMING PASSWORD
```

NOTE: *For the complete syntax of the Set/Define Server Incoming command, see page 13-128.*

In Figure 12-47, the first command prevents all incoming Telnet and Rlogin connections. The second command permits the connections, but requires that the login password be entered before the connection is permitted.

12.4.2 Outgoing Rlogin Connections

The Set / Define Server Rlogin setting controls whether or not outgoing Rlogin connections are permitted. By default, outgoing Rlogin is disabled; to change this setting, use the following command:

Figure 12-48: Permitting Outgoing Rlogin Connections

```
Local>> DEFINE SERVER RLOGIN ENABLED
```

To configure incoming Rlogin connections, see *Incoming Telnet/Rlogin Connections* on page 12-21.

12.4.3 Port Access

A port's access may be set to one of the following: dynamic, local, remote, or none. **Dynamic** permits both local and remote logins, **local** permits only local logins, and **remote** permits only remote logins. **None** prevents all incoming and outgoing connections; the port is unusable.

To configure a port's access setting, use the **Set/Define Ports Access** command.

Figure 12-49: Configuring Connection Type

```
Local>> DEFINE PORT 2 ACCESS REMOTE
Local>> DEFINE PORT 2 ACCESS DYNAMIC
```

NOTE: *For more information about configuring a port's access, refer to Accessing a Port on page 9-1.*

12.4.4 Packet Filters and Firewalls

Filters enable the LRS to restrict packet traffic. Each filter specifies a particular rule, for example, only IP packets will be permitted passage. Packets that pass the filter will be forwarded; packets that don't will be discarded.

Filters are organized into ordered filter lists, which are referenced by name. For example, a filter named **firewall** may permit forwarding of packets that match a particular IP rule, but deny passage to packets that match a generic rule.

NOTE: *For a complete explanation of filter rules, see Set/Define Filter on page 13-74.*

Filter lists are associated with sites. Sites use filter lists for the following purposes:

Table 12-1: Types of Filter Lists

Type of Filter List	Purpose
Idle	Determines whether the site will remain active. Packets that pass the filter will reset the site's idle timer, preventing the site from being timed out.
Incoming	Determines whether to forward incoming packets received from a remote site. Packets that pass the filter will be forwarded.
Outgoing	Determines whether to forward outgoing packets to a remote site. Packets that pass the filter will be forwarded.
Startup	Determines whether a site will initiate a connection to a remote site. When a packet passes the filter, the LRS will initiate an outgoing connection. (If an outgoing connection currently exists, this filter will be ignored).

When a site with an associated filter list receives a packet, the LRS will compare the packet against each filter starting with the first filter on the list. If the packet matches any of the filters, the packet will be forwarded or discarded according to the filter's specification. If the packet does not match any of the filters in the list, it will not be forwarded.

12.4.4.1 Filter Order

The order that filters appear in a list is important. For example, consider the following filter list.

1. Allow any packets
2. Deny all IP traffic matching a particular rule

When this filter list is associated with a site, all packets will be forwarded. Packets will be compared to the first filter in the list, and all packets will match specification "any packets". Therefore, all packets will be forwarded without being compared to the second filter.

Switching the order of the filters will have very different effects. Examine the filter list below, where the order of the two filters is reversed.

1. Deny all IP traffic matching a particular rule
2. Allow any packets

When this filter list is used, any IP traffic matching the specified rule will be discarded. Therefore, some IP packets will be discarded without being compared to the second filter.

12.4.4.2 Preventing all IP, IPX, or AppleTalk Traffic

To prevent all packet traffic from a particular protocol (for example, all IP packets), filter lists do not need to be used. Use the **Define Site IP**, **Define Site IPX**, or **Define Site AppleTalk Disabled** command:

Figure 12-50: Preventing IPX Packet Traffic

```
Local>> DEFINE SITE irvine IPX DISABLED
```

12.4.4.3 Setting up Filter Lists

Configuring filter lists involves two primary steps: creating the filter list, and associating the list with a particular site.

12.4.4.3.1 Creating a Filter List

When a filter list is created, it must be assigned a name of no more than 12 characters. The remainder of the configuration consists of a series of rules that will filter packet traffic in a particular way.

Use the **Set/Define Filter** command to create a new filter.

Figure 12-51: Define Filter Command

```
Local>> DEFINE FILTER firewall ADD 1 DENY IP SRC 192.0.1.0 255.255.255.0
```

Each rule is assigned a particular position in the filter list, denoted by a number. In Figure 12-51, the rule **Deny IP** will be added to the **firewall** filter in the first position of the list. If a position number isn't specified with the Set / Define Filter command, the rule will be added to the end of the filter list.

NOTE: *Set/Define Filter has many parameters. Please refer to page 13-74 for the complete syntax of this command.*

12.4.4.3.2 Associating a Filter List With a Site

A single filter list can be associated with many sites. Each site may use a filter list as an incoming, outgoing, startup, or idle filter.

NOTE: *Filter list types are described in Table 12-1 on page 12-23.*

To associate a filter list with a site, use the **Define Site Filter** command.

Figure 12-52: Associating a Filter List With Sites

```
Local>> DEFINE SITE irvine FILTER IDLE firewall
Local>> DEFINE SITE dallas FILTER INCOMING firewall
```

In Figure 12-52, filter **firewall** will be used as an idle filter for site **irvine**, and as an incoming filter for site **dallas**.

NOTE: *An example firewall setup is described in Creating a Firewall on page 12-31.*

NOTE: *Filters can also be used with RADIUS. See the Filter-ID attribute on page E-3 for more information.*

12.5 Event Logging

Event logging enables a network administrator to track network and user activity.

Logging can be configured at a number of levels. For example, one level of logging may record only system problems related to authentication, and another level may record all authentication activities (all passwords).

12.5.1 Destination

In order to use logging, the LRS must be configured to send logging information to one of following destinations:

- A TCP/IP host running **syslog**
- A Novell fileserver

NOTE: *If you intend to log information to a Novell fileserver, you must add the LRS as a print server using PCONSOLE.*

- The LRS memory
- The LRS serial console port, typically port 1

To specify the logging destination, use the **Set/Define Logging Destination** command:

Figure 12-53: Specifying Logging Destination

```
Local>> DEFINE LOGGING DESTINATION CONSOLE
Local>> DEFINE LOGGING DESTINATION 192.0.1.5:
Local>> DEFINE LOGGING DESTINATION betty:
```

NOTE: *The complete syntax of Set/Define Logging is given on page 13-96.*

A colon must be appended to the IP address or IP host name. Use of an IP address is suggested. A backslash (\) must be appended to Novell fileserver names.

To see logging information that is stored in the LRS memory, enter the **Show/Monitor/List Logging Memory** command. The following command will display the log and update the display continuously.

Figure 12-54: Displaying Logging Saved to Memory

```
Local>> MONITOR LOGGING MEMORY
```

12.5.2 Logging Levels

The following table lists the different areas that can be logged and the logging options available for each area:

Table 12-2: Events Logged by the LRS

To Log Events Associated With:		The Following Options are Available: (Numbers Reflect Logging Level)
AppleTalk	1	Errors
	2	Packets that Trigger Remote Connections
	3	Routing Table / Interface Changes
	4	Incoming / Outgoing RTMP / ZIP Packets
Authentication	1	System Problems
	2	Failures and Successes
	3	All Logins and Logouts
	4	Incorrect Passwords
	5	All Passwords, and RADIUS Warnings
Commands		Enabled
		Disabled
Dialback	1	Problems
	2	Unauthorized Users
	3	Dialback Failures
	4	Dialback Successes
	5	Dialback Attempts
	6	Modem Chat
IP	1	Errors
	2	Packets that Trigger Remote Connections
	3	Routing Table / Interface Changes
	4	Incoming / Outgoing RIP Packets
	5	Resulting Routing Table
	6	Contents of All RIP Packets
	7	Routed Packets

Table 12-2: Events Logged by the LRS, cont.

To Log Events Associated With:		The Following Options are Available: (Numbers Reflect Logging Level)
IPX	2	Critical Conditions
	3	Error Conditions
	4	Warnings
	5	Normal but Significant Conditions
	6	Informational Messages
	7	Debug-level Messages
Modems	1	Problem
	2	Call Statistics Dump From Modem
	3	Setup
Networks		Enabled
		Disabled
PPP	1	Local System Problems
	2	Remote System Problems
	3	Negotiation Failures
	4	Negotiation Data
	5	State Transitions
	6	Full Debugging
Printers		Enabled
		Disabled
Sites	1	Usage Summary
	2	Detailed Usage Summary
	3	Errors
	4	Connections
	5	Bandwidth
	6	Network Addressing
	7	Chat Scripts
	8	Modems and Dialback
System		Enabled
		Disabled

For example, to record all logins and send the information to the console port, use the following command:

Figure 12-55: Logging All Logins

```
Local>> DEFINE LOGGING AUTHENTICATION 3
```

NOTE: *Caution: Logging passwords may compromise security.*

Each logging level logs all events associated with lower logging levels. For example, if logging level 6 is specified, the events associated with levels 1-5 will also be logged.

To disable all logging of a particular area (for example, IPX), use the **Set/Define Logging None** command:

Figure 12-56: Disabling IPX Logging

```
Local>> DEFINE LOGGING IPX NONE
```

To disable all logging, use the following command:

Figure 12-57: Disabling Event Logging

```
Local>> DEFINE LOGGING DESTINATION NONE
```

12.6 Examples

12.6.1 Database Search Order

The LRS must be configured for authentication using an existing NetWare bindery and UNIX password file. The configuration must meet the following criteria:

- The majority of users are listed in the NetWare bindery, located on the **doc_server** NetWare file server.
- A large group of users is listed in a RADIUS authentication database. The RADIUS server's IP address is 192.0.1.55, and port 1640 is used rather than the default RADIUS authentication port.
- Two other groups of users are listed in UNIX password files; the files are on hosts 192.0.1.87 and 192.0.1.99.
- Any additional users will be added to the local database.
- A RADIUS accounting server has been set up at host 192.0.1.176 to log accounting information.

Figure 12-58 shows how to configure the LRS in this situation:

Figure 12-58: Configuring Database Order

```
Local>> DEFINE AUTHENTICATION NETWARE PRECEDENCE 1
Local>> DEFINE AUTHENTICATION NETWARE PRIMARY doc_server
Local>> DEFINE AUTHENTICATION RADIUS PRECEDENCE 2
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.55 PORT 1640
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 3
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.87
Local>> DEFINE AUTHENTICATION TFTP SECONDARY 192.0.1.99
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 4
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING ENABLED
Local>> DEFINE AUTHENTICATION RADIUS ACCOUNTING PRIMARY 192.0.1.176
```

12.6.2 Terminal User Forced to Execute Command

Terminal user **jerry** does not have an existing account on UNIX or the NetWare fileserver. He will only use the LRS to Telnet to his own remote host, **venus**. The following figure shows the commands necessary to add jerry to the local database.

Figure 12-59: A Single User Entry

```
Local>> DEFINE AUTHENTICATION USER “jerry” PASSWORD “3no37” COMMAND “TELNET
venus;LOGOUT” ALTER DISABLED
```

When jerry connects to the LRS, he is prompted for a login password, then his own username and password. When authenticated, he is automatically telnetted to host venus and logged out of the LRS.

Jerry will see the following:

Figure 12-60: Results of User Authentication with Command

```
Type HELP at the ‘Local_1>’ prompt for assistance.

Login password> badger (not echoed)
Username> jerry
Password> 3no37 (not echoed)

Telnet/TCP protocol emulation v2.2
SunOS UNIX (venus)
Login:_
```

12.6.3 Multiple-User Authentication

A large number of users need to connect to the LRS. These users must be authenticated. The LRS must be configured to meet the following criteria:

- All users will connect to port 2.
- 50 users have their usernames and passwords stored in a UNIX password file.
- Another 20 users are PPP users that share site **pppUsers** for their connections. This site's password is **special**.
- There is one SLIP user that will use site **SlipMan**. This site has password **exception**; once the password is entered, the site must automatically enter SLIP mode.

Port 2 must be configured to automatically detect PPP so that it can begin running PPP and CHAP when necessary. The port must not be dedicated to PPP, however, because other connections will be using the same port.

In order to authenticate the SLIP user, SLIPdetect must be disabled.

Figure 12-61 displays the commands necessary for this configuration:

Figure 12-61: Authentication for Multiple Users

```
Local>> DEFINE AUTHENTICATION TFTP PRECEDENCE 1
Local>> DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.88
Local>> DEFINE PORT 2 AUTHENTICATE ENABLED

Local>> DEFINE SITE PPPusers LOCAL “special”
Local>> DEFINE PORT 2 PPPDETECT ENABLED

Local>> DEFINE PORT 2 SLIPDETECT DISABLED
Local>> DEFINE SITE “SlipMan” IP REMOTEADDRESS 192.0.1.17
Local>> DEFINE SITE “SlipMan” LOCAL “exception”
Local>> DEFINE SITE “SlipMan” PROTOCOL SLIP
```

12.6.4 Outgoing LAN to LAN Connection

An LRS in Dallas must connect to an LRS in Seattle. The Dallas LRS must be configured in the following manner:

- The LRS in Dallas must have a site for the connection to the Seattle LRS. The site's name is **seattle**.
- PPP will be used for the connection.
- PAP authentication will be used.
- To authenticate itself, the LRS in Dallas must send username **dallas** and password **texas**.

The following commands must be entered on the Dallas LRS:

Figure 12-62: Configuring Remote Site Authentication

```
Local>> DEFINE SITE seattle AUTHENTICATION PAP ENABLED
Local>> DEFINE SITE seattle AUTHENTICATION USERNAME dallas
Local>> DEFINE SITE seattle AUTHENTICATION REMOTE “texas”
```

12.6.5 Creating a Firewall

If your site involves an internet connection, it is a good idea to set up a firewall to augment current security. A firewall prevents outside users from freely accessing your network by controlling which services on your network are available to internet users.

A local network consists of addresses **192.0.1.0** through **192.0.1.24**. Site **irvine** is used to manage connections to this network. Irvine requires a firewall that does the following:

- Prevents IP spoofing
- Permits outgoing Telnet connections
- Permits SMTP (Simple Mail Transfer Protocol) traffic to the local SMTP server, **192.0.1.102**. The backup SMTP server is **192.0.1.103**
- Permits NNTP (Network News Transfer Protocol) traffic between the local NNTP server, **192.0.1.104**, and the remote NNTP server, **192.0.2.100**
- Permits outgoing FTP connections
- Denies X-Windows traffic, but permits incoming TCP/IP traffic to ports 1023 and higher.
- Permits DNS queries to the local Domain Name Server, **192.0.1.101**
- Permits ICMP (Internet Control Message Protocol) messages
- Permits outgoing finger requests

The firewall will be named **fw_i**. Packets that do not specifically match the filters in fw_i will be denied passage through the LRS.

NOTE: *Due to the length of the commands in the following examples, the keywords Define and Filter are shortened to **Def** and **Filt**.*

The **Set/Define Filter Create** command is used to create the firewall.

Figure 12-63: Creating the Filter List

```
Local>> DEF FILT fw_i CREATE
```

To prevent IP spoofing, the **Define Filter Add Deny IP SRC** command is used. This filter will block any packets from an outside network that claim to have originated from the local network.

This filter is placed at the beginning of the filter list; if it were not, spoofed IP packets could be permitted passage by filters positioned before this rule.

Figure 12-64: Preventing IP Spoofing

```
Local>> DEF FILT fw_i ADD DENY IP SRC 255.255.255.0 192.0.1.0
```

NOTE: *The CERT advisory on IP spoofing is available from* ***ftp://cert.org/pub/cert_advisories/CA-95:01.IP.spoofing****.*

To permit outgoing Telnet connections initiated from the local network, the following command is used:

Figure 12-65: Permitting Outgoing Telnet Connections

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ TELNET DPORT GT 1023 ACK
```

To permit SMTP traffic between the LRS and the local and backup SMTP servers, the following commands are required:

Figure 12-66: Permitting SMTP Traffic to SMTP Servers

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ SMTP SPORT GT 1023 DST 255.255.255.255
192.0.1.102

Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ SMTP DPORT GT 1023 ACK DST
255.255.255.255. 192.0.1.102

Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ SMTP SPORT GT 1023 DST 255.255.255.255
192.0.1.103

Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ SMTP DPORT GT 1023 ACK DST
255.255.255.255 192.0.1.103
```

To permit NNTP traffic between the local and remote NNTP servers, the following commands are required:

Figure 12-67: Permitting Traffic Between NNTP Servers

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ NNTP SPORT GT 1023 DST 255.255.255.255
192.0.1.104 SRC 255.255.255.255 192.0.2.100

Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ NNTP DPORT GT 1023 ACK DST
255.255.255.255 192.0.1.104 SRC 255.255.255.255 192.0.2.100
```

To permit outgoing FTP connections, the following commands are used:

Figure 12-68: Permitting Outgoing FTP Connections

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FTP DPORT GT 1023 ACK

Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FTPDATA DPORT GT 1023
```

The following three commands deny incoming X-Windows traffic to well-known ports 6000-6023, but permit incoming TCP/IP connections to ports greater than 1023. This configuration also allows PASV-mode FTP data.

Figure 12-69: Controlling X-Windows Traffic

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT GT 1023 DPORT GT 6024 ACK
Local>> DEF FILT fw_i ADD DENY IP TCP SPORT GT 1023 DPORT GE 6000 ACK
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT GT 1023 DPORT GT 1023 ACK
```

The three commands below permit UDP- and TCP-based queries and answers to the local Domain Name Server:

Figure 12-70: Permitting DNS Queries

```
Local>> DEF FILT fw_i ADD ALLOW IP UDP DPORT EQ DNS DST 255.255.255.255 192.0.1.101
Local>> DEF FILT fw_i ADD ALLOW IP TCP DPORT EQ DNS SPORT GT 1023 DST 255.255.255.255
192.0.1.101
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ DNS DPORT GT 1023 ACK DST
255.255.255.255 192.0.1.101
```

To permit ICMP messages (except for redirect messages), a generic IP rule is defined:

Figure 12-71: Permitting ICMP Messages

```
Local>> DEF FILT fw_i ADD ALLOW IP ICMP IPGENERIC OFFSET 0 MASK 0xf0000000 NE 0x50000000
```

Outgoing finger requests are permitted and incoming requests are prevented using this command:

Figure 12-72: Permitting Outgoing Finger Requests

```
Local>> DEF FILT fw_i ADD ALLOW IP TCP SPORT EQ FINGER DPORT GT 1023 ACK
```

To use firewall fw_i as an incoming filter list for site **irvine**, the **Define Site Filter Incoming** command is used:

Figure 12-73: Configuring a Firewall

```
Local>> DEF SITE irvine FILTER INCOMING fw_i
```

12.6.6 Dialback

An LRS must be configured to prevent all users from connecting with the exception of two users, **sam** and **paul**. When sam and paul attempt to connect to the LRS, the modem must dial them back to verify their identities.

The modem is connected to LRS port 2, and there isn't a corresponding modem profile. The generic modem profile must be used. The following example assumes that modem profile type 3 is the generic modem profile (Use the List Modem command to view available modem profiles).

Figure 12-74: Enabling Modem Handling / Selecting a Modem Type

```
Local>> DEFINE PORT 2 MODEM ENABLED
Local>> DEFINE PORT 2 MODEM TYPE 3
%Info: Port speed changed to 57600.
%Info: Port flow control changed to CTS.
```

The following commands are used to configure dialback:

Figure 12-75: Configuring Dialback

```
Local>> DEFINE PORT 2 DIALBACK ENABLED
Local>> DEFINE DIALBACK sam “123-4567”
Local>> DEFINE DIALBACK paul “867-5309”
Local>> DEFINE DIALBACK BYPASS DISABLED
Local>> LOGOUT PORT 2
```

12.7 Troubleshooting

To troubleshoot authentication problems, use event logging. To configure event logging, use the **Set/Define Logging** command, discussed on page 13-96. The following example assumes the terminal is connected to the console port (port 1).

Figure 12-76: Configuring Authentication Event Logging

```
Local>> SET LOGGING DESTINATION CONSOLE
Local>> SET LOGGING AUTHENTICATION 4
Fri Jan 26 13:44:40 1996 LRS_00DD12: SYSTEM: notice: log closed
Fri Jan 26 13:44:40 1996 LRS_00DD12: SYSTEM : notice: syslog started
Fri Jan 26 13:44:49 1996 LRS_00DD12: AUTH: info: Denied Port 4 User john Password
badpass Method Local
Fri Jan 26 13:45:27 1996 LRS_00DD12: AUTH: info: Granted Port 4 User john Password
goodpass Method Local
Fri Jan 26 13:45:39 1996 LRS_00DD12: AUTH: notice: Port 4 user john privilege password
denied.
Fri Jan 26 13:45:49 1996 LRS_00DD12: AUTH: notice: Port 4 user john privilege password
granted.
```

12.8 Quick Reference

Incoming Authentication: Character Mode Logins			
To	**Use This Command**	**Example(s)**	**What Example Does**
Set the Login Password	Set / Define Server Login Password, page 13-129.	`DEFINE SERVER LOGIN PASSWORD badger`	Defines “badger” as the LRS login password. See *Login Password* on page 12-1 for more information.
Require the Login Password for Character Mode Logins to a Particular Port	Set / Define Ports Password, page 13-116.	`DEFINE PORT 2 PASSWORD ENABLED`	Requires the login password for character mode logins to port 2. See *Login Password* on page 12-1 for more information.
Enable Username / Password Authentication for a Particular Port	Set / Define Ports Authenticate, page 13-104.	`DEFINE PORT 2 AUTHENTICATION ENABLED`	Requires a username / password pair for character mode logins to port 2. See *Username/Password Pairs* on page 12-2 for more information.
Use Dialback for Character Mode Logins	1. Define Ports Modem Control, page 13-20.	`DEFINE PORT 2 MODEM CONTROL ENABLED`	Enables modem operation on port 2. See *Dialback from Local Mode* on page 12-5 for more information.
	2. Define Ports Modem Type, page 13-27.	`DEFINE PORT 2 MODEM TYPE 11`	Applies the settings in modem profile 11 to port 2.
	3. Define Ports Dialback, page 13-15.	`DEFINE PORT 2 DIALBACK ENABLED`	Enables dialback operation on port 2.
	4. Define Ports Dialback Bypass, page 13-15.	`DEFINE DIALBACK BYPASS DISABLED`	Controls what happens when users not in the dialback database attempt to a connection to the LRS. In this example, users not in the database will not be able to connect.

Incoming Authentication: Character Mode Logins, cont.

To	Use This Command	Example(s)	What Example Does

Use Dialback for Character Mode Logins, cont.	5. Set / Define Dialback Bypass, page 13-73.	`DEFINE DIALBACK FRANK BYPASS`
		
		`DEFINE DIALBACK BOB "555-1235"`
			Adds users "Frank" and "Bob" to the dialback database. User Frank will be permitted to connect to the LRS without dialback occurring. When Bob attempts to connect, he will be dialed back at 555-1235.
			
			All other users will be prevented from connecting.

Prompt Users for a Site's Local Password When the Set PPP / Set SLIP Command is Used	Define Site Authentication Prompt, page 13-32.	`DEFINE SITE irvine AUTHENTICATION PROMPT ENABLED`	When a user enters Set PPP <sitename> or Set SLIP <sitename>, they will be prompted for that site's local password. See *Starting PPP/SLIP From Character Mode* on page 12-4 for more information.

Incoming Authentication: Virtual Port Logins

To	Use This Command	Example(s)	What Example Does
Require the Login Password for Incoming Telnet and Rlogin Attempts	Set / Define Server Incoming, page 13-128.	`DEFINE SERVER INCOMING PASSWORD`	Required that incoming Telnet and Rlogin users enter the LRS login password. See *Virtual Port Logins* on page 12-2 or *Login Password* on page 12-1 for more information.
Require Username / Password Authentication on Virtual Ports	Set / Define Ports Authenticate, page 13-104.	`DEFINE PORT 0 AUTHENTICATE ENABLED`	Requires a username / password pair for incoming Telnet / Rlogin connections. See *Virtual Port Logins* on page 12-2 for more information.

Incoming Authentication: PPP Logins

To	Use This Command	Example(s)	What Example Does
Use CHAP to Authenticate Incoming Callers	Define Ports PPP CHAP Remote, page 13-29.	`DEFINE PORT 2 PPP CHAP REMOTE`	Uses CHAP to transmit the incoming username / password pair. See *How the Username/Password is Transmitted* on page 12-2 for more information.
Use PAP to Authenticate Incoming Callers	Define Ports PPP PAP Remote, page 13-29.	`DEFINE PORT 2 PPP PAP REMOTE`	Uses PAP to transmit the incoming username / password pair. See *How the Username/Password is Transmitted* on page 12-2 for more information.
Define the Password Expected From the Incoming Caller for a Particular Site	Define Site Authentication Local, page 13-32.	`DEFINE SITE irvine AUTHENTICATION LOCAL "wallaby"`	Defines "wallaby" as the local password for site irvine. When an incoming caller enters "irvine" and "wallaby" as its username and password, site irvine will be used to manage the connection. See *Comparing the Username/Password to Authentication Databases* on page 12-3 for more information.
Send a Username / Password Pair to the Remote Host	Define Site Authentication Username, page 13-32.	`DEFINE SITE irvine AUTHENTICATION USERNAME seattle`	When the remote host requests authentication information from site irvine, the LRS will send "seattle" as its username. See *Offering Authentication Information to the Incoming Caller* on page 12-3 for more information.
		`DEFINE SITE irvine AUTHENTICATION REMOTE gopher`	When the remote host requests authentication information from site irvine, the LRS will send "gopher" as its password.
	Define Ports PPP CHAP Local, page 13-29.	`DEFINE PORT 2 PPP CHAP LOCAL`	Uses CHAP to send a username / password pair to the remote host.
	Define Ports PPP PAP Local, page 13-29.	`DEFINE PORT 2 PPP PAP LOCAL`	Uses PAP to send a username / password pair to the remote host.

Incoming Authentication: PPP Logins, cont.

To	Use This Command	Example(s)	What Example Does
Use Dialback to Authenticate Incoming PPP Users	Define Site Authentication Dialback, page 13-32.	`DEFINE SITE irvine AUTHENTICATION DIALBACK ENABLED`	Enables dialback for PPP users using site “irvine”. See *Dialback* on page 12-6 for more information.

Incoming Authentication: SLIP Logins

To	Use This Command	Example(s)	What Example Does
Authenticate Users Before SLIP is Started	Set / Define Ports SLIPdetect, page 13-120.	`DEFINE PORT 2 SLIPDETECT DISABLED`	Disables SLIP autodetection on port 2. See *SLIP Logins* on page 12-4 for more information.
	Define Ports SLIP, page 13-31.	`DEFINE PORT 2 SLIP DISABLED`	Disables dedicated SLIP on port 2.
	Define Ports SLIP, page 13-31.	`DEFINE PORT 2 SLIP ENABLED`	Re-enables SLIP on port 2.
Use Dialback to Authenticate Incoming SLIP Users	Define Site Authentication Dialback, page 13-32.	`DEFINE SITE irvine AUTHENTICATION DIALBACK ENABLED`	Enables dialback for SLIP users using site “irvine”. See *Dialback* on page 12-6 for more information.

Incoming Authentication: General

To	Use This Command	Example(s)	What Example Does
Prevent a User from Making Multiple Authenticated Logins	Set / Define Authentication Unique, page 13-72.	`DEFINE AUTHENTICATION UNIQUE ENABLED`	Prevents a single user from logging into more than one authentication-enabled port. See *Restricting Multiple Authenticated Logins* on page 12-20 for more information.

Authentication Databases: Local

To	Use This Command	Example(s)	What Example Does
Specify the Precedence of the Local Database (NVR)	Set / Define Authentication Local Precedence, page 13-62.	`DEFINE AUTHENTICATION LOCAL PRECEDENCE 1`	When an incoming caller submits a username / password pair, it will be compared to the local database before other databases. See *Specifying the Precedence* on page 12-8 for more information.
Add a Username / Password Pair to the Local Database	Set / Define Authentication User Password, page 13-72.	`DEFINE AUTHENTICATION USER "elmo" PASSWORD "badger"`	Adds user "elmo" and its corresponding password, "badger" to the local database. See *Username/Password Pairs* on page 12-8 for more information.
Execute a Series of Commands When a Particular User Logs into the LRS	Set / Define Authentication User Command, page 13-72.	`DEFINE AUTHENTICATION USER "elmo" COMMAND "telnet 192.0.1.67; logout"`	When user "elmo" logs into the LRS, he will be automatically telnetted to host 192.0.1.67. See *Forcing Execution of Commands* on page 12-8 for more information.
Permit a Particular User to Change His / Her Password	Set / Define Authentication User Alter, page 13-72.	`DEFINE AUTHENTICATION USER "elmo" ALTER ENABLED`	Permits user "elmo" to change his password. See *Permitting Users to Change Their Passwords* on page 12-9 for more information.
Force a Particular User to Enter a New Password Upon Next Login	Set / Define Authentication User Expired, page 13-72.	`DEFINE AUTHENTICATION USER "elmo" EXPIRED`	Requires that user "elmo" enter a new password the next time he logs into the LRS. See *Forcing Selection of a New Password* on page 12-9 for more information.

Authentication Databases: Local, cont.

To	Use This Command	Example(s)	What Example Does
Display the Current Entries in the Local Database	Show / Monitor / List Authentication Users, page 13-148.	`SHOW AUTHENTICATION USERS`	Displays information about the current users in the local database. See *Displaying the Local Database* on page 12-9 for more information.
Remove a Particular User From the Local Database	Clear / Purge Authentication User, page 13-5.	`PURGE AUTHENTICATION USER "elmo"`	Removes user "elmo" from the local database. See *Purging the Local Database* on page 12-9 for more information.

Authentication Databases: Kerberos

To	Use This Command	Example(s)	What Example Does
Synchronize the LRS and the Kerberos Clocks	Set / Define IP Timeserver, page 13-90.	`DEFINE IP TIMESERVER 192.0.1.110`	Designates host 192.0.1.110 as the time-server for the LRS. See *Configuration* on page 12-10 for more information.
Specify the Precedence of the Kerberos Server	Set / Define Authentication Kerberos Precedence, page 13-63.	`DEFINE AUTHENTICATION KERBEROS PRECEDENCE 2`	When an incoming caller submits a user-name / password pair, it will be compared to the database with precedence number 1, then to the Kerberos server. See *Configuration* on page 12-10 for more information.
Designate the Primary Kerberos Server	Set / Define Authentication Kerberos Primary, page 13-63.	`DEFINE AUTHENTICATION KERBEROS PRIMARY 192.0.1.52`	Designates host 192.0.1.52 as the primary Kerberos server. See *Configuration* on page 12-10 for more information.

Authentication Databases: Kerberos, cont.

To	Use This Command	Example(s)	What Example Does
Designate a Backup Kerberos Server	Set / Define Authentication Kerberos Secondary, page 13-63.	`DEFINE AUTHENTICATION KERBEROS SECONDARY 192.0.1.53`	Designates host 192.0.1.53 as the backup Kerberos server. This server will be used when the primary server is unavailable. See *Configuration* on page 12-10 for more information.
Specify the Kerberos Realm	Set / Define Authentication Kerberos Realm, page 13-63.	`DEFINE AUTHENTICATION KERBEROS REALM PHRED.COM`	Defines “PHRED.COM” as the Kerberos realm. See *Configuration* on page 12-10 for more information.
Define the Kerberos Principle	Set / Define Authentication Kerberos Principle, page 13-63.	`DEFINE AUTH KERBEROS PRINCIPLE “kerbauth”`	Defines “kerbauth” as the Kerberos principle. See *Configuration* on page 12-10 for more information.
Define the Kerberos Instance	Set / Define Authentication Kerberos Instance, page 13-63.	`DEFINE AUTH KERBEROS INSTANCE “lrs_name”`	Defines “lrs_name” as the Kerberos instance. See *Configuration* on page 12-10 for more information.
Define the Kerberos Authenticator	Set / Define Authentication Kerberos Authenticator, page 13-63.	`DEFINE AUTH KERBEROS AUTHENTICATOR “passwd”`	Defines “passwd” as the Kerberos authenticator. See *Configuration* on page 12-10 for more information.
Define the Kerberos Key Version Number (KVNO)	Set / Define Authentication Kerberos KVNO, page 13-63.	`DEFINE AUTHENTICATION KERBEROS KVNO 1`	Sets the key version number to 1. See *Configuration* on page 12-10 for more information.

Authentication Databases: NetWare Bindery

To	Use This Command	Example(s)	What Example Does
Specify the Precedence of the NetWare Bindery	Set / Define Authentication NetWare Precedence, page 13-66.	`DEFINE AUTHENTICATION NETWARE PRECEDENCE 3`	When an incoming caller submits a username / password pair, it will be compared to the databases with precedence numbers 1 and 2, then to the NetWare bindery. See *NetWare Bindery* on page 12-11 for more information.
Designate the Primary NetWare Bindery	Set / Define Authentication NetWare Primary, page 13-66.	`DEFINE AUTHENTICATION NETWARE PRIMARY doc_server`	Designates host “doc_server” as the primary NetWare bindery. See *NetWare Bindery* on page 12-11 for more information.
Designate a Backup NetWare Bindery	Set / Define Authentication NetWare Secondary, page 13-66.	`DEFINE AUTHENTICATION NETWARE SECONDARY spare_server`	Designates host “spare_server” as the backup NetWare bindery. This server will be used when the primary bindery is unavailable. See *NetWare Bindery* on page 12-11 for more information.

Authentication Databases: RADIUS

To	Use This Command	Example(s)	What Example Does
Specify the Precedence of the RADIUS Server	Set / Define Authentication RADIUS Precedence, page 13-67.	`DEFINE AUTHENTICATION RADIUS PRECEDENCE 4`	When an incoming caller submits a username / password pair, it will be compared to the databases with precedence numbers 1, 2, and 3, then to the RADIUS server. See *RADIUS* on page 12-12 for more information.

Authentication Databases: RADIUS, cont.

To	Use This Command	Example(s)	What Example Does
Designate the Primary RADIUS Authentication Server	Set / Define Authentication RADIUS Primary, page 13-67.	`DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.50`	Designates host 192.0.1.50 as the primary RADIUS server. See *RADIUS* on page 12-12 for more information.
Designate a Backup RADIUS Authentication Server	Set / Define Authentication RADIUS Secondary, page 13-67.	`DEFINE AUTHENTICATION RADIUS SECONDARY 192.0.1.51`	Designates host 192.0.1.51 as the backup RADIUS server. This server will be used when the primary server is unavailable. See *RADIUS* on page 12-12 for more information.
Configure the RADIUS Secret String	Set / Define Authentication RADIUS Secret, page 13-67.	`DEFINE AUTHENTICATION RADIUS SECRET "sd9we923nv9870udf"`	Sets the specified string as the secret string shared by the RADIUS client (LRS) and the RADIUS server. See *RADIUS Authentication* on page 12-12 for more information.
Designate the Primary RADIUS Accounting Server	Set / Define Authentication RADIUS Accounting, page 13-67.	`DEFINE AUTH RADIUS ACCOUNTING PRIMARY "acct_server"`	Designates host "acct_server" as the primary RADIUS accounting server. See *RADIUS Accounting* on page 12-14 for more information.
Designate a Backup RADIUS Accounting Server	Set / Define Authentication RADIUS Accounting, page 13-67.	`DEFINE AUTH RADIUS ACCOUNTING SECONDARY "acct2_server"`	See *RADIUS Accounting* on page 12-14 for more information.

Authentication Databases: SecurID

To	Use This Command	Example(s)	What Example Does
Specify the Precedence of the SecurID Server	Set / Define Authentication SecurID Precedence, page 13-69.	`DEFINE AUTHENTICATION SECURID PRECEDENCE 5`	When an incoming caller submits a username / password pair, it will be compared to the databases with precedence numbers 1, 2, 3, and 4, then to the SecurID server. See *SecurID* on page 12-15 for more information.
Designate the Primary SecurID Server	Set / Define Authentication SecurID Primary, page 13-69.	`DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.50`	Designates host 192.0.1.50 as the primary SecurID server. See *SecurID* on page 12-15 for more information.
Designate a Backup SecurID Server	Set / Define Authentication SecurID Secondary, page 13-69.	`DEFINE AUTHENTICATION SECURID SECONDARY 192.0.1.51`	Designates host 192.0.1.51 as the backup SecurID server. This server will be used when the primary server is unavailable. See *SecurID* on page 12-15 for more information.

Authentication Databases: UNIX Password File

To	Use This Command	Example(s)	What Example Does
Specify the Precedence of the UNIX Password File	Set / Define Authentication TFTP Precedence, page 13-71.	`DEFINE AUTHENTICATION TFTP PRECEDENCE 6`	When an incoming caller submits a username / password pair, it will be compared to the databases with precedence numbers 1, 2, 3, 4, and 5, then to the UNIX password file. See *UNIX Password File* on page 12-16 for more information.

Authentication Databases: UNIX Password File, cont.

To	Use This Command	Example(s)	What Example Does
Specify the Primary TFTP Host	Set / Define Authentication TFTP Primary, page 13-71.	`DEFINE AUTHENTICATION TFTP PRIMARY 192.0.1.50`	Designates host 192.0.1.50 as the primary TFTP host. The password file (specified below) will be checked on this host before other hosts. See *UNIX Password File* on page 12-16 for more information.
Designate a Backup TFTP Host	Set / Define Authentication TFTP Secondary, page 13-71.	`DEFINE AUTHENTICATION TFTP SECONDARY 192.0.1.51`	Designates host 192.0.1.51 as the backup TFTP host. This host will be used when the primary host is unavailable. See *UNIX Password File* on page 12-16 for more information.
Specify the Pathname of the Password File	Set / Define Authentication TFTP Filename, page 13-71.	`DEFINE AUTHENTICATION TFTP FILENAME "/tftpboot/passwd"`	When a login attempt is made, the username / password pair will be compared to the "passwd" file in the "tftpboot" directory on the TFTP host. See *UNIX Password File* on page 12-16 for more information.

Outgoing LAN to LAN Authentication: Character Mode Logins

To	Use This Command	Example(s)	What Example Does
Configure a Chat Script	See Chapter 4, *Additional Remote Networking.*		

Outgoing LAN to LAN Authentication: PPP Logins

To	Use This Command	Example(s)	What Example Does
Use CHAP for Outgoing Authentication	Define Site Authentication CHAP, page 13-32.	`DEFINE SITE dallas AUTHENTICATION CHAP ENABLED`	Enables outgoing CHAP authentication on site “dallas”. See *PPP Logins* on page 12-17 for more information.
Use PAP for Outgoing Authentication	Define Site Authentication PAP, page 13-32.	`DEFINE SITE dallas AUTHENTICATION PAP ENABLED`	Enables outgoing PAP authentication on site “dallas”. See *PPP Logins* on page 12-17 for more information.
Define the Username Sent to the Remote Host	Define Site Authentication User, page 13-32.	`DEFINE SITE dallas AUTHENTICATION USER “seattle”`	When site “dallas” is used, the LRS will send username “seattle” to the remote host during outgoing authentication. See *PPP Logins* on page 12-17 for more information.
Define the Password Sent to the Remote Host	Define Site Authentication Remote, page 13-32.	`DEFINE SITE dallas AUTHENTICATION REMOTE “badger”`	When site “dallas” is used, the LRS will send password “badger” to the remote host during outgoing authentication. See *PPP Logins* on page 12-17 for more information.

Outgoing LAN to LAN Authentication: SLIP Logins

To	Use This Command	Example(s)	What Example Does
Configure Outgoing SLIP Authentication	All outgoing SLIP authentication must be done with chat scripts before SLIP starts. See Chapter 4, *Additional Remote Networking*.		

Restricting Users

To	Use This Command	Example(s)	What Example Does
Become the Privileged User / Stop Being the Privileged User	Set Privileged / Noprivileged, page 13-124.	`SET PRIVILEGED`	Establishes privileged (superuser) status. The privileged password must be entered after the Set Privileged command. See *Privileged Commands* on page 12-18 for more information.
		`SET NOPRIVILEGED`	Restores the session to non-privileged status.
Forcibly Become the Privileged User (Override Another Port's Privileged Status)	Set Privileged / Noprivileged Override, page 13-124.	`SET PRIVILEGED OVERRIDE`	Removes privileged status from the currently privileged user, and establishes privileged status for the current session. See *Privileged Commands* on page 12-18 for more information.
Enable or Disable Users from Starting PPP on a Port	Define Ports PPP, page 13-28.	`DEFINE PORT 2 PPP DISABLED`	Disables the use of the Set PPP command on port 2. See *Controlling Use of the Set PPP/SLIP Commands* on page 12-18 for more information.
Enable or Disable Users from Starting SLIP on a Port	Define Ports SLIP, page 13-31.	`DEFINE PORT 2 SLIP DISABLED`	Disables the use of the Set SLIP command on port 2. See *Controlling Use of the Set PPP/SLIP Commands* on page 12-18 for more information.
Secure a Port	Set / Define Ports Security, page 13-118.	`DEFINE PORT 2 SECURITY ENABLED`	Secures port 2. Users on port 2 will be prevented from editing many of the port's settings. See *Securing a Port* on page 12-19 for more information.

Restricting Users, cont.

To	Use This Command	Example(s)	What Example Does
Lock a Port	Lock, page 13-51.	`LOCK`	Prompts the user for a password. Once the password is entered, the port is locked. The password must be entered to unlock the port. See *Locking a Port* on page 12-19 for more information.
Unlock a Port Without the Lock Password	Unlock Port, page 13-166.	`UNLOCK PORT 2`	Unlocks port 2. See *Locking a Port* on page 12-19 for more information.
	Logout, page 13-51.	`LOGOUT PORT 2`	Logs out port 2. This will unlock the port and disconnect any current sessions. See *Locking a Port* on page 12-19 for more information.
Execute a Series of Commands When a User Logs Into the LRS	Set / Define Authentication User Command, page 13-72.	`DEFINE AUTHENTICATION USER bob COMMAND "SET PPP dialin_users; logout"`	When user "bob" logs into the LRS, PPP will automatically be started and site "dialin_users" will be used for the connection. **NOTE**: This command only applies when the Local database is being used for authentication. See *Forcing Execution of Commands* on page 12-19 for more information.
Place a Port in Menu Mode	Set / Define Menu, page 13-100.	`DEFINE MENU 4 "Telnet irvine" "TELNET 192.0.1.53"`	Defines a menu item "Telnet irvine"; this item is number 4 on the menu. When "Telnet irvine" is selected from the menu, the user will be telnetted to host 192.0.1.53. See *Menu Mode* on page 12-20 for more information.

Restricting Users, cont.

To	Use This Command	Example(s)	What Example Does
Place a Port in Menu Mode, cont.	Set / Define Ports Menu, page 13-114.	`DEFINE PORT 2 MENU ENABLED`	Places port 2 in menu mode. Users on this port will only be able to choose items from the menu; they cannot enter commands. See *Menu Mode* on page 12-20 for more information.
Restrict Incoming Networking Callers to a Particular IP Address	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.125`	Restricts incoming callers to IP address 192.0.1.125. See *IP Address Restriction* on page 12-21 for more information.
Restrict Incoming Remote Networking Callers to a Range of IP Addresses	Define Site IP Remoteaddress, page 13-39.	`DEFINE SITE irvine IP REMOTEADDRESS 192.0.1.110 192.0.1.250`	Restricts incoming callers to IP addresses between 192.0.1.110 and 192.0.1.250. See *IP Address Restriction* on page 12-21 for more information.
Force Incoming Telnet / Rlogin Users to Enter a Password	Set / Define Server Incoming Password, page 13-128.	`DEFINE SERVER INCOMING PASSWORD`	Requires that incoming Telnet and Rlogin users enter the LRS login password. See *Incoming Telnet/Rlogin Connections* on page 12-21 for more information.
Prevent all Incoming Telnet / Rlogin Connections	Set / Define Server Incoming None, page 13-128.	`DEFINE SERVER INCOMING NONE`	Blocks all incoming Telnet and Rlogin connections. See *Incoming Telnet/Rlogin Connections* on page 12-21 for more information.
Enable / Disable Outgoing Rlogin Connections	Set / Define Server Rlogin, page 13-134.	`DEFINE SERVER RLOGIN ENABLED`	Enables outgoing Rlogin connections. See *Outgoing Rlogin Connections* on page 12-22 for more information.

Restricting Users, cont.

To	Use This Command	Example(s)	What Example Does
Restrict Access to a Port	Set / Define Ports Access, page 13-104.	`DEFINE PORT 2 ACCESS LOCAL`	Restricts port 2 to local logins. See *Port Access* on page 12-22 for more information.
		`DEFINE PORT 2 ACCESS REMOTE`	Restricts port 2 to remote logins.
		`DEFINE PORT 2 ACCESS DYNAMIC`	Allows local and remote logins on port 2.
		`DEFINE PORT 2 ACCESS NONE`	Prevents all logins to port 2.
Prevent all IP Traffic	Define Site IP, page 13-39.	`DEFINE SITE irvine IP DISABLED`	Prevents all IP traffic on site “irvine”. See *Preventing all IP, IPX, or AppleTalk Traffic* on page 12-24 for more information.
Prevent all IPX Traffic	Define Site IPX, page 13-41.	`DEFINE SITE irvine IPX DISABLED`	Prevents all IPX traffic on site “irvine”. See *Preventing all IP, IPX, or AppleTalk Traffic* on page 12-24 for more information.
Create a Filter List	Set / Define Filter, page 13-74.	`DEFINE FILTER firewall ADD 1 DENY IP SRC 192.0.1.0 255.255.255.0`	Creates a filter named “firewall”. This filter has one rule, which denies IP traffic from host 192.0.1.0. See *Setting up Filter Lists* on page 12-24 for more information.
Associate a Filter List With a Particular Site	Define Site Filter, page 13-37.	`DEFINE SITE dallas FILTER INCOMING firewall`	Associates filter list “firewall” with site “dallas”. This filter list will be used to filter incoming packet traffic. See *Setting up Filter Lists* on page 12-24 for more information.

Event Logging

To	Use This Command	Example(s)	What Example Does
Specify a Destination for Logging Information	Set / Define Logging Destination, page 13-96.	`DEFINE LOGGING DESTINATION CONSOLE`	Sends logging information to the LRS console port. See *Destination* on page 12-25 for more information.
		`DEFINE LOGGING DESTINATION 192.0.1.5`	Sends logging information to host 192.0.1.5.
Specify the Events to Log	Set / Define Logging, page 13-96.	`DEFINE LOGGING AUTHENTICATION 3`	Logs authentication events at level 3 (all logins). See *Logging Levels* on page 12-26 for more information.
Disable a Specific Type of Event Logging	Set / Define Logging, page 13-96.	`DEFINE LOGGING IPX NONE`	Disables all IPX event logging. See *Logging Levels* on page 12-26 for more information.
Disable all Event Logging	Set / Define Logging Destination, page 13-96.	`DEFINE LOGGING DESTINATION NONE`	Disables all event logging. See *Logging Levels* on page 12-26 for more information.

13 Command Reference

13 - Command Reference

This chapter describes all commands that can be used with the LRS. The following items are included in the description of each command:

- The command's full syntax, shown in diagram form
- Any restrictions on the command, such as whether you must be the privileged user to use it

NOTE: *For information on becoming the privileged user, see Set Privileged/Noprivileged on page 13-124.*

- Potential errors that may be encountered when using the command
- Descriptions of each associated parameter

NOTE: *Multiple optional parameters can be entered on the same command line, subject to the maximum command line length of 132 characters.*

- Default settings, where applicable
- Examples of the command
- Cross-references to related commands

13.1 Command Line Interface

13.1.1 Command Types

There are subtle differences between each group of commands, as explained below.

13.1.1.1 Set and Define

Set Changes the unit immediately but not permanently. To make the change permanent, enter the Save command.

Define Changes the **permanent** characteristics of ports, servers, and services.

Define Port and Define SLIP settings take effect after the current user logs out. Define Site takes effect when a site is started. Define Server, Define Telnet Host, and Define Service settings take effect when the LRS is rebooted.

NOTE: *Most Define commands are documented together with their corresponding Set commands.*

13.1.1.2 Show, Monitor, and List

Show Displays the current settings, those made using the Set command but not yet defined or saved as permanent changes.

Monitor Displays current operating characteristics, which are updated every three seconds until a key is pressed. Monitor commands may only be used by the privileged user.

List Displays settings that will take effect the next time the LRS is rebooted.

NOTE: *Monitor and List commands are documented together with their corresponding Show commands.*

13.1.1.3 Clear and Purge

Clear Removes an item immediately, but does not make a permanent change.

Purge Removes an item permanently, but doesn't take effect until the unit is rebooted.

NOTE: *Most Purge commands are listed with their corresponding Clear commands, but some are listed separately under the Purge keyword.*

13.1.2 About Strings

When a command calls for a string, the following two things must be taken into consideration.

First, any user-entered strings should be enclosed in quotes to retain the case entered. If a string is not enclosed in quotes, it will be changed to all uppercase characters, and any spaces will cause the LRS to interpret the different parts of the string as different command parameters.

In addition, string lengths are generally limited to thirty-one alphanumeric characters for pathnames and file server names, fifteen alphanumeric characters for filenames, and six alphabetic characters for the privileged and login passwords. When a string differs from the norm, its limitations are noted.

13.1.3 Conventions Used in This Chapter

The following conventions are used to explain the syntax of the commands:

- Optional parameters are enclosed in brackets **[ ]**; one or more of these parameters may be used, or the command can be used without adding any of these parameters.
- Required parameters are enclosed in curly braces **{ }**; one and only one of these parameters must be used.
- User-supplied parameters, such as a particular port number or host name, are shown in *italics.*

13.2 Apropos

APROPOS *keyword*

Displays commands containing the specified keyword. If a command containing the keyword cannot be found, the LRS will display "nothing appropriate."

The LRS will not display all relevant commands. If there are analogous commands, such as Set Ports and Define Ports, only one will be shown (in this case, Set Ports).

Restrictions Privileged commands containing the specified keyword will only be displayed if you are currently the privileged user.

Parameters

keyword
An alphanumeric string. You do not have to type the complete command keyword in order to get a response; partial strings will yield appropriate commands that contain that string.

Examples

```
APROPOS SITE
```

See Also

Help, page 13-49.

13.3 Backwards

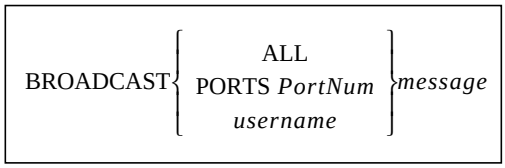
BACKWARDS

Switches sessions from the current session to the most recently started previous session. If there is only one active session, it resumes. Repeating the command will cycle you “backward” through the active sessions. If you reach the beginning of the session list, entering this command returns you to the most recent session.

See Also

Forwards, page 13-49; Show / Monitor Sessions, page 13-161; *Sessions*, page 9-4.

13.4 Broadcast



Sends a message to another port, all ports, or a specific user on the server. Broadcast may only be used if broadcasts have been enabled on the server using the Set / Define Server Broadcast command.

Restrictions

You must be the privileged user to use the All parameter.

Secure users may not send broadcasts.

Errors

And error will be returned if the port broadcasted to is flow controlled or the server does not have broadcast enabled. The sender is notified if a message was not received.

Parameters

All
Sends the message to all ports.

Ports
Specifies a particular port as recipient of the message. Must be used with the *PortNum* parameter.

PortNum
A particular LRS port.

username
A particular user as recipient of the message.

message
One word, or several words in quotes. The message will be sent exactly as typed if enclosed in quotes, or in uppercase if not. The message length is limited only by the length of the command line.

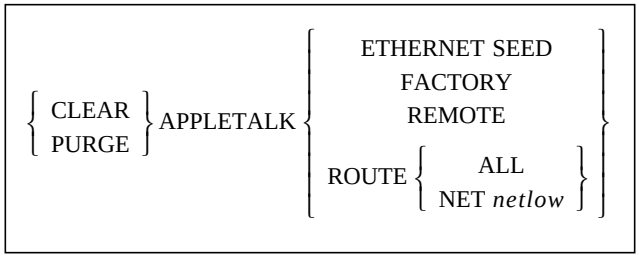
Examples

```
Local> BROADCAST PORT 7 “ready for lunch?”

Local> BROADCAST fred “Meeting in 10 minutes.”
```

See Also Set / Define Server Broadcast, page 13-125; *Configuring a Timeserver*, page 2-7.

13.5 Clear/Purge

13.5.1 Clear/Purge AppleTalk



Removes information configured on the LRS for the AppleTalk protocol.

Restrictions You must be the privileged user to use this command.

Errors Clear AppleTalk Factory will not work. Purge AppleTalk Factory must be used instead.

Parameters

Ethernet Seed
Removes all configured seed information for the Ethernet interface, including the network number range and all zones on that network.

Factory
Returns AppleTalk information to its factory default settings.

Remote
Removes the network number and zone used for dialin users.

Route
Removes information related to AppleTalk routes to LRS sites.

All
Removes all AppleTalk routes to LRS sites.

Net
Removes routes to sites on the specified network.

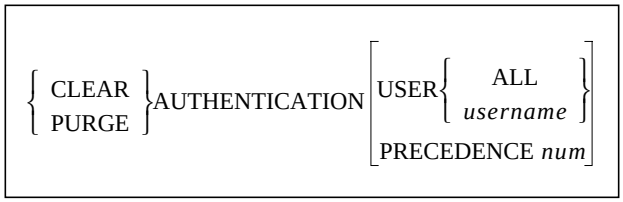
netlow
A network number of up to 16 bits. It is only necessary to specify the low number of a network range to identify the range for removal.

Examples

```
Local>> CLEAR APPLETALK ROUTE NET 16
```

See Also Set / Define AppleTalk commands, beginning on page 13-59; Show / Monitor / List AppleTalk, page 13-147; *AppleTalk Networking*, page 7-5.

13.5.2 Clear/Purge Authentication



Removes information stored in the local authentication database.

Restrictions You must be the privileged user to use this command.

Parameters

User
Clears or purges a user from the local authentication database.

All
Clears or purges all users.

username
A specific username to clear or purge.

Precedence
Clears or purges a given precedence slot. Must be used in conjunction with the *num* parameter.

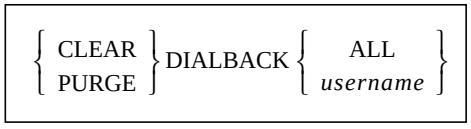
num
A precedence number of 1 through 6.

Examples

```
Local> CLEAR AUTHENTICATION USER “bob”

Local> PURGE AUTHENTICATION PRECEDENCE 2
```

See Also Set / Define Authentication, page 13-62; Set / Define Authentication Unique, page 13-72; Show / Monitor / List Authentication, page 13-148; Chapter 12, *Security*.

13.5.3 Clear/Purge Dialback



Removes a dialback setting for a particular username, or for all usernames.

Restrictions You must be the privileged user to use this command.

Errors Clear Dialback will return an error if the specified username isn’t found, or if *All* is specified and no entries are configured.

Parameters

All
Clears dialback settings for all usernames.

username
Clears dialback settings for the specified username.

Examples

```
Local>> CLEAR DIALBACK ALL

Local>> PURGE DIALBACK robert
```

See Also Define Ports Dialback, page 13-15; Set / Define Dialback, page 13-73; Show / Monitor / List Dialback, page 13-148; *Dialback*, page 12-34.

13.5.4 Clear/Purge Filter

{ CLEAR / PURGE } FILTER *filtername*

Removes a specified packet filter.

Restrictions You must be the privileged user to use this command.

Parameters

filtername
A particular packet filter to be removed.

Examples

```
Local>> PURGE FILTER abc
```

See Also Set / Define Filter, page 13-74; Show / Monitor / List Filter, page 13-148; *Filter Lists*, page 4-1.

13.5.5 Clear/Purge Hosts

{ CLEAR / PURGE } [TELNET] HOSTS { ALL / *HostName* }

Removes a TCP / IP host entry from the LRS table of known hosts. If Clear is used and the host was seen through the **rwho** facility, it will reappear as soon as that machine broadcasts again. A host will also reappear if a user Connects to it.

Restrictions You must be the privileged user to use this command.

Errors Clear Telnet Hosts will fail if there are any active Telnet connections on the server.

Parameters

All
Removes the names of all known hosts.

HostName
The name of a Telnet host to be removed.

Examples

```
Local>> CLEAR HOSTS alex
```

See Also Set / Define Telnet Hosts, page 13-146; Show / Monitor / List Hosts, page 13-149.

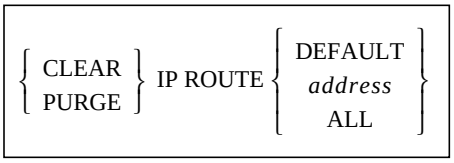
13.5.6 Clear IP Ethernet

Clear IP Ethernet is not a valid command. Use Purge IP Ethernet, described on page 13-53.

13.5.7 Clear IP Factory

Clear IP Factory is not a valid command. Use Purge IP Factory, described on page 13-53.

13.5.8 Clear/Purge IP Route



Removes a static IP route.

Restrictions You must be the privileged user to use this command.

Parameters

Default
Clears or purges default IP routes.

address
An IP address in standard numeric format (for example, 193.53.2.2).

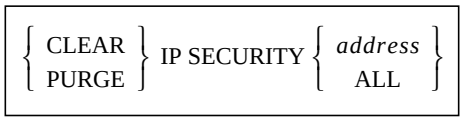
All
Clears or purges all static IP routes.

Examples

```
Local>> PURGE IP ROUTE 192.0.1.1

Local>> PURGE IP ROUTE DEFAULT
```

See Also Set / Define IP Route, page 13-87; Show / List Protocols IP Routes, page 13-157; *IP Routing*, page 5-11.

13.5.9 Clear/Purge IP Security



Removes the specified IP security table entry.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.53.2.2).

All
Clears or purges the entire security table.

Examples

```
Local>> CLEAR IP SECURITY 192.0.1.1
```

See Also Set / Define IP Security, page 13-88; Show / Monitor / List IP, page 13-149; *IP Address Restriction*, page 12-21.

13.5.10 Clear/Purge IP Trusted

Removes all entries from the trusted router table.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.53.2.2).

All
Clears or purges all entries in the router table.

Examples

```
Local>> PURGE IP TRUSTED 192.0.1.1

Local>> PURGE IP TRUSTED ALL
```

See Also Set / Define IP Trusted, page 13-90; Show / Monitor / List IP Trusted, page 13-149; *Routing Tables*, page 5-12.

13.5.11 Clear IPX Factory

Clear IPX Factory is not a valid command. Use Purge IPX Factory, described on page 13-54.

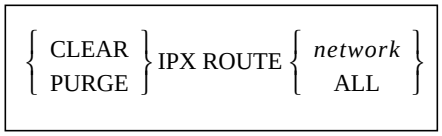
13.5.12 Clear/Purge IPX Keepalive

Removes the keepalive (spoof) entries.

Restrictions You must be the privileged user to use this command.

See Also Define Site IPX Keepalive, page 13-41; Show / Monitor / List IPX Keepalive, page 13-151; *Spoofing*, page 4-5.

13.5.13 Clear/Purge IPX Route



Removes the default static IPX route.

Restrictions You must be the privileged user to use this command.

Parameters

network
An IPX network number in hexadecimal format.

All
Clears or purges all static routes.

Examples

```
Local>> CLEAR IPX ROUTE 63EB
```

See Also Set / Define IPX Route, page 13-93; Show / Monitor / List IPX, page 13-151; *Static Routing*, page 6-7.

13.5.14 Clear/Purge IPX Service

Removes a static IPX service.

Restrictions You must be the privileged user to use this command.

Parameters

ServiceName
A string of up to 48 bytes in length.

ServiceType
A service type of 1 through 4 hexadecimal digits. A service type of 0xffff clears or purges all services for that service name.

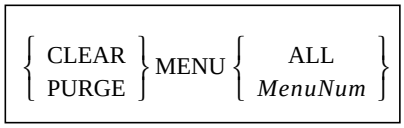
All
Clears or purges all static services.

Examples

```
Local>> PURGE IPX SERVICE NTX 4

Local>> CLEAR IPX SERVICE NTX ffff
```

See Also Set / Define IPX Service, page 13-94; Show / Monitor / List IPX, page 13-151; *Services and Sockets*, page 6-11.

13.5.15 Clear/Purge Menu



Removes a specified menu entry or all menu entries.

Restrictions You must be the privileged user to use this command.

Parameters

All
Clears all menu entries.

MenuNum
An integer from 1 through 36 specifying a particular menu entry to be removed.

Examples

```
Local>> CLEAR MENU ALL

Local>> CLEAR MENU 2
```

See Also Set / Define Menu, page 13-100; Set / Define Ports Menu, page 13-114; Show / Monitor / List Menu, page 13-152; *Menu Mode*, page 9-18.

13.5.16 Clear/Purge Protocols NetWare Access

Removes a specified entry or all entries from the NetWare access list.

Restrictions You must be the privileged user to use this command.

Errors This command will return an error if the specified entry isn't found, or if All is specified and no access list entries have been configured.

Parameters

All
Removes all entries.

fileserver
A fileserver name of up to 31 characters.

Examples

```
Local>> PURGE PROTOCOL NETWARE ACCESS ALL

Local>> CLEAR PROTOCOL NETWARE ACCESS lab_fs4
```

See Also Set / Define NetWare Access, page 13-100; Show / List Protocols NetWare Access, page 13-157.

13.5.17 Clear/Purge Service

Removes an LRS service. Clearing a service only disables it until re-initialization of the LRS. For a permanent removal, the Purge command must be used.

Restrictions You must be the privileged user to use this command.

Errors Clear Service fails when there are sessions connected to the service or when there are connect requests in the service's queue. These conditions can be corrected with the Logout Port and Remove Queue commands.

Parameters

Local
Specifies that all local services should be removed.

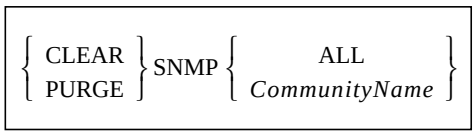
ServiceName
A specific service to be removed.

Examples

```
Local>> PURGE SERVICE LOCAL

Local>> CLEAR SERVICE FILESERVER
```

See Also Set / Define Service commands, beginning on page 13-138; Set / Define IPX Service, page 13-94; Show / Monitor / List Services, page 13-160; Show / Monitor / List IPX Services, page 13-151; *Sessions*, page 9-4.

13.5.18 Clear/Purge SNMP



Removes entries from the SNMP security table.

Restrictions You must be the privileged user to use this command.

Parameters

All
Specifies all SNMP table entries should be removed.

CommunityName
A specific SNMP community to be removed.

Examples

```
Local>> CLEAR SNMP "mycomm"
```

See Also Set / Define SNMP, page 13-146; Set / Define Filter IP *keyword*, page 13-74; Show / Monitor / List SNMP, page 13-162; Appendix C, *SNMP Support*.

13.5.19 Clear/Purge Telnet Hosts

See Clear / Purge Hosts on page 13-6.

13.6 Cls

```
CLS
```

Clears the screen on your terminal device if the port is configured as Type ANSI.

13.7 Connect

```
CONNECT { {TELNET | TCP} host [:port][:envstring]
          RLOGIN host [:port][:envstring] [username]
          LOCAL target[:envstring] }
```

Establishes a session with a TCP / IP host. If no hostname is specified, a connection to any *preferred* host is attempted.

NOTE: *The keyword "Connect" is not needed for Telnet or Rlogin connections, but must be included in the command for TCP or Local connections.*

A colon and session environment string can be added to the connect request (see *Setting Session Characteristics* on page 9-6). A colon and a port number can be added to the hostname for TCP / Telnet / Rlogin sessions; in this case the specified port number will be used for the connection. There should be no spaces between the hostname, colon, and port number or environment string.

Parameters

Telnet
The port is dedicated to the specified Telnet host. Must be used in conjunction with the *host* parameter.

TCP
Establishes a raw TCP connection to the host / port number specified.This is useful for non-standard applications that do not desire any interpretation of the data stream (for example, UUCP).

Rlogin
Forces an Rlogin connection to the remote host. Must be used in conjunction with the *host* parameter. May also take a *username* after the host parameter, in which case a username is sent to the remote Rlogin host.

host
A text host name or an IP address in standard numeric format (for example, 192.0.1.183).

envstring
Sets up the connection environment before the session is started. The string is constructed with a sequence of key letters, some of which are prefaced by either "+" or "-." The key letters are:

D	+D = Backspace mode	-D = Delete mode
E	+E = Local Echo mode	-E = Remote Echo mode
I	I = Interactive mode	
P	+P = Passall mode	-P = Passthru mode
C	+C = CR = CRLF,	-C = CR = LF
T	TCP mode (i.e. uninterpreted data stream)	
R	Rlogin protocol (sets port number to 513 if not already set)	
Q	Queued (i.e. RTEL) connection	

Local
Establishes a connection to a local service or port specified with the *target* parameter.

target
A local service or port name.

Examples

```
Local> CONNECT

Local> CONNECT TELNET 145.34.35.11:245

Local> CONNECT TCP labsun

Local> CONNECT RLOGIN 145.34.35.14

Local> CONNECT RLOGIN docserver mary
```

See Also Set / Define Ports Preferred, page 13-117; Define Ports Dedicated, page 13-14; Disconnect, page 13-48; *Preferred/Dedicated Telnet Hosts*, page 9-9.

13.8 Define NetWare Internal

DEFINE [PROTOCOL] NETWARE INTERNAL [NETWORK] *NetNumber*

Specifies the internal network number to use when internal routing is enabled.

Restrictions You must be the privileged user to use this command.

Parameters

NetNumber
An internal network number of up to 8 hexadecimal digits that defaults to the last four segments of the LRS hardware address.

Examples

```
Local>> DEFINE NETWARE INTERNAL NETWORK ABCD1234
```

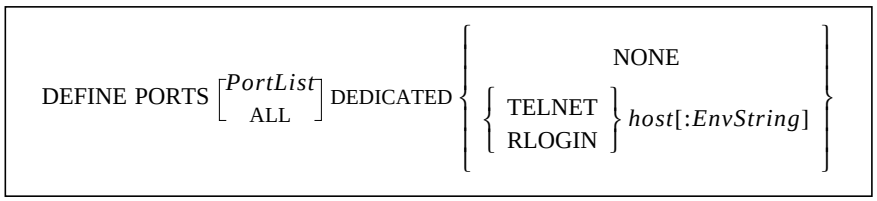
See Also Set / Define NetWare Routing, page 13-103; Set / Define NetWare Encapsulation, page 13-101; *Routing*, page 6-2.

13.9 Define Ports

Configures Define-only port characteristics including dedicated connections, dialback security, modem, PPP, and SLIP options. These options cannot be configured using Set commands.

Define Port commands are only a small part of the port configuration options. Refer to the **Set/ Define Ports** commands beginning on page 13-104 for additional options.

13.9.1 Define Ports Dedicated



Sets up a dedicated Telnet host or service that this port will connect to whenever it is logged in. If dedicated to a service, the user will be logged off the server when the remote service is logged out.

If the port is dedicated to a Telnet host, an environment string can be part of the dedicated hostname. There should be no spaces between the hostname, colon, and environment string.

WARNING: Dedicating all LRS ports is dangerous, as it leaves no easy way to log into the server. (In other words, users can no longer quickly access the Local> prompt). If all ports are dedicated, users must connect via the NetWare or Telnet console ports, or the LRS must have incoming logins enabled.

Restrictions

You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

None
Clears any existing Dedicated service.

Telnet
The port is dedicated to this Telnet host. Must be used in conjunction with the *host* parameter.

Rlogin
The port is dedicated to this Rlogin host. Must be used in conjunction with the *host* parameter.

host
A text host name or an IP address in standard numeric format (for example, 192.0.1.183).

EnvString
Sets up the connection environment before the session is started. The string is constructed with a sequence of key letters, some of which are prefaced by either "+" or "-." The key letters are:

D	+D = Backspace mode	-D = Delete mode
E	+E = Local Echo mode	-E = Remote Echo mode
I	I = Interactive mode	
P	+P = Passall mode	-P = Passthru mode
C	+C = CR = CRLF,	-C = CR = LF
T	TCP mode (i.e. uninterpreted data stream)	
R	Rlogin protocol (sets port number to 513 if not already set)	
Q	Queued (i.e. RTEL) connection	

Examples

```
Local>> DEFINE PORT 5 DEDICATED TELNET 192.0.1.221

Local>> DEFINE PORT 2 DEDICATED TELNET irvine:+D
```

See Also
Connect, page 13-12; Set / Define Ports Preferred, page 13-117; Define Ports PPP Dedicated, page 13-28; Set Ports SLIP Dedicated, page 13-120; Show / Monitor / List Ports, page 13-155; *Setting Session Characteristics*, page 9-6.

13.9.2 Define Ports Dialback

Turning on Dialback causes the LRS to check the dialback table (see **Set/Define Dialback**) each time a user logs in. If the entered username is not in the table, the port is logged out. If the username is in the table, the port is logged out and the LRS sends the dialback string to the port and awaits a second login. Typically the dialback string will cause the a modem attached to the port to call the user back at a certain telephone number for security reasons. Ports with dialback enabled have a 30-second time limit for entering the username when logging in.

In order to use Dialback functionality, modem control must be enabled, and a modem profile must be associated with the port. When Dialback is enabled, Modem Control is enabled by default. However, disabling Dialback does not disable Modem Control; Modem Control must explicitly be disabled if so desired.

Restrictions
You must be the privileged user to use this command.

Parameters

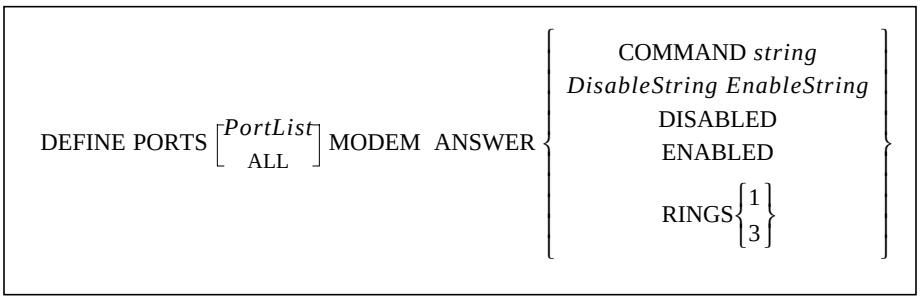
PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Examples

```
Local>> DEFINE PORT 5 DIALBACK ENABLED
```

See Also Set / Define Dialback, page 13-73; Clear / Purge Dialback, page 13-5; Show / Monitor / List Dialback, page 13-148; Define Ports Modem Control, page 13-20; Define Ports Modem Type, page 13-27; Show / Monitor / List Ports, page 13-155; *Dialback*, page 10-11; *Dialback*, page 12-34.

13.9.3 Define Ports Modem Answer



Permits or prevents a modem from automatically answering the line, optionally after a specified number of rings.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Command
Changes the answer command that is actually sent to the modem to make it answer the line. Commonly set to “A” or “ATA”.

DisableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be disabled. Commonly set to “s0=0”.

EnableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be enabled. Commonly set to “s0=1”.

Rings
Enter either 1 or 3 to tell the LRS how many rings to wait before answering the line. When Define Ports Modem CallerID is enabled, the ring value should be set to 3 to give the LRS time to gather Caller-ID information.

NOTE: *USR Sportster and USR Courier users must set switch 5 to match the LRS Modem Answer settings.*

Default Disabled (no strings defined), 1 Ring.

Examples

```
Local>> DEFINE PORT 2 MODEM ANSWER ENABLED

Local>> DEFINE PORT 2 MODEM ANSWER “s0=0” “s0=1”
```

See Also Define Ports Modem CallerID, page 13-18; *Profile Settings*, page 10-4; *Caller-ID*, page 10-12.

13.9.4 Define Ports Modem Attention

DEFINE PORTS [*PortList* / ALL] MODEM ATTENTION *string*

Defines a string to get the modem's attention.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to "at".

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM ATTENTION "at"
```

See Also *Profile Settings*, page 10-4.

13.9.5 Define Ports Modem Busy

DEFINE PORTS [*PortList* / ALL] MODEM BUSY*string*

Defines a string that the LRS will expect from the modem on outbound calls to signal that the remote number is busy or otherwise unavailable.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to "BUSY".

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM BUSY "BUSY"
```

See Also *Profile Settings*, page 10-4.

13.9.6 Define Ports Modem CallerID

Configures whether the LRS will look for and attempt to decode Caller-ID information for incoming calls. The LRS should be set to wait for three rings before answering the line so that it has enough time to gather the Caller-ID information. The ring setting can be configured with the Define Ports Modem Answer Rings command.

Restrictions You must be the privileged user to use this command.

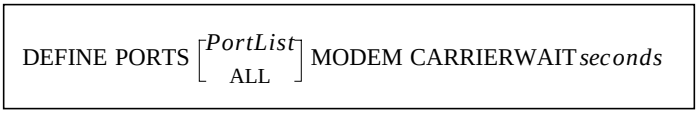
Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Default Disabled.

See Also Define Ports Modem Answer, page 13-16; *Caller-ID*, page 10-12.

13.9.7 Define Ports Modem Carrierwait



Defines the length of time that a server will wait for a carrier on incoming and autodialed outgoing calls. If a carrier is not received in that length of time, the LRS assumes that it will not be received. The call will fail and the modem will be reset.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

seconds
A time value between 1 and 250 seconds.

Default 60 seconds.

Examples

```
Local>> DEFINE PORT 2 MODEM CARRIERWAIT 40
```

See Also *Carrierwait string*, page 10-5.

13.9.8 Define Ports Modem Commandprefix

Defines a string to send before the “Init” and other configuration strings.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “at”.

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM COMMANDPREFIX “at”
```

See Also *Profile Settings*, page 10-4.

13.9.9 Define Ports Modem Compression

Enables or disables data compression in the modem.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

DisableString
A string of up to 12 characters. When this string is received by the modem, data compression will be disabled.

EnableString
A string of up to 12 characters. When this string is received by the modem, data compression will be enabled.

NOTE: *Both the DisableString and the EnableString must be entered.*

Default Disabled (no strings defined).

Examples

```
Local>> DEFINE PORT 2 MODEM COMPRESSION ENABLED

Local>> DEFINE PORT 2 MODEM COMPRESSION “%c” “%c1”
```

See Also *Profile Settings*, page 10-4; *Compression*, page 10-8.

13.9.10 Define Ports Modem Connected

DEFINE PORTS [*PortList* / ALL] MODEM CONNECTED *ConnectString*

Defines a string to expect on outbound calls when the modem is connected to the remote location.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

ConnectString
A string of up to 12 characters. Commonly set to “CONNECT”.

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM CONNECT “CONNECT”
```

See Also *Profile Settings*, page 10-4.

13.9.11 Define Ports Modem Control

DEFINE PORTS [*PortList* / ALL] MODEM[CONTROL] {ENABLED / DISABLED}

Enables or disables modem handling on the specified port(s). For the description and syntax of particular parameters used in conjunction with this command (for example, Define Ports Modem Ring), refer to the individual entries that follow.

When modem handling is enabled, the assertion and deassertion of modem signals (DSR, DTR, and DCD) control the port’s interaction with the modem, including initializing the modem upon booting and resetting the modem between uses. The LRS monitors DCD to determine if a connection exists. If DCD drops, the LRS will log the port out and drop DTR.

Modem Control must be **disabled** to use Dsrlogout. Modem Control implies Dsrlogout, in that the LRS will attempt to log out any connections if the port’s DSR signal drops.

NOTE: *Modem Control should not be disabled on ports that have modems attached.*

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Default Disabled.

See Also Set / Define Ports Dsrlogout, page 13-110; Show / Monitor / List Ports Modem, page 13-155; Chapter 10, *Modems*.

13.9.12 Define Ports Modem Dial

DEFINE PORTS [*PortList* / ALL] MODEM DIAL *DialString*

Defines a string to send to the modem to cause it to dial. This string is preceded by the **Command-prefix** string.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

DialString
A string of up to 12 characters. Often touch tone dialing is activated with "dt" and pulse dialing is activated with "dp".

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM DIAL "dt"
```

See Also Define Ports Modem Commandprefix, page 13-19; *Profile Settings*, page 10-4.

13.9.13 Define Ports Modem Error

DEFINE PORTS [*PortList* / ALL] MODEM ERROR *string*

Defines a string to expect on outbound calls when the modem encounters an error.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters set to "ERROR" by default.

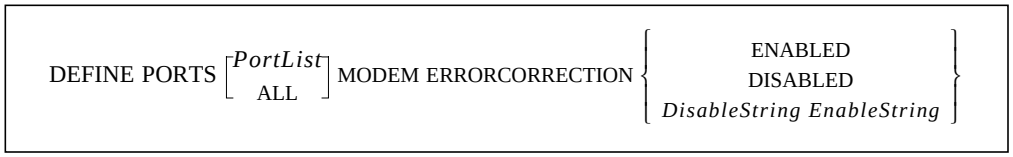
Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM ERROR "ERROR"
```

See Also *Profile Settings*, page 10-4; Define Ports Modem Errorcorrection, next.

13.9.14 Define Ports Modem Errorcorrection



Enables or disables error correction in the modem.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

DisableString
A string of up to 12 characters. When the modem receives this string, automatic answering will be disabled.

EnableString
A string of up to 12 characters. When this string is received by the modem, error correction will be enabled.

NOTE: *Both the DisableString and the EnableString must be entered.*

Default Disabled (no strings defined).

Examples

```
Local>> DEFINE PORT 2 MODEM ERRORCORRECTION ENABLED

Local>> DEFINE PORT 2 MODEM ERRORCORRECTION “&q5” “q0”
```

See Also *Profile Settings*, page 10-4; Define Ports Modem Error, previous.

13.9.15 Define Ports Modem Getsetup

Defines a string to send to the modem to cause it to return its setup. This string is preceded by the **Commandprefix** string. If the string is set to ““, the LRS will not attempt to get the modem’s setup. The LRS will always send the **Save** string after configuration. Modems that do not return their configuration in a single screen should do this.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “&v”.

Default Depends on modem and modem profile.

Examples `Local>> DEFINE PORT 2 MODEM GETSETUP “&v”`

See Also Define Ports Modem Commandprefix, page 13-19; *Profile Settings*, page 10-4.

13.9.16 Define Ports Modem Init

DEFINE PORTS [*PortList* / ALL] MODEM INIT *string*

Defines an initialization string to send to the modem. This string is preceded by the **Command-prefix** string.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 64 characters.

Default Depends on modem and modem profile.

Examples `Local>> DEFINE PORT 2 MODEM INIT “&fw1&c1&d3s2=128”`

See Also Define Ports Modem Commandprefix, page 13-19; *Profile Settings*, page 10-4.

13.9.17 Define Ports Modem Nocarrier

DEFINE PORTS [*PortList* / ALL] MODEM NOCARRIER *string*

Defines a string to expect on outbound calls when the modem can dial, but doesn’t connect.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “NO CARRIER”.

Default Depends on modem and modem profile.

Examples `Local>> DEFINE PORT 2 MODEM NOCARRIER “NO CARRIER”`

See Also *Profile Settings*, page 10-4.

13.9.18 Define Ports Modem Nodialtone

DEFINE PORTS [*PortList* / ALL] MODEM NODIALTONE *string*

Defines a string to expect on outbound calls when the modem can't detect a dial tone.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to "NO DIAL".

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM NODIAL "NO DIAL"
```

See Also *Profile Settings*, page 10-4.

13.9.19 Define Ports Modem OK

DEFINE PORTS [*PortList* / ALL] MODEM OK *string*

Defines a string to expect after the **Attention** string is sent to the modem.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to "OK".

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM OK "OK"
```

See Also Define Ports Modem Attention, page 13-17; *Profile Settings*, page 10-4.

13.9.20 Define Ports Modem Reset

DEFINE PORTS [*PortList* / ALL] MODEM RESET *string*

Defines a string that will cause the modem to reset and reload its configuration from NVR.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “Z”.

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM RESET “Z”
```

See Also *Profile Settings*, page 10-4.

13.9.21 Define Ports Modem Ring

DEFINE PORTS [*PortList* / ALL] MODEM RING *string*

Defines a string that the modem returns if it ringing.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “RING”.

Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM RING “M&M”
```

See Also *Profile Settings*, page 10-4.

13.9.22 Define Ports Modem Save

Defines a string that forces the modem to save its configuration to NVR.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters. Commonly set to “&w”.

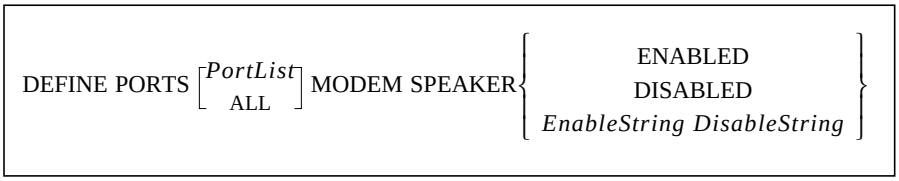
Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM SAVE “&w”
```

See Also *Profile Settings*, page 10-4.

13.9.23 Define Ports Modem Speaker



Enables or disables the modem’s speaker. The speaker allows the user to hear the modem’s dialup and connect sequences for debugging purposes.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

EnableString
A string of up to 12 characters. Commonly set to “m1/1”. When this string is received by the modem, the modem’s speaker will be enabled.

DisableString
A string of up to 12 characters. Commonly set to “m0”. When this string is received by the modem, the modem’s speaker will be disabled.

Default Disabled (no strings defined).

Examples

```
Local>> DEFINE PORT 2 MODEM SPEAKER ENABLED

Local>> DEFINE PORT 2 MODEM SPEAKER “m11” “m0”
```

See Also *Profile Settings*, page 10-4.

13.9.24 Define Ports Modem Statistics

Defines a string to send to the modem to collect connection statistics after each call. This string is preceded by the **Commandprefix** string.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

string
A string of up to 12 characters.

Default Depends on modem and modem profile.

Examples

```
Local> DEFINE PORT 2 MODEM STATISICS “statreport”
```

See Also Define Ports Modem Commandprefix, page 13-19; Set / Define Logging Modem, page 13-96.

13.9.25 Define Ports Modem Type

Specifies a predefined modem profile. Use the Show Modem command (page 13-153) to see a list of available profiles.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

TypeNum
A predefined modem profile number.

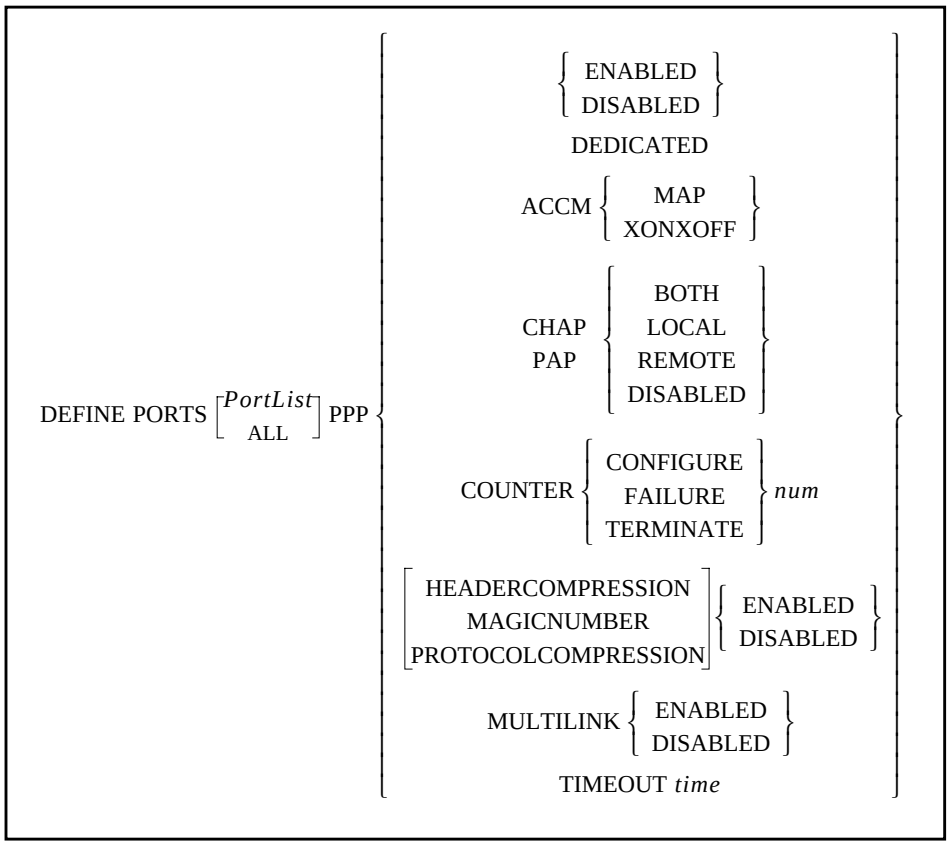
Default Depends on modem and modem profile.

Examples

```
Local>> DEFINE PORT 2 MODEM TYPE 12
```

See Also Show / Monitor / List Modem, page 13-153; *Modem Profiles*, page 10-2.

13.9.26 Define Ports PPP



This command does not start PPP; it merely enables PPP to be run on the port and configures PPP-related settings.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Enabled/Disabled
Enables or disables PPP on a specified port, but does not start PPP.

Dedicated
Configures a port to always be in PPP mode. The port will automatically run PPP when it is started. No other protocol can be run on the port; it will continue to run PPP until it is logged out.

ACCM
Enters an asynchronous control map in hexadecimal. Bits turned on represent ASCII characters that will be escaped in the PPP data stream. See *Character Escaping* on page 8-1 for more information.

map
A hexadecimal value between 0x00000000 and 0xffffffff.

XONXOFF
A default map that escapes the XON and XOFF software flow control characters.

CHAP
Configures the Challenge Handshake Authentication Protocol (CHAP). See *CHAP* on page 8-2 for more information.

PAP
Configures the Password Authentication Protocol (PAP). See *PAP* on page 8-2 for more information.

Both
Enables authentication for this node and the remote node.

Disabled
Turns off CHAP / PAP authentication.

Local
The LRS will authenticate itself to the remote node.

Remote
The remote node will authenticate itself to the LRS.

Counter
Specifies the number of configuration retries for the Link Protocol and all Network Control protocols.

Configure
Specifies the number of Configure-Requests to send before giving up negotiation. The number must be specified using the num parameter, discussed below.

Failure
Specifies the number of Configure-Naks to send before giving up negotiation.

Terminate
Specifies the number of Terminate-Requests to send before disconnecting.

num
An integer between 1 and 255.

HeaderCompression
Enables or disables compression of PPP headers. See *Header Compression* on page 8-1 for more information.

MagicNumber
Controls PPP magic numbers.

ProtocolCompression
Configures the compression of protocol information in PPP.

Timeout
Sets the timeout value, in tenths of seconds, for the Link Control Protocol and all Network Control protocols.

time
An integer between 1 and 255, representing a length of time in tenths of seconds. For example, a setting of 25 equals 2.5 seconds.

Multilink
Allows the LRS to add the specified port to a PPP connection to increase bandwidth on demand.

Defaults

PPP: Disabled.

Map value: 0x00000000.

CHAP and PAP: Disabled.

Counter Configure: 10 requests.
Counter Failure: 5 Configure-NAKs.
Counter Terminate: 2 requests.

HeaderCompression, MagicNumber, ProtocolCompression: Enabled.

Timeout: 30 seconds.

Multilink: Disabled.

Examples

```
Local>> DEFINE PORT PPP ACCM 0x000a0000

Local>> DEFINE PORT PPP CHAP LOCAL

Local>> DEFINE PORT PPP PAP REMOTE

Local>> DEFINE PORT PPP COUNTER FAILURE 5

Local>> DEFINE PORTS 2-4 PPP HEADERCOMPRESSION ENABLED

Local>> DEFINE PORT 2 PPP MAGICNUMBER ENABLED

Local>> DEFNE PORT 3 PPP TIMEOUT 25

Local>> DEFNE PORT 3 PPP MULTILINK ENABLED
```

See Also

Define Ports PPPdetect, page 13-30; Purge Port PPP, page 13-54; Set / Define Logging PPP, page 13-96; Set PPP, page 13-124; Show / Monitor / List Ports PPP, page 13-155; *PPP*, page 1-2; Chapter 8, *PPP*.

13.9.27 Define Ports PPPdetect

DEFINE PORTS [*PortList* | ALL] PPPDETECT { ENABLED | DISABLED }

Automatically detects incoming PPP characters and starts running PPP.

Restrictions

You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

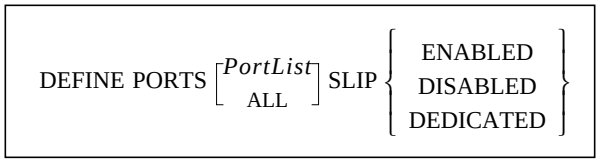
Default

Disabled.

See Also

Define Ports PPP, page 13-28; Show / Monitor / List Ports PPP, page 13-155; *Automatic Detection of PPP*, page 8-4.

13.9.28 Define Ports SLIP



Define Port SLIP Enabled / Disabled determine whether or not SLIP can be run on the specified port. When Define Port SLIP Dedicated is used, the port will always be in SLIP mode.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specify the desired port(s). Port numbers can be separated with commas (for lists) or dashes (for ranges).

Dedicated
The specified port will automatically run SLIP when it is started. No other protocol can be run on the port; it will continue to run SLIP until it is logged out.

Default Disabled.

See Also Set / Define Ports SLIPdetect, page 13-120; Set SLIP, page 13-145; Show / Monitor / List Ports SLIP, page 13-155; *PPP and SLIP*, page 3-8.

13.10 Define Site

Creates a new site with the given name. See the following Define Site commands for additional site configuration options.

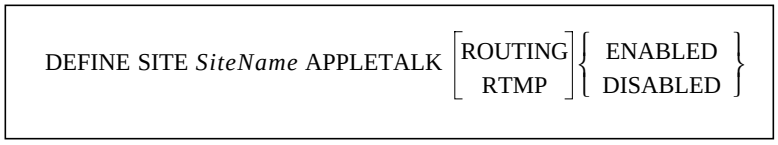
Restrictions You must be the privileged user to use this command.

Examples

```
Local>> DEFINE SITE irvine
```

See Also The additional Define Site commands listed on the following pages.

13.10.1 Define Site AppleTalk



Enables or disables the AppleTalk protocol for a site, and configures general routing information for the site.

Restrictions You must be the privileged user to use this command.

Parameters

Routing
Specifies that the site is for a LAN to LAN connection (if enabled) or a remote node connection (if disabled).

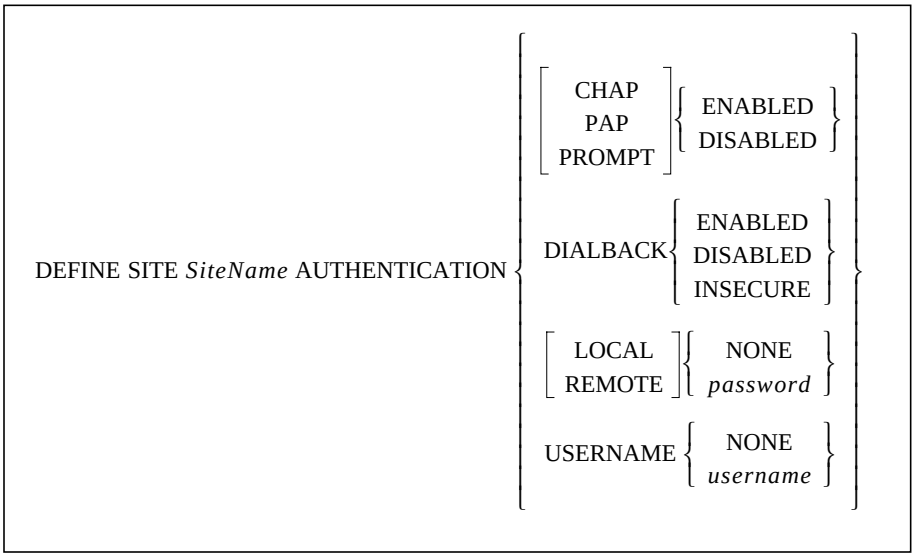
RTMP
Configures whether the site will accept packets that update the AppleTalk routing table. When this option is enabled, the site will accept RTMP update packets from other routers on the network.

Examples

```
Local>> DEFINE SITE irvine APPLETALK ENABLED

Local>> DEFINE SITE dallas APPLETALK ENABLED APPLETALK ROUT-
ING ENABLED
```

See Also Set / Define AppleTalk commands, page 13-59; Show / Monitor / List AppleTalk, page 13-147; *AppleTalk Networking*, page 7-5.

13.10.2 Define Site Authentication



Defines authentication information, such as site names and passwords, for link protocols that support authentication (for example, PPP).

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
A site name of up to 12 characters.

CHAP
Enables or disables the Challenge Handshake Authentication Protocol for outgoing calls.

PAP
Enables or disables the Password Authentication Protocol for outgoing calls.

Prompt
When Prompt is enabled, incoming callers will be prompted for the local password before starting PPP or SLIP.

Dialback
If Dialback is enabled, when the site receives an incoming connection, the LRS will hang up and initiate an outgoing connection to verify the caller's identity. If Insecure dialback is enabled, the caller may be given the option of specifying the dialback telephone number.

The site must have at least one port and a telephone number defined for the outgoing connection (See Define Site Port).

Insecure
Allows CBCP-aware PPP clients the option of choosing their own number for dialback. Be sure to read the cautions listed under *Dialback Using Call-back Control Protocol (CBCP)* on page 12-6.

Local
Defines the password required from the remote host. Must be used in conjunction with the *None* or *password* parameters.

Remote
Defines the password to be sent to the remote host. Must be used in conjunction with the *None* or *password* parameter.

Username
Define the username to be sent to the remote site. Must be used in conjunction with the *None* or *username* parameters.

None
Specifies that a password or username will not need to be used.

password
A password of up to 10 alphanumeric characters.

username
A username of up to 10 characters.

NOTE: *CHAP and PAP are part of PPP.*

Defaults

Dialback, Prompt, CHAP, and PAP: Disabled.

Local, Remote, and Username: None (no password or username defined).

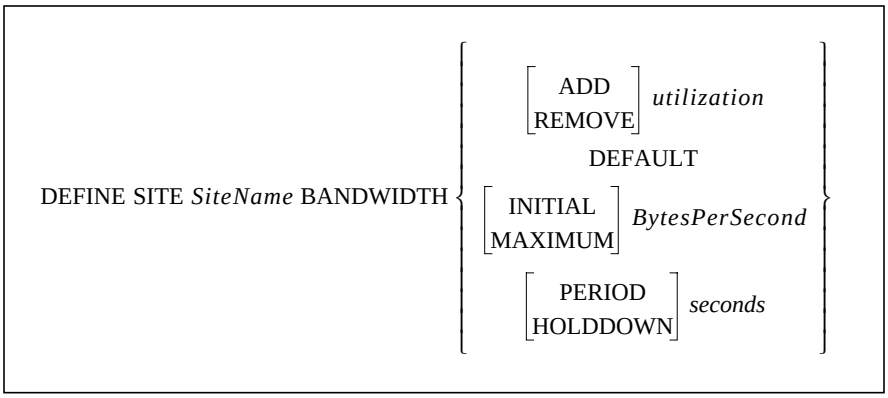
Examples

```
Local>> DEFINE SITE irvine AUTHENTICATION CHAP ENABLED

Local>> DEFINE SITE irvine AUTHENTICATION REMOTE NONE
```

See Also

Clear / Purge Authentication, page 13-5; Set / Define Authentication, page 13-62; Define Ports Dialback, page 13-15; Show / Monitor / List Authentication, page 13-148; Chapter 12, *Security*.

13.10.3 Define Site Bandwidth



Sets the initial or maximum amount of bandwidth that should be used when connecting to the specified site. Also controls how the LRS calculates the bandwidth needed, and how often it is checked to see if it is within the desired range.

NOTE: *This command is only useful when Multilink (bandwidth on demand) is enabled. See Define Ports PPP Multilink on page 13-28 and Bandwidth On Demand on page 4-9 for more information.*

Restrictions

You must be the privileged user to use this command.

Parameters

SiteName
A site name of up to 12 characters.

Add
Attempts to add bandwidth whenever usage reaches a specified percentage. Must be used in conjunction with the *utilization* parameter.

Remove
Removes bandwidth when usage falls below a certain percentage. Must be used in conjunction with the *BytesPerSecond* parameter.

utilization
The percentage of usage above which the LRS will attempt to add bandwidth and below which the LRS will remove bandwidth.

Default
Returns the bandwidth to the LRS's default setting.

Initial
Sets the initial amount of bandwidth. Must be used in conjunction with the *BytesPerSecond* parameter.

Maximum
Sets the maximum amount of bandwidth. Must be used in conjunction with the *BytesPerSecond* parameter.

BytesPerSecond
The precise bandwidth amount, up to 6,550,000 bytes per second. The server will add ports until it reaches the specified amount.

BytesPerSecond is truncated to the nearest 100. For example, a setting of 3840 is truncated to 3800.

NOTE: *A BytesPerSecond value below of 99 or less truncates to zero, disabling bandwidth.*

Period
Sets the number of seconds (specified by the seconds parameter) used to calculate average utilization statistics. The value is expressed as percent usage over a period of time.

Holddown
Specifies the minimum amount of time, in seconds, after adding or removing bandwidth to the remote site before bandwidth can be adjusted again. Must be used in conjunction with the *seconds* parameter.

Adding bandwidth after it has been removed or removing bandwidth after it has been added requires double the number of *seconds*. For example, if a holddown value of 5 is specified, adding bandwidth after it has been removed will require a 10 second delay.

Defaults Add and Remove: Disabled (utilization = 0).

Default: bring up one port.

Initial and Maximum: 100 bytes per second.

Period: 60 seconds.

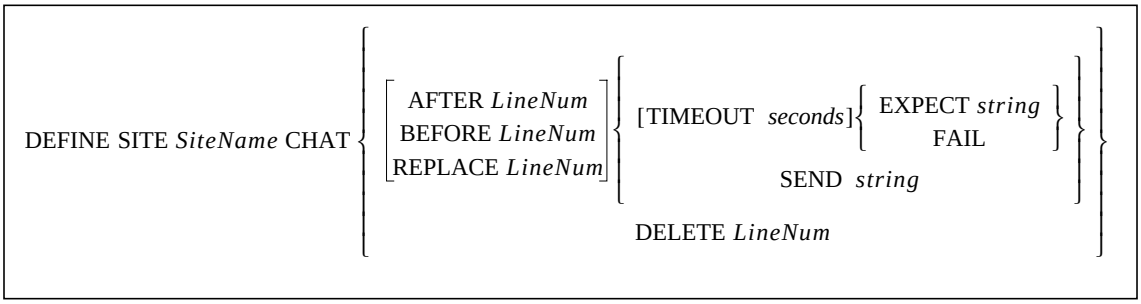
HoldDown timer: 60 seconds.

Examples

```
Local>> DEFINE SITE irvine BANDWIDTH INITIAL 123

Local>> DEFINE SITE irvine BANDWIDTH ADD 50

Local>> DEFINE SITE irvine BANDWIDTH PERIOD 6
```

See Also Define Ports PPP Multilink, page 13-28; Define Site Port Bandwidth, page 13-43; Show / Monitor / List Sites Bandwidth, page 13-161; *Bandwidth On Demand*, page 4-9.

13.10.4 Define Site Chat



Configures a **chat script** to automate the login sequence when connecting to a remote site. Chat scripts are a set of commands that send data to the remote site and wait for certain replies after the modems (if any) have connected. Based on the replies, other commands are executed.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

After
Inserts a line after another line.

Before
Inserts a line before another line.

Replace
Replaces a line with another line, specified with the *LineNum* parameter.

NOTE: *The default is to append information to the end of the script.*

Timeout
Sets the time to wait before commands, or the number of times to wait for input on a command before giving up. Must be used in conjunction with the *seconds* parameter.

seconds
A number of seconds or tries between zero and 65500.

Expect
Looks for a *string* before executing the next line of the script.

string
The following special characters can be used in CHAT script expect strings, which are case-sensitive.

String	Meaning	String	Meaning
\N (0x0 hex)	Newline	\b (0x8 hex)	Backspace
\r (0xd hex)	Return	\n (0xda hex)	Newline
\t (0x14 hex)	Tab	\\ (0x5c hex)	\
\s (0x20 hex)	Space	\octal	Octal value (i.e., \101 = ”A“)

Fail
Uses the number specified as the Timeout *seconds* parameter to set the number of times the search for a string (specified with the Expect parameter) can fail before the whole script will give up. Each time the Expect command fails, the script continues at the last Fail command. This permits looping while waiting for a given prompt.

A sample script is displayed below.

```
Local>> DEFINE SITE irvine CHAT TIMEOUT 4 FAIL

Local>> DEFINE SITE irvine CHAT SEND “”

Local>> DEFINE SITE irvine CHAT TIMEOUT 2 EXPECT “login:”
```

This script will send a newline and wait for the string “login:” for two seconds. If found, the script will continue. If not, the script will search again three times before failing.

Send
Sends the specified string, followed by a newline character (0xd hex, 13 ASCII). If a string is not specified, only a carriage return is sent.

Delete
Removes a line.

LineNum
The line to remove.

Defaults Timeout: 0 (none defined).

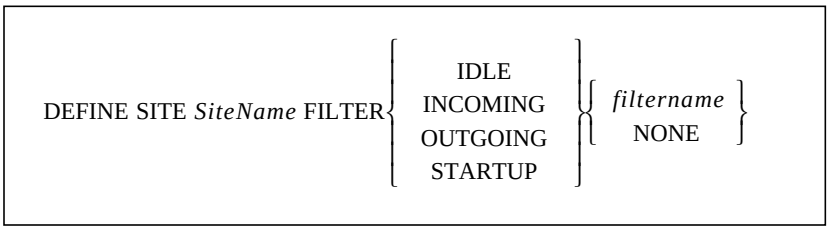
marker and string: not defined.

Examples

```
Local>> CHAT REPLACE 1 EXPECT “login:”

Local>> CHAT DELETE 1

Local>> CHAT TIMEOUT 2 EXPECT “login:”

Local>> DEFINE SITE irvine CHAT SEND “hello?”

Local>> DEFINE SITE irvine CHAT REPLACE 4 TIMEOUT 3 EXPECT
“login:”
```

See Also Show / Monitor / List Sites CHAT, page 13-161; *Chat Scripts*, page 4-7.

13.10.5 Define Site Filter



Configures packet filters for the site. If a particular packet filter is not configured, all packets are considered matches of that filter type and are accepted. For example, if no incoming packet filter is configured, all packets will be accepted as incoming packets and will be allowed in.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

Idle
Configures the packet filter that resets the idle timer. Packets that pass this filter will reset the timer, keeping the site from timing out and disconnecting. Must be used in conjunction with the *filtername* parameter.

Incoming
Configures the packet filter for packets that come into the LRS from the remote site. Packets that do not pass this filter will be dropped. Must be used in conjunction with the *filtername* parameter.

Outgoing
Configures the packet filter for packets going from the LRS to the remote site. Packets that do not pass this filter will be dropped. Must be used in conjunction with the *filtername* parameter.

Startup
Configures the packet filter for regulating connections. Packets that pass this filter can cause the site to initiate a connection. Packets that do not pass this filter will be dropped if a link is not already in place, but will continue to their destination if a link has already been established. Must be used in conjunction with the *filtername* parameter.

filtername
Sets the filter to be used for a specific type of packet filtering. Filter names must be 3 characters or fewer.

None
Clears any previously-set filter for that site.

Examples

```
Local>> DEFINE SITE irvine FILTER IDLE a3f

Local>> DEFINE SITE irvine FILTER IDLE m00

Local>> DEFINE SITE irvine FILTER IDLE gb
```

See Also Clear / Purge Filter, page 13-6; Set / Define Filter, page 13-74; Show / Monitor / List Filter, page 13-148; *Filter Lists*, page 4-1.

13.10.6 Define Site Idle

DEFINE SITE *SiteName* IDLE *seconds*

Sets the maximum time, in seconds, that the specified site may be idle before the link is shut down ("timed out").

NOTE: *The LRS must be idle for at least 10 seconds before the link can be shut down.*

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

seconds
The maximum length of time (specified by an integer between 10 and 65,000) that the site can remain idle before the link disconnects. A time setting of 0 will disable timeouts.

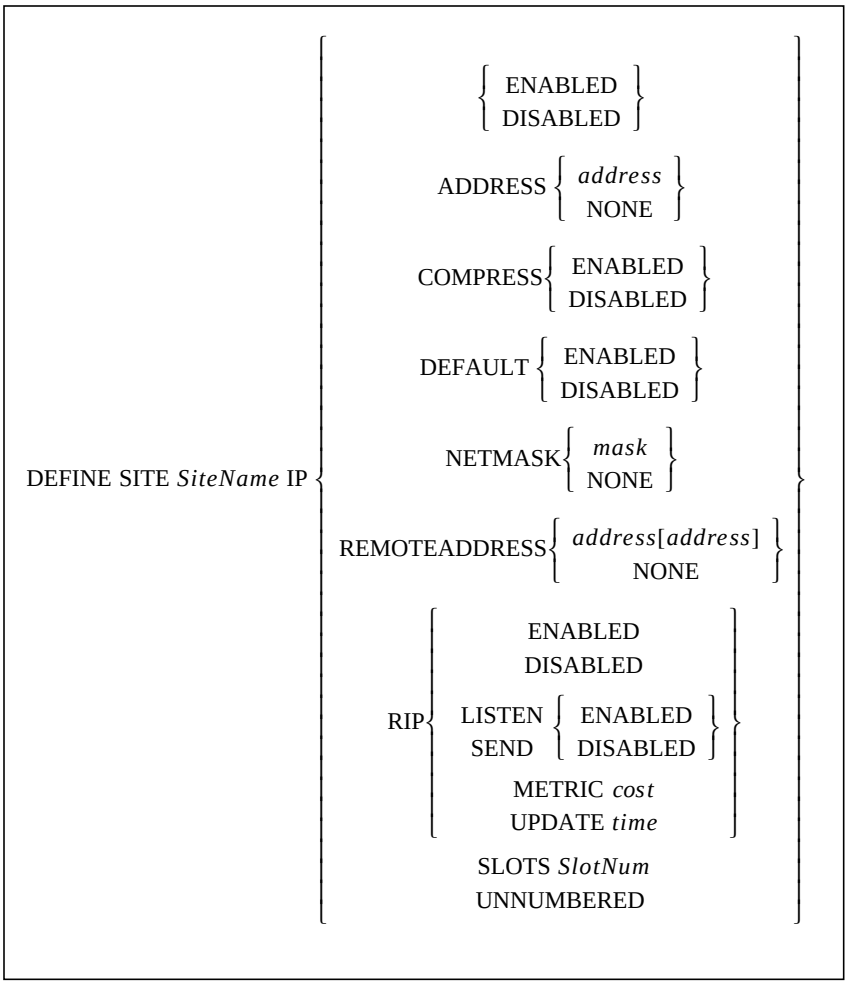
Default Idle time: 600 seconds.

Examples

```
Local>> DEFINE SITE irvine IDLE 600
```

See Also Define Site Filter Idle, page 13-37; Set / Define Server Inactivity, page 13-127; *Reducing Cost*, page 4-14.

13.10.7 Define Site IP



Configures the Internet Protocol (IP).

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

Enabled/Disabled
Enables or disables the site's use of IP. May be used instead of packet filters to prevent all IP packets from being forwarded.

Address
Sets the IP address (specified with the *address* parameter) on this server's IP interface.

Compress
Enables or disables header compression for the specified protocol.

Default
Advertises this server as the default route to the remote host.

Netmask
Sets the IP Netmask on this server's IP interface.

mask
A value that is used to remove bits that you do not want.

Remoteaddress
Sets the IP address (specified with the *address* parameter) of the remote host. If two address are specified, it indicates an acceptable range of addresses for the remote host.

Callers cannot use IP addresses with the host part of the address set to zero or -1; these addresses are reserved for broadcast packets. If the specified range includes such an address (for example, 192.4.5.0 or 192.4.5.255) and a caller requests this address, the connection will be denied.

address
An IP address in standard numeric format. For example, 192.0.1.3.

None
Clears a current IP address, Remoteaddress address, Othermask, or Netmask.

Unnumbered
An IP address is not to be expected from the remote site.

RIP
Enables or disables RIP parameters, and allows specification of update times and hop counts for the interface.

Enabled/Disabled
Enables or disables both listen and send at the same time.

Listen
Enables or disables RIP listening only.

Send
Enables or disables RIP sending only.

Metric
Configures the cost ("hop-count") of this interface. Routes learned through this interface will have this value added to their metric. Must be used in conjunction with the cost parameter.

cost
An integer between 1 and 16.

NOTE: *Metric is commonly used to make a given interface less desirable for backup routing situations.*

Update
Configures the time, in seconds, between sending a RIP packet. Must be used in conjunction with the *time* parameter.

time
An integer between 10 and 255 representing the number of seconds between updates.

Slots
Configures the number of header compression slots. Must be used in conjunction with the SlotNum parameter.

SlotNum
An integer between 1 and 254.

Defaults

IP, Compress, and RIP: Enabled.

Address, Netmask, and RemoteAddress: None.

Default: Disabled.

RIP Metric: 1.

Rip Updates: every 30 seconds.

Header compression slots: 16.

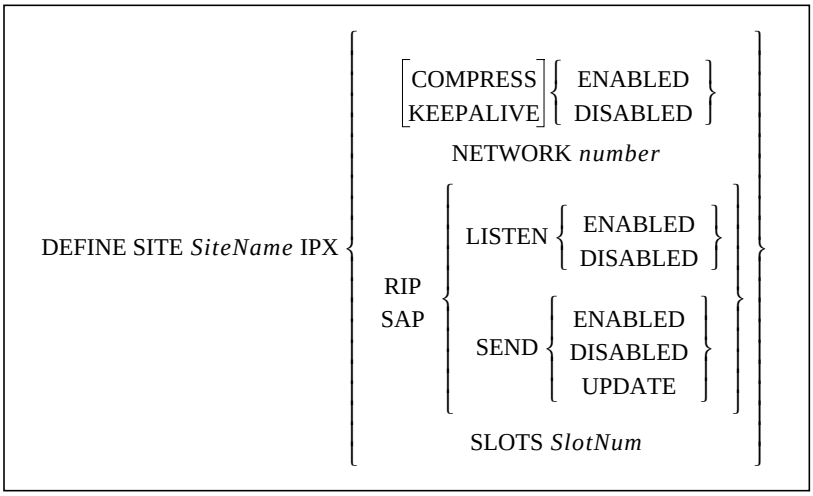
Examples

```
Local>> DEFINE SITE irvine IP SLOTS 16
Local>> DEFINE SITE irvine IP RIP UPDATE 30
Local>> DEFINE SITE irvine IP UNNUMBERED
Local>> DEFINE SITE irvine IP RIP METRIC 4
Local>> DEFINE SITE irvine IP COMPRESS ENABLED
Local>> DEFINE SITE irvine IP FORWARD ENABLED
```

See Also

Purge Site, page 13-54; Set / Define Logging Sites, page 13-96; Show / Monitor / List Sites, page 13-161; *IP Configuration*, page 4-3.

13.10.8 Define Site IPX



Configures the IPX Protocol. To simply turn on or turn off IPX routing for a site, enter Define Site *SiteName* IPX Enabled / Disabled.

Restrictions

You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

Enabled/Disabled
When used without the Compress or Keepalive keywords, enables or disables the site's use of IPX. May be used instead of packet filters to prevent all IPX packets from being forwarded.

Compress
Enables or disables header compression for the specified protocol.

Network
Configures the IPX network number to use for the specified site.

number
Enter the network number in hexadecimal digits from 0x0001 to 0xff00.

RIP
Configures the Routing Information Protocol (RIP) on this server's IPX interface.

SAP
Configures the Service Advertising Protocol (SAP) on this server's IPX interface.

Listen
Enables or disables RIP listening.

Send
Enables or disables RIP sending. Can also be used in conjunction with the Update parameter described below.

Keepalive
Enables or disables keepalive spoofing. When enabled, the LRS will send keepalive packets and responses to and from a file server and workstation. This permits the connection between the workstation and file server (or between two LRSs) to remain idle when there isn't interactive packet traffic; connections will not be initiated simply for keepalive packets.

Update
When used with the Send parameter, sends information only when the information is updated. This is the default setting for RIP and SAP.

Slots
Configures the number of header compression slots. Must be used in conjunction with the SlotNum parameter.

SlotNum
An integer between 1 and 254.

Defaults

Compress and Listen: Enabled.

Network number: 0x0.

Send: Update

Header compression slots: 0 (no header compression used).

Examples

```
Local>> DEFINE SITE irvine IPX COMPRESS ENABLED

Local>> DEFINE SITE IPX RIP LISTEN ENABLED

Local>> DEFINE SITE irvine IPX SAP SEND UPDATE

Local>> DEFINE SITE irvine IPX SLOTS 16
```

See Also

Purge Site, page 13-54; Set / Define Logging Sites, page 13-96; Show / Monitor / List Sites, page 13-161; *IPX Configuration*, page 4-5.

13.10.9 Define Site MTU

DEFINE SITE *SiteName* MTU *MaxSize*

Configures the maximum sized packet that the remote site may send to the LRS. Packets larger than this will be fragmented by the remote site.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
A site name of up to 12 characters.

MaxSize
Between 32 and 1522 bytes, inclusive.

NOTE: *The LRS will negotiate MTU with the remote site, so the actual MTU may be lower than what is configured.*

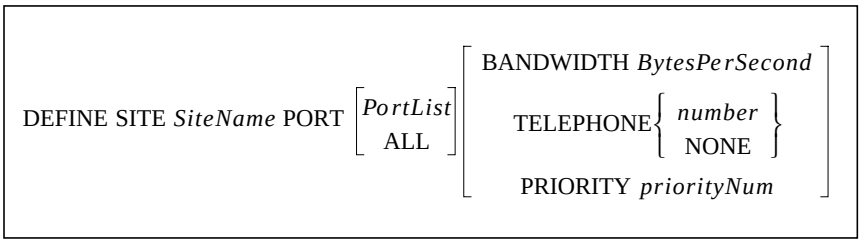
Default 1522 bytes.

Examples

```
Local>> DEFINE SITE irvine MTU 256
```

See Also Set / Define IP All / Ethernet MTU, page 13-82; Chapter 3, *Basic Remote Networking*.

13.10.10 Define Site Port



Configures a port that a site will use for its outgoing calls. Each port must have a telephone number associated with it. If multiple ports are associated with a site, they must be prioritized.

NOTE: *To purge the port setting from the site, see Purge Site on page 13-54.*

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
A site name of up to 12 characters.

PortList/All
Specifies a particular LRS port, a list or range of ports, or all ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *A port must be defined before the Bandwidth, BytesPerSecond, and Telephone parameters can be used.*

Bandwidth
Gives the LRS a bandwidth estimate for the device (for example, a modem) that is attached to the port. Must be used in conjunction with the *BytesPerSecond* parameter.

NOTE: *See Estimating Each Port's Bandwidth on page 4-10 for more information on how to use the port bandwidth setting.*

BytesPerSecond
The bandwidth value. The value can range from 100 to 6,550,000 bytes per second.

Telephone
Specifies a telephone number for this port. This number will override the number defined for the site as a whole. Must be used in conjunction with either the *number* parameter or the *None* parameter.

number
A telephone "number" of up to 24 characters (characters can be of any type).

None
No specific telephone number will be set for this port.

Priority
Specifies a priority level for a particular port. Higher priority ports will be dialed before ports with lower priority numbers. Must be used with the *prioritynum* parameter.

priorityNum
An integer between 1 and 100 representing the priority level of the specified port.

Default Bandwidth: 100 bytes per second.

Examples

```
Local>> DEFINE SITE irvine PORT 2 TELEPHONE "8675309"

Local>> DEFINE SITE irvine PORT 2 BANDWIDTH 28800
```

See Also Define Site Bandwidth, page 13-34; Define Site Telephone, page 13-45; Purge Site, page 13-54; Show / Monitor / List Sites, page 13-161; *How Bandwidth is Controlled*, page 4-9.

13.10.11 Define Site Protocol

DEFINE SITE *SiteName* PROTOCOL { PPP | SLIP }

Defines the “line” or “link layer” protocol that this site should use for outgoing calls. Resets the Maximum Transmission Unit (MTU) value to the default PPP or SLIP MTU value.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

PPP
PPP will be used for outgoing calls.

SLIP
SLIP will be used for outgoing calls.

Default PPP.

See Also Define Site MTU, page 13-43; *Link Layer Support*, page 1-2; *PPP and SLIP*, page 3-8.

13.10.12 Define Site Telephone

DEFINE SITE *SiteName* TELEPHONE { *number* | NONE }

Defines the telephone number of the remote site. Before you can assign a telephone number, you must associate the site with an LRS port or ports.

Restrictions You must be the privileged user to use this command.

Errors An error is returned if there is no port associated with the site.

Parameters

SiteName
Enter a site name of up to 12 characters.

number
A telephone “number” of up to 24 characters. Characters of any type can be used.

None
No telephone number will be defined for this site.

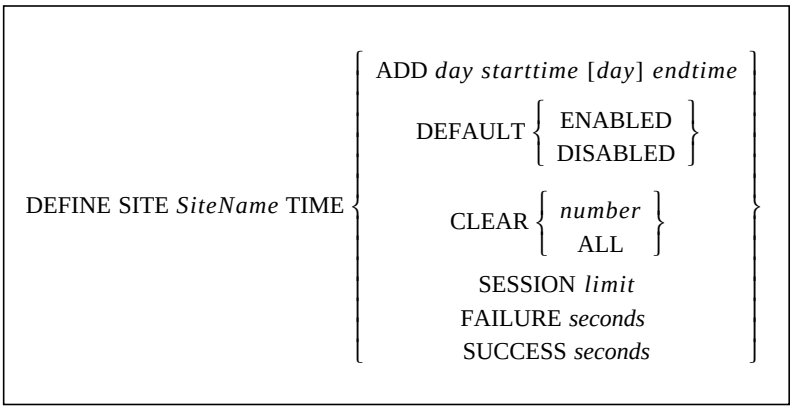
Default None (no telephone number is defined).

Examples

```
Local>> DEFINE SITE irvine TELEPHONE “8675309”
```

See Also Define Site Port Telephone, page 13-43; *Assign A Telephone Number to the Port or Site*, page 3-16.

13.10.13 Define Site Time



Configures the time ranges during which outgoing connections are allowed from this site, and during which bandwidth can be adjusted for this site.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
Enter a site name of up to 12 characters.

Add
When the Default setting is Enabled (see below), specifies when connections are not allowed. When the Default setting is Disabled, specifies when connections are allowed.

day
Specify the days during which Adding will start and stop. Must be followed by both starttime and endtime parameters. If a second day is not specified, it is understood that the start time and end time occur on the same day.

starttime, endtime
Specify the time when Add will go into effect, and the time when Add will end, on the specified day. Times are specified in hh:mm format and are ordered with respect to their time settings rather than the order in which they were entered. Specified times are combined if appropriate.

NOTE: *Show/Monitor/List Sites SiteName Time displays the time ranges and their order.*

Default
Set the default access parameter for the site.

If the default is enabled, connections are allowed except during the times specified. If the default is disabled, connections are restricted except during the times specified.

Clear
Remove a time range.

number
A time range to be removed. Time ranges are listed in numerical order.

All
Remove all time ranges.

Session
Sets the total time, in seconds, that this site can be active before it is logged out. Must be used in conjunction with the *limit* parameter.

limit
Specify a time range from 10 to 65,000 seconds. A setting of zero disables the session limit.

Success
Specifies a delay after a successful connection before another connection will be attempted. Must be used in conjunction with the *seconds* parameter.

Failure
Specifies a delay after a failed connection attempt before another connection will be attempted. Must be used in conjunction with the *seconds* parameter.

NOTE: *The success and failure settings control the time between calls. If the connection worked, the LRS waits for the success delay to pass before attempting another connection. If the connection did not work, the LRS waits for the failure delay to pass.*

seconds
A delay time of 1 to 65000 seconds.

Connection
Specifies the minimum amount of time, in seconds, after a connection drops or fails before attempting to form another connection. Must be used in conjunction with the seconds parameter.

Defaults

Default: Disabled (connections are allowed only during times specified).

Success: 1 second.

Failure: 30 seconds.

Session: 0 seconds (disabled).

Examples

```
Local>> DEFINE SITE irvine TIME ADD mon 8:00 mon 17:00

Local>> DEFINE SITE irvine CLEAR TIME 3
```

See Also

Set / Define Server Clock, page 13-126; Set / Define Server Timezone, page 13-136; Set / Define IP Timeserver, page 13-90; Set / Define IPX Timeserver, page 13-95; Show / Monitor / List Sites Time, page 13-161; *Getting Timesetting Information*, page 4-16.

13.11 Disconnect

Terminates the current session (if no session is specified), the specified session, or all sessions.

Examples

```
Local> DISCONNECT
```

```
Local> DISCONNECT SESSION 3
```

See Also Connect, page 13-12; Show / Monitor Sessions, page 13-161; *Exiting Sessions*, page 9-5.

13.12 Finger

This command is based on the UNIX Finger command that displays local and remote users.

If a *username* is specified, information about that username will be displayed. If the *user@host* parameters are specified, information regarding user *user* on TCP / IP host *host* will be displayed. Using the Finger command without any parameters will display the current logins.

Restrictions Secure users cannot use the finger command.

Errors An error is displayed if the host cannot be accessed.

Parameters

username
A username. If this parameter is omitted, all users on the host will be displayed.

@host
The "at" character, followed by a hostname.

Finger
Displays a list of current processes.

Examples

```
Local> FINGER bob
```
(shows user bob on LRS)

```
Local> FINGER @hydra
```
(shows users on host hydra)

```
Local> FINGER bob@hydra
```
(shows user bob on hydra)

```
Local> FINGER FINGER
```
(displays LRS process list)

See Also Show / Monitor Users, page 13-163.

13.13 Forwards

FORWARDS

Cycles forward through your sessions in the order displayed by the Show Sessions command. The next session on the list becomes the active session. If there is only one active session, the session will resume. If the bottom of the session list is reached (the most recently started session) and this command is entered, the session at the top of the session list is resumed.

Errors An error is displayed if no sessions are active.

See Also Backwards, page 13-3; Set / Define Ports Forward Switch, page 13-112; Show / Monitor Sessions, page 13-161; *Sessions*, page 9-4.

13.14 Help

HELP[*command*[*parameter*]]

Accesses the LRS Help system. Using the Help command without any parameters displays all available commands. Specifying a command gives information about that command and a list of its parameters. Specifying a parameter gives information about the parameter, including any sub-parameters it may have.

Restrictions You must be the privileged user to view all Help text.

NOTE: *To become the privileged user, see Set Privileged/Noprivileged on page 13-124.*

Parameters

command
An LRS command name.

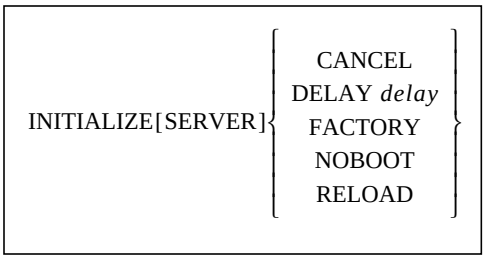
parameter
An LRS parameter name. More than one parameter can be added to the Help command.

Examples

```
Local> HELP

Local> HELP CONNECT

Local>> HELP DEFINE SERVER BROADCAST
```

See Also Apropos, page 13-2.

13.15 Initialize Server



Controls LRS initialization and behavior after the unit is booted. When the server is initialized, all changes made using Set commands will be lost unless corresponding Define or Save commands were also made.

Restrictions You must be the privileged user to use this command.

Parameters

Cancel
Cancels any pending initialization.

Delay
Schedules the initialization to take place after a specified number of minutes. Must be used in conjunction with the delay parameter.

delay
An integer between zero and 120, representing seconds before the initialization. Zero specifies an immediate reboot.

NOTE: *Show/Monitor/List Server will display the time remaining before a scheduled initialization.*

Factory
Reloads the factory settings. All configurations made with Define and Save commands will be cleared and will have to be reconfigured.

Noboot
Forces the LRS to remain in the Boot Configuration Program instead of booting.

Reload
On Flash ROM equipped units, re-downloads the operational code and reprograms the Flash ROM.

Examples

```
Local>> INITIALIZE DELAY 12

Local>> INITIALIZE RELOAD DELAY 12

Local>> INITIALIZE FACTORY

Local>> INITIALIZE CANCEL
```

See Also *Rebooting the LRS*, page 2-6; *Reloading Operational Software*, page 2-7.

13.16 Lock

LOCK

Locks a port without disconnecting sessions. Users will be queried for a password (6 alphanumeric characters maximum) and asked to verify it. The port is then locked until the correct password is used to unlock it. If a user forgets the password, the privileged user must either logout the port using the Logout command (disconnecting all sessions) or use the Unlock Port command.

NOTE: *The password and verification are not displayed as the user types them.*

Restrictions Secure users may not lock their ports.

Examples

```
Local> LOCK
Password> donut (the passwords will not be echoed)
Verification> donut
Unlock password> donut
Local>
```

See Also Set / Define Server Lock, page 13-129; Unlock Port, page 13-166; Logout, page 13-51; Set / Define Ports Security, page 13-118; *Locking a Port*, page 9-9.

13.17 Logout

LOGOUT [PORT *PortList* | SITE *SiteName*]

Logs out a port or a site on the server. Active sessions are disconnected, and all site circuits are closed.

Restrictions Only privileged users can log out a port or site other than their own.

Parameters

Port
Logs out the list of ports specified with the *PortList* parameter.

PortList
Specifies a port or series of ports to be logged out. Multiple ports must be separated by commas (for lists) or dashes (for ranges).

NOTE: *If the PortList parameter isn't specified, the current port will be logged out.*

Site
Logs out a site, closing all circuits. Must be used in conjunction with the Site-Name parameter.

SiteName
A site name of up to 12 characters.

Examples

```
Local> LOGOUT
Local>> LOGOUT PORT 2,4-6
```

See Also *Automatic Logouts*, page 9-11.

13.18 Mode

MODE[COM *SerPort*:]*baudrate*[,*parity*[,*charsize*[,*stopbits*]]]

Immediately and permanently configures the serial port parameters. Mode is provided for DOS compatibility.

NOTE: *There should be no spaces between user-entered parameters (see Examples).*

Restrictions You must be the privileged user to use this command.

Parameters

SerPort
A serial port number.

baudrate
One of the following baud rates: 300, 600, 1200, 2400 4800, 9600, 19200, 38400, 57600, or 115200.

parity
One of the following parity settings: Odd, Even, or None.

charsize
7 or 8.

stopbits
1 or 2.

Examples

```
Local> MODE COM2:9600,odd,7
```

See Also Set / Define Ports Character Size, page 13-109; Set / Define Ports Parity, page 13-115; Set / Define Ports Speed, page 13-120; *Port Modes*, page 9-3.

13.19 Monitor

Displays current operating characteristics. The displayed information is updated every 3 seconds until a key is pressed. Each Monitor command and its parameters are documented together with the corresponding Show command (see Show / Monitor / List on page 13-146).

NOTE: *For a comparison between Show, Monitor, and List commands, see Show, Monitor, and List on page 2-3.*

Restrictions You must be the privileged user to use this command.

13.20 Netstat

NETSTAT

Displays the currently active network connections. Information is displayed for all supported protocols; the LRS currently supports the TCP / IP and IPX protocols. This information is primarily meant for debugging network problems.

Restrictions Secure users may not use this command.

13.21 Ping

PING *hostname*

Sends a TCP / IP request for an echo packet to another network host. This provides an easy way to test network connections to other TCP / IP hosts. In general, any host that supports TCP / IP will respond to the request if it is able, regardless of login restrictions, job load, or operating system.

NOTE: *If there is no reply from the host, this may indicate a network or TCP/IP configuration problem.*

Parameters

hostname
Text name or IP address of the network host.

Examples

```
Local> PING 192.0.1.23

Local> PING HYDRA.LOCAL.NET
```

See Also LRS **Installation Guide**.

13.22 Purge IP Ethernet

PURGE IP ETHERNET *num*

Removes the specified secondary Ethernet from the LRS permanent memory.

Restrictions You must be the privileged user to use this command.

Parameters

num
An integer specifying a secondary Ethernet. Numbering begins at 1.

See Also Set / Define IP All / Ethernet, page 13-82, Show / List Protocols IP Interfaces, page 13-157.

13.23 Purge IP Factory

PURGE IP FACTORY

Resets IP router options to their factory defaults.

Restrictions You must be the privileged user to use this command.

13.24 Purge IPX Factory

```
PURGE IPX FACTORY
```

Resets all IPX protocol options to their factory defaults.

Restrictions You must be the privileged user to use this command.

13.25 Purge Port

```
PURGE PORT { PortList } [ PPP ]
           { ALL      } [ MODEM ]
```

Resets a port to the factory default PPP or Modem settings, but without affecting any other port settings. When used without the PPP or Modem keywords, both PPP and modem settings are purged.

Restrictions You must be the privileged user to use this command.

Parameters

PPP
Resets all Link Control Protocol parameters on the specified port.

Modem
Clears the specified port's modem init information.

PortNum
Specifies a particular LRS port.

See Also Show / Monitor / List Ports, page 13-155; Define Ports commands, beginning on page 13-14; Set / Define Ports commands, beginning on page 13-104.

13.26 Purge Site

```
PURGE SITE { SiteName } [PORT [PortNum]]
           { ALL      }       [ ALL   ]
```

Removes a site, or removes ports from a site.

Restrictions You must be the privileged user to use this command.

SiteName
Enter a site name of up to 12 characters.

All
When used before the Port parameter, removes all ports from the specified site. When used either without the port parameter or both before and after the port parameter, removes all ports from all sites.

Port
Removes a port from a site. Must be used in conjunction with the *Port-Num* or *All* parameters.

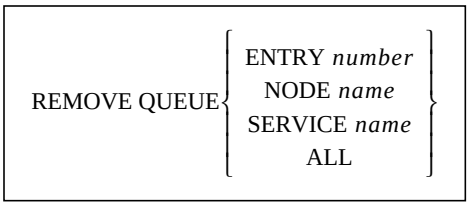
PortNum
An integer between 1 and 16.

Examples

```
Local>> PURGE SITE irvine PORT 2
```

See Also Define Site Port, page 13-43.

13.27 Remove Queue



Removes requests for local services from that service's queue. A particular request or all requests may be specified.

Restrictions You must be the privileged user to use this command.

Parameters

Entry
Specifies a particular queue entry to be removed. Must be used in conjunction with the *number* parameter.

number
A queue entry number.

Node
Specifies a particular node from which all connection requests will be removed. Must be used in conjunction with the *name* parameter.

Service
Specifies a particular local service; all entries queued to this service will be deleted. Must be used in conjunction with the *name* parameter.

name
A node or service name.

All
Removes all entries in the local service queue.

Examples

```
Local>> REMOVE QUEUE NODE hydra

Local>> REMOVE QUEUE ENTRY 5

Local>> REMOVE QUEUE SERVICE MODEM

Local>> REMOVE QUEUE ALL
```

See Also Show / Monitor Queue, page 13-158.

13.28 Resolve

RESOLVE *string*

Attempts to resolve a TCP/IP name from the local host table and/or network nameserver.

Parameters

string
A TCP/IP hostname. Hostnames are usually limited to 64 characters, so the string is limited to 64 characters.

Errors

An error is returned to signal either that the attempted name service failed, or that the specified hostname is invalid.

13.29 Resume

RESUME [[SESSION] *number*]

Leaves character (Local>) mode and resumes the current (active) session. To resume a session other than the current one, specify a session number with the *number* parameter.

Parameters

number
A session number, which can range from one to the total number of sessions that you currently have open.

Errors

An error is returned if there are no active or defined sessions.

Examples

```
Local> RESUME

Local> RESUME SESSION 4
```

See Also

Switching Between Sessions, page 9-5.

13.30 Rlogin

RLOGIN [*hostname* [*username*]]

Requests an Rlogin connection to a specified host, or the preferred TCP host if no host is specified.

NOTE: *Rlogin is an abbreviation for Connect Rlogin, described on page 13-12.*

Errors

An error is returned if Rlogin is not enabled. Secure users may only use the Rlogin command if it has been enabled for the server by a privileged user.

Parameters

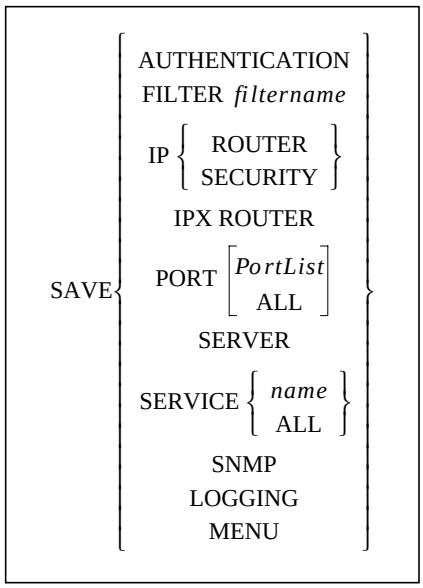
hostname
A text host name or an IP address in standard numeric format (for example, 192.0.1.183).

username
A username to use as the login name.

See Also

Connect, page 13-12; Set/Define Ports Password, page 13-116; *Establishing Sessions*, page 5-7.

13.31 Save



Saves current configurations (made with the Set command) into the permanent database. This treats configurations as if they were made using the Define command.

To easily make current changes permanent, use the Save command after you have configured the port, service, server or printer. This eliminates the need to issue a corresponding Define command for each Set command.

Restrictions You must be the privileged user to use this command.

Errors Save without a parameter is invalid.

Parameters

Authentication
Saves authentication database preferences and the local authentication database.

Filter
Saves the packet filter settings for the specified filter. Must be used in conjunction with the *filtername* parameter.

IP Router
Saves the state of the IP router.

IP Security
Saves the current IP security table to the permanent database.

IPX Router
Saves the state of the IPX router.

Menu
Saves all of the menu items setup using the Set Menu command (see page 13-100) to the permanent database.

Port
Saves the status of particular ports to the permanent database.

PortList
A port number or list of ports. Port numbers should be separated with commas (for lists) or dashes (for ranges).

All
Saves the settings for all ports or services to the permanent database.

Server
Save all the server characteristics to the permanent database.

Service
Save the current characteristics of a local service to the permanent database. To specify which services will be saved, the *All* parameter (for all local services) or a service name can be specified.

NOTE: *No more than one service per port can be defined at any time; if more than one service is defined, the Save Service command may fail.*

name
A service name.

SNMP
Saves all parameters associated with SNMP.

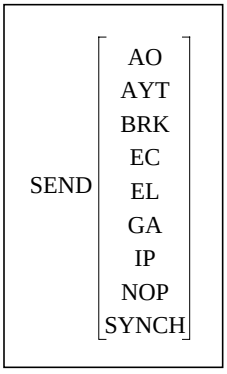
Logging
Saves the current logging configuration to the permanent database.

Examples

```
Local>> SAVE PORT 2

Local>> SAVE SERVICE NTX
```

See Also *Set and Define*, page 13-1.

13.32 Send



Sends Telnet commands through a session.

NOTE: *This command is only functional for Telnet TCP connections.*

Parameters

AO
Abort Output

AYT
Are You There

BRK
Break

EC
Erase Character

EL
Erase Line

GA
Go Ahead

IP
Interrupt Process

NOP
No Operation

SYNCH
Synchronize

13.33 Set/Define AppleTalk

13.33.1 Set/Define AppleTalk Ethernet Seed

```
{ SET    }
{ DEFINE } [PROTOCOLS] APPLETALK ETHERNET SEED { netlow nethigh                    }
                                               { ZONE zonename [ DEFAULT]          }
```

Specifies LRS Ethernet seed information, including AppleTalk zones associated with the LRS. If a default zone isn't specified, the first zone entered will automatically be assumed as the default.

If there is another seed router on the network, the LRS will copy seed information from it; configurations made with this command will be ignored.

NOTE: *AppleTalk routing should be disabled before seed configuration, and re-enabled only when all seed information has been entered.*

Restrictions You must be the privileged user to use this command.

Parameters

netlow
The lowest number of the network number range used for the Ethernet. Network numbers range from 1 to 65,280.

nethigh
The highest number of the network number range used for the Ethernet. Network numbers range from 1 to 65,280.

Zone
Specifies the zone(s) on the network. Multiple zones may be entered, but they must be entered on different command lines. If no default zone is specified, the first zone name entered is assumed to be the default.

zonename
A zone name of up to 32 alphanumeric characters.

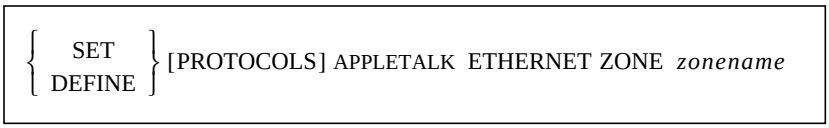
Default
Specifies that the named zone is the default zone for the network. Any subsequent default zone configuration overrides the previous default.

Examples

```
Local> DEFINE PROTO APPLETALK ETHERNET SEED ZONE marketing
DEFAULT
```

See Also Clear / Purge AppleTalk, page 13-4; Set / Define AppleTalk Routing, page 13-62; Show / Monitor / List AppleTalk, page 13-147; *Zones*, page 7-1; *AppleTalk Routing*, page 7-2; *Configuring the LRS*, page 7-3.

13.33.2 Set/Define AppleTalk Ethernet Zone



Specifies the zone to which the LRS belongs. This can be configured at any time without having to disable and re-enable AppleTalk routing.

Restrictions You must be the privileged user to use this command.

Parameters

zonename
A zone name of up to 32 alphanumeric characters.

Examples

```
Local> DEFINE PROTOCOLS APPLETALK ETHERNET ZONE comm_zone
```

See Also Show / Monitor / List AppleTalk, page 13-147; *Address Information*, page 7-3.

13.33.3 Set/Define AppleTalk Remote

Configures the addressing information needed for users dialing into the LRS for a remote node AppleTalk network connection. Only one zone / netnum pair can be configured for remote node users.

Restrictions You must be the privileged user to use this command.

Parameters

zonename
Enter the desired name for the AppleTalk zone used for remote node (dial-in) users. Zone names can be up to 32 alphanumeric characters.

netnum
Enter a non-extended network number to be used for the specified zone. Network numbers may range from 1 to 65,279.

Examples

```
Local> DEFINE PROTOCOLS APPLETALK REMOTE accounting 20
```

See Also Define Site AppleTalk, page 13-31; Show / Monitor / List AppleTalk, page 13-147; *Remote Node Connections*, page 7-6.

13.33.4 Set/Define AppleTalk Route

{ SET / DEFINE } [PROTOCOLS] APPLETALK ROUTE *zonename sitename metric netlow* [*nethigh*]

Configures routes to AppleTalk sites that the LRS will advertise on its attached Ethernet segment.

Restrictions You must be the privileged user to use this command.

Parameters

zonename
Enter a zone name of up to 32 alphanumeric characters.

sitename
Enter a site name of up to 12 characters. The LRS will use this site when making a connection to the specified zone.

metric
Enter a number from 1 to 15 representing the number of “hops” a packet takes to arrive at the site.

netlow
Specify the lowest number of the network number range used for the site as a 16-bit integer. For an extended network, the *nethigh* value must also be entered, even if it is the same number.

nethigh
Specify the highest number of the network number range used for the site. Although this parameter is not required for non-extended AppleTalk networks, it must be specified for extended networks, even if it is the same value as *netlow*.

Examples

```
Local> DEFINE APPLETALK ROUTE sales salesite 5 14 18.
```

See Also Clear / Purge AppleTalk, page 13-4; Define Site AppleTalk, page 13-31; Set / Define AppleTalk Routing, page 13-62; Set / Define AppleTalk Ethernet Seed, page 13-59; Show / Monitor / List AppleTalk, page 13-147; *LAN to LAN Connections*, page 7-5.

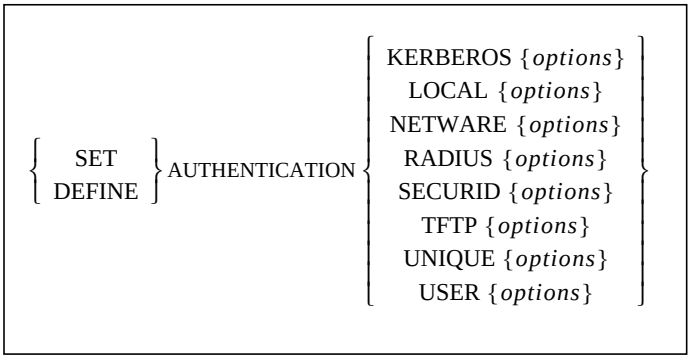
13.33.5 Set/Define AppleTalk Routing

Turns AppleTalk routing on or off. You must disable routing before defining zone name and network number pairs, then enable routing when finished. This ensures that other AppleTalk routers will receive and store the full list of zone / netnum pairs associated with the LRS.

Restrictions You must be the privileged user to use this command.

See Also Set / Define AppleTalk Route, page 13-61; Set / Define AppleTalk Ethernet Seed, page 13-59; Show / Monitor / List AppleTalk, page 13-147; *AppleTalk Routing*, page 7-2.

13.34 Set/Define Authentication



Configures the authentication system. Logins on ports with authentication enabled will be prompted for a username and a password pair, which will be checked sequentially against up to six databases: a Kerberos database, the LRS local database (NVR), a NetWare bindery, a RADIUS server, a SecurID server, or a UNIX password file (via TFTP).

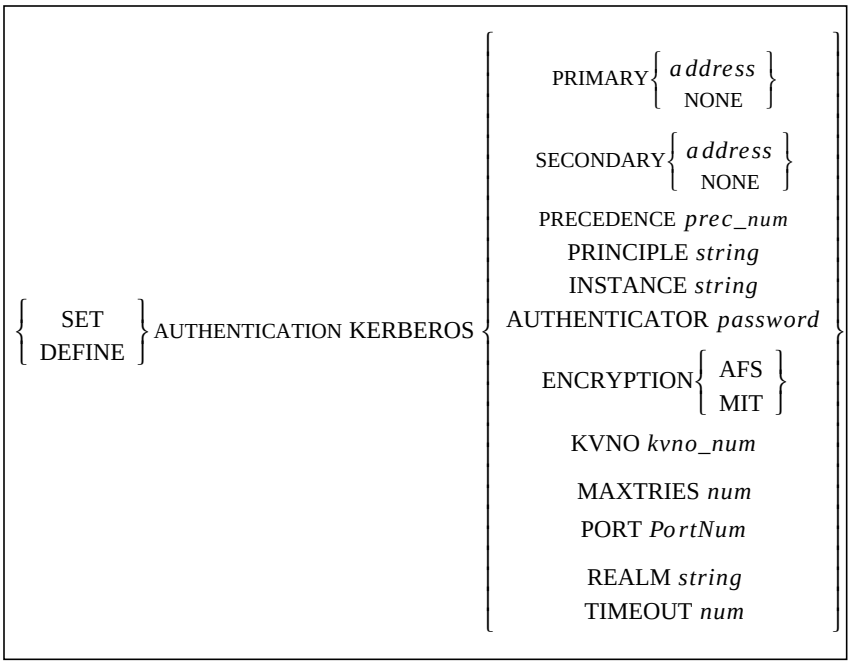
To configure one or more of the six databases, refer to the appropriate command on the following pages; for example, Set / Define Authentication NetWare is shown on page 13-66.

NOTE: *Precedence settings should be configured carefully. If a database is configured for a precedence slot that has already been filled by another database, it will take over the precedence setting and return all of the previous database's settings to their factory defaults.*

Restrictions You must be the privileged user to use any authentication command.

See Also Define Site Authentication, page 13-32; Chapter 12, *Security*.

13.34.1 Set/Define Authentication Kerberos



Specifies that a Kerberos database will be used for authentication. Specific Kerberos options are explained in greater detail in the *Kerberos* section on page 12-9.

Restrictions You must be the privileged user to use this command.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

If the LRS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username / password), the secondary database or server (discussed below) will be checked. If the user is authenticated at any point, the search process will stop and the login will be permitted.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

Secondary
Sets the secondary database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *prec_num* parameter.

prec_num
A precedence number between 1 and 6.

Principle
A label that identifies the authentication service that the LRS requests from the Kerberos server. Must be used in conjunction with the *string* parameter.

Instance
A label that is used to distinguish among variations of the principle. Must be used in conjunction with the *string* parameter.

string
A string of up to 40 alphanumeric characters.

Authenticator
Specifies the password for the principle/instance pair. Must be used in conjunction with the *password* parameter.

password
A case-sensitive password of up to 40 alphanumeric or 8 hexadecimal characters. To preserve case, alphanumeric passwords must be enclosed in quotes.

Encryption
Specifies that either the Andrew File System (AFS) or MIT encryption algorithm will be used to create the Kerberos keys. The LRS encryption method should match the Kerberos server encryption method.

MIT
Enables use of the MIT encryption algorithm.

AFS
Enables use of the Andrew File System encryption algorithm.

Port
Specifies the UDP/IP Port number used to communicate with the Kerberos server. The number applies to both the primary and secondary servers. Must be used in conjunction with the *PortNum* parameter.

PortNum
An integer between 1 and 65535.

Timeout
Specifies the timeout period for a response from the Kerberos server. Must be used in conjunction with the *seconds* parameter.

seconds
An integer between 1 and 255, inclusive.

Maxtries
Specifies the maximum number of times that the LRS will attempt to contact the Kerberos server. Must be used in conjunction with the *tries* parameter.

tries
An integer between 1 and 255, inclusive.

Realm
Sets the Kerberos realm that the LRS resides in. Often set to a name that mirrors the Internet domain name system. Must be used in conjunction with the *string* parameter, discussed on the previous page.

KVNO (Key Version Number)
Ensures that the LRS and the Kerberos server are using the correct authenticator for the defined principle/instance pair. The LRS KVNO must match the Kerberos server's KVNO. Must be used in conjunction with the *knvno_num* parameter.

kvno_num
An integer between 1 and 255, inclusive.

Defaults

Principle: rcmd.

Instance: lrs.

Encryption: MIT.

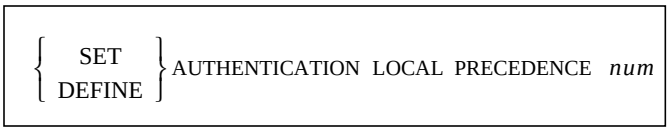
PortNum: 750.

Timeout: 3 seconds.

MaxTries: 5.

See Also Define Site Authentication, page 13-32; *Kerberos*, page 12-9.

13.34.2 Set/Define Authentication Local



Specifies that an LRS database (saved in NVR or RAM) will be used for authentication.

Restrictions You must be the privileged user to use this command.

Parameters

Precedence
Set the precedence in which this database or server is checked. Must be used in conjunction with the *prec_num* parameter.

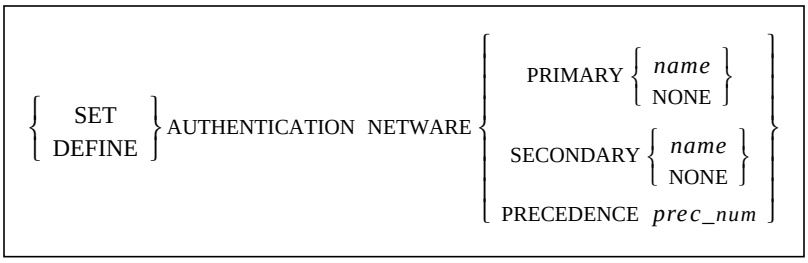
prec_num
A precedence number between 1 and 6, usually set to 1.

Examples

```
Local>> DEFINE AUTHENTICATION LOCAL PRECEDENCE 1
```

See Also Define Site Authentication, page 13-32; Set/Define Authentication Unique, page 13-72; *Local (NVR) Database*, page 12-8.

13.34.3 Set/Define Authentication NetWare



Specifies that a NetWare fileserver's database will be used for authentication.

Restrictions You must be the privileged user to use this command.

Parameters

Primary
Specifies the first database or server to be checked. A specific name may be set with the *name* parameter, or the None parameter may be used to indicate that the database or file will not be used.

If the LRS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/password), the secondary database or server (discussed below) will be checked. If the user is authenticated at any point, the search process will stop and the login will be permitted.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

Secondary
Sets the secondary database or server to be checked. A specific name may be set with the *name* parameter, or the None parameter may be used to indicate that the server will not be used.

name
A NetWare file server name of up to 31 characters.

None
Clears the current server name.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *prec_num* parameter.

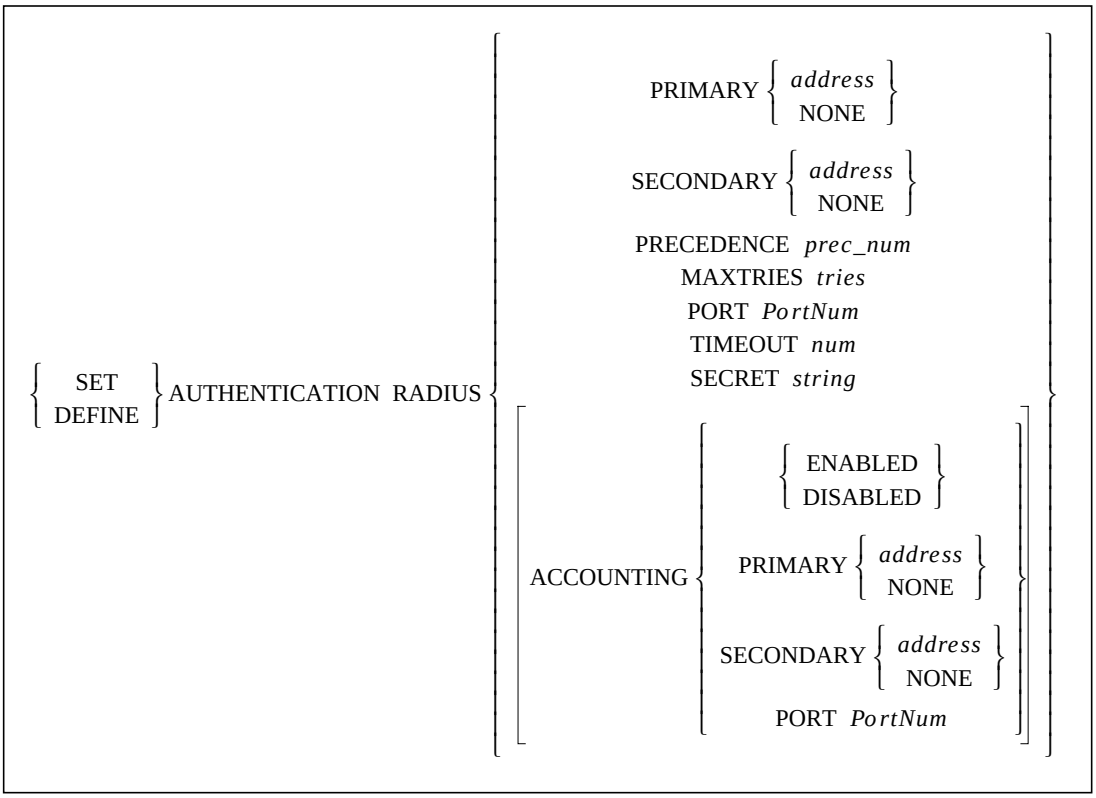
prec_num
A precedence number between 1 and 6.

Examples

```
Local>> SET AUTHENTICATION NETWARE PRIMARY doc_server
```

See Also Define Site Authentication, page 13-32; *NetWare Bindery*, page 12-11.

13.34.4 Set/Define Authentication RADIUS



Specifies that a RADIUS server will be used for authentication and/or accounting.

Restrictions You must be the privileged user to use this command.

Parameters

Primary
Specifies the first server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

If the LRS fails to authenticate the user using the primary or server (due to network failure, server failure, missing or incorrect username/password), the secondary database will be checked. If the user is authenticated at any point, the search process stops and the login is permitted.

If the user cannot be authenticated using the secondary server, the dataserver with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

Secondary
Sets the secondary server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *prec_num* parameter.

prec_num
A precedence number between 1 and 6.

Maxtries
Specifies the maximum number of times that the LRS will attempt to contact the RADIUS server. Maxtries must be used in conjunction with the *tries* parameter.

tries
An integer between 1 and 255, inclusive.

Port
Specifies that authentication or accounting information should be sent to a specific port on the server, specified with the *PortNum* parameter.

PortNum
A port number between 0 and 65535, inclusive.

Timeout
Specifies the timeout period for a response from the RADIUS server. Must be used in conjunction with the *num* parameter.

num
An integer between 1 and 255, inclusive.

NOTE: *For accounting, the LRS has to hold onto packets until they can be verified. If the Maxtries and Timeout values are too large, you can overflow the LRS and it will begin to drop accounting packets. This can be avoided by setting retries and timeouts to lower values.*

Secret
Specifies the Secret to be Shared between the RADIUS client and server. Must be used in conjunction with the string parameter.

string
A string of up to 64 characters. This string must be identical to that used by the RADIUS server for this LRS.

Accounting
Specifies that RADIUS accounting information will be sent to a RADIUS accounting server. Accounting can be enabled even if the LRS does not use a RADIUS server for authentication.

Primary
Specifies the primary accounting server to which accounting information will be sent. If the primary server cannot be reached, the secondary server will be tried.

Secondary
Specifies the secondary accounting server to which accounting information will be sent when the primary server cannot be reached.

PortNum
A port number between 0 and 65535, inclusive.

Defaults Authentication port: 1645.

Maxtries: 3.

Timeout: 1 (second).

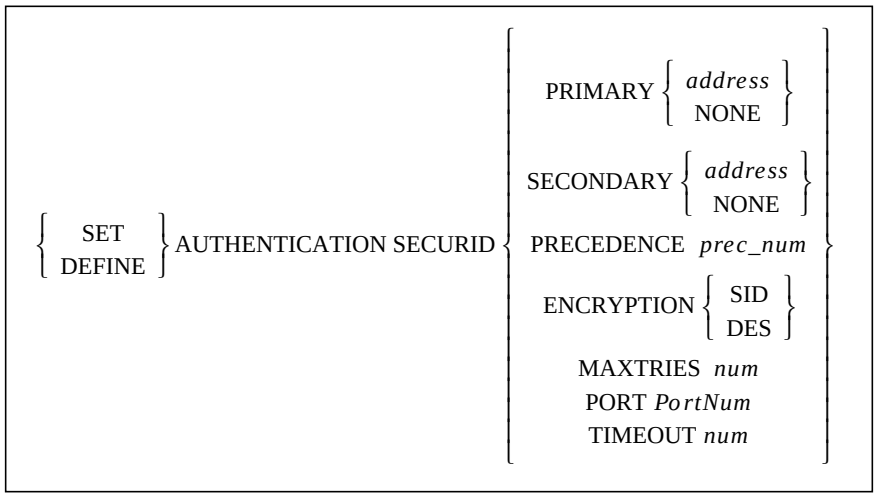
Accounting port: 1646.

Examples

```
Local>> DEFINE AUTHENTICATION RADIUS PRIMARY 192.0.1.55:1234
Local>> DEFINE AUTHENTICATION RADIUS TIMEOUT 10 MAXTRIES 4
Local>> DEFINE AUTENTICATION RADIUS ACCOUNTING ENABLED
```

See Also Clear / Purge Authentication, page 13-5; Define Site Authentication, page 13-32; Show / Monitor / List Authentication, page 13-148; *RADIUS*, page 12-12.

13.34.5 Set/Define Authentication SecurID



Specifies that a Security Dynamics ACE / SecurID server will be used for authentication.

Restrictions You must be the privileged user to use this command.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

Secondary
If the LRS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username / password), the secondary database or server will be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *prec_num* parameter.

prec_num
A precedence number between 1 and 6.

Encryption
SecurID (SID) or DES encryption will be used for authentication.

SID
Enables use of SecurID encryption.

DES
Enables use of DES encryption.

Maxtries
Specifies the maximum number of times the LRS will attempt to contact the SecurID server. Must be used in conjunction with the *tries* parameter.

tries
An integer between 1 and 255, inclusive.

Port
Specifies the UDP/IP Port number used to communicate with the primary and secondary SecurID servers. Must be used in conjunction with the *PortNum* parameter.

PortNum
An integer between 1 and 65535.

Timeout
Specifies the timeout period for a response from the SecurID server.Must be used in conjunction with the *seconds* parameter.

seconds
An integer between 1 and 255, inclusive.

Defaults

Encryption: DES.

MaxTries: 5.

UDP/IP port: 755

Timeout: 3 seconds.

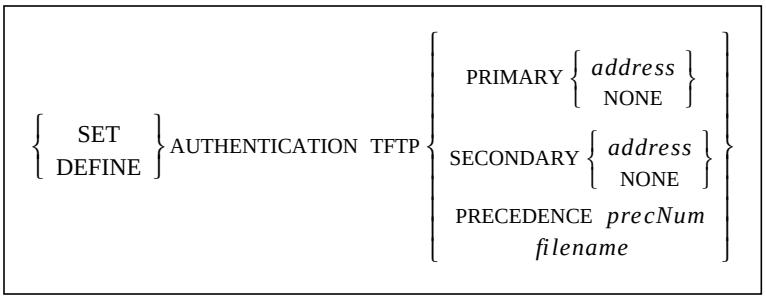
Examples

```
Local>> DEFINE AUTHENTICATION SECURID PRIMARY 192.0.1.55

Local>> DEFINE AUTHENTICATION SECURID TIMEOUT 10 MAXTRIES 4

Local>> DEFINE AUTHENTICATION SECURID ACCOUNTING ENABLED
```

See Also

Define Site Authentication, page 13-32; *SecurID*, page 12-15.

13.34.6 Set/Define Authentication TFTP



Specifies that a UNIX password file will be used for authentication. This file will be read via the TFTP protocol.

NOTE: *A TFTP-readable password file may reduce network security.*

Restrictions You must be the privileged user to use this command.

Parameters

Primary
Specifies the first database or server to be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the database or file will not be used.

Secondary
If the LRS fails to authenticate the user using the primary database or server (due to network failure, server failure, missing or incorrect username/password), the secondary database or server will be checked. A specific address may be set with the address parameter, or the None parameter may be used to indicate that the server will not be used.

If the user cannot be authenticated using the secondary database or server, the database or server with the next precedence level will be checked. If all precedence levels fail to authenticate the user, the user is prevented from logging in.

address
A text host name (if a DNS is available for name resolution) or an IP address in standard numeric format (for example, 193.23.71.49).

None
Clears the current server address.

Precedence
Set the precedence in which this database or server is checked. The precedence number must be specified using the *precNum* parameter.

precNum
A precedence number between 1 and 6.

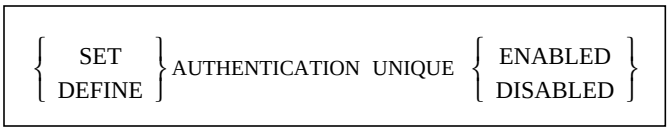
filename
Specifies a TFTP password file name of up to 32 characters. If spaces or lowercase characters are used, the filename must be enclosed in quotes.

Examples

```
Local>> SET AUTHENTICATION TFTP FILENAME radicchio
```

See Also Define Site Authentication, page 13-32; *UNIX Password File*, page 12-16.

13.34.7 Set/Define Authentication Unique

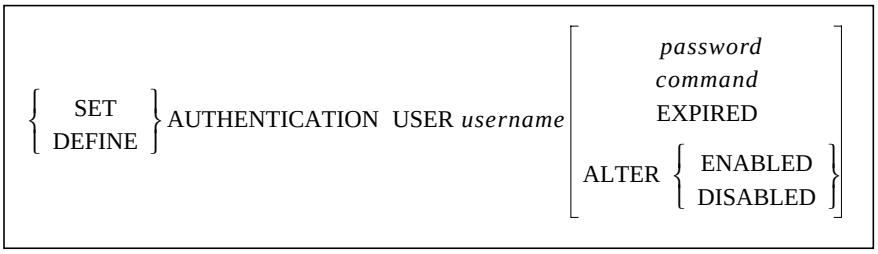


When enabled, the authentication code prevents multiple incoming authenticated logins by the same user. It does not prevent the user from making additional non-authenticated connections.

Restrictions You must be the privileged user to use this command.

See Also *Restricting Multiple Authenticated Logins*, page 12-20.

13.34.8 Set/Define Authentication User



Configures entries to the local database. To indicate which username entry will be modified, a username must be specified using the username parameter.

Restrictions You must be the privileged user to use this command.

Parameters

username
A username of up to 16 characters. The name is converted to all uppercase unless it is enclosed in quotes.

password
A password of up to 16 characters that the user must enter. The password is converted to all uppercase unless it is enclosed in quotes.

NOTE: *Users who don't have passwords configured for them will always be granted access.*

command
A command or series of commands that will be executed after login. Commands must be enclosed in quotes and separated by semicolons. The combined length of a series of commands cannot exceed 100 characters.

Expired
Forces a user to select a new password upon next login.

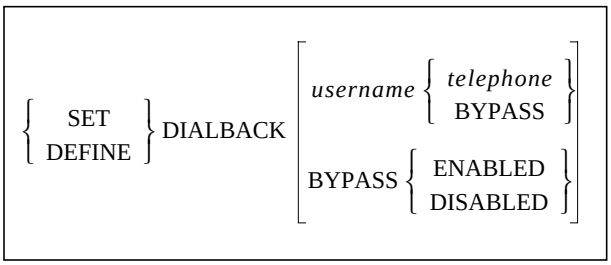
Alter
Enables or disables a user's ability to change his password. The password can be changed with the Set / Define Password command.

Examples

```
Local>> SET AUTH USER "fred" COMMAND "TELNET athena;LOGOUT"
```

See Also Define Site Authentication, page 13-32; Set / Define Authentication Local, page 13-65; Set / Define Password, page 13-103; *Local (NVR) Database*, page 12-8.

13.35 Set/Define Dialback



The Dialback feature enables a system manager to set up a dialback list of authorized users for incoming modem connections. Dialback lists include usernames and corresponding phone numbers. When a username entered matches one in the list, the port is logged out and the LRS sends the corresponding phone number to the serial port, at which time the port's modem profile initiates the modem connection.

Restrictions You must be the privileged user to use this command.

Parameters

username
A text name, up to 16 characters long. If white space or lowercase characters are used, the username must be enclosed in quotes.

telephone
A telephone number.

NOTE: *The atdt command should not be entered in the telephone number string. The modem profile will prepend any necessary command prefixes.*

Bypass
When the Bypass parameter is associated with a username, the port will not be logged out, and the user will not be dialed back, when attempting to connect to the LRS. The word "bypass" must be associated with the username in the dialback database in order for dialback to be bypassed.

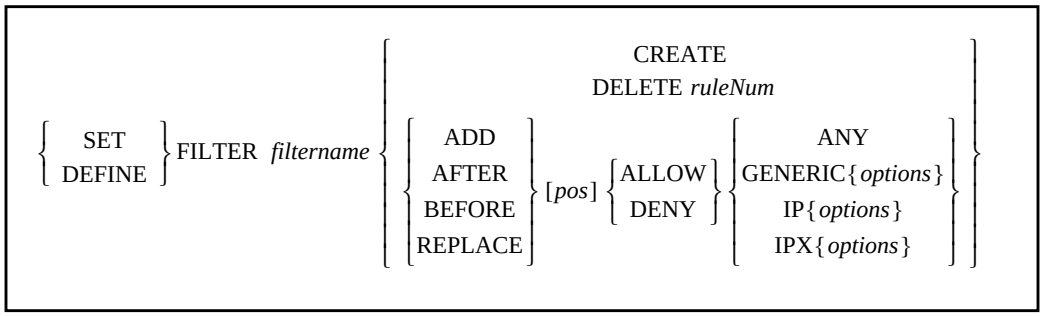
When Bypass is used with the Enabled parameter (that is, not associated with a username), users not in the dialback database are immediately given the local prompt. When disabled, users not in the database are denied access.

Examples

```
Local>> SET DIALBACK "susan" 867-5309
```

See Also Define Ports Dialback, page 13-15; *Dialback,* page 9-18; *Dialback*, page 12-6; *Dialback,* page 12-34.

13.36 Set/Define Filter



Creates or deletes a packet filter, or configures a rule in that filter that is used to manage network traffic. These packet filters are applied to packets arriving from or going to remote dialup sites.

Each rule consists of a name, a position, an action (allow or deny) and a protocol segment. To configure protocol *options*, refer to the appropriate command on the following pages. Due to space considerations, the command syntax from the Add braces to the Allow / Deny braces in the above diagram is represented by an ellipse (...) in the remaining Set / Define Filter commands.

Restrictions

You must be the privileged user to use this command.

Parameters

filtername
The name of the filter in which the new rule will be included, up to 12 letters in length.

Create
Creates a new filter with the specified filtername. Filters must be created before their rules can be added, deleted, or otherwise modified.

Delete
Removes the specified rule from the named filter.

ruleNum
The number of the rule to be deleted.

Add
Adds a rule after another rule. If no position is specified, the rule is added to the end of the list of rules.

After
Inserts a rule after another rule. If no position is specified, the rule is added to the end of the list of rules.

Before
Inserts a rule before another rule. If no position is specified, the rule is added to the beginning of the list of rules.

Replace
Replaces an existing rule with a new one. If no position is specified, the first rule in the list is replaced.

pos
A location in the filter list to perform a specific function, such as Add.

Allow
Allows passage of data packets that meet the defined filter criteria. The criteria consist of all specified parameters after Allow.

Deny
Denies passage of data packets that meet the defined filter criteria. The criteria consist of all specified parameters after Deny.

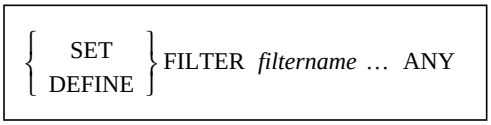
Examples

```
Local>> DEFINE FILTER abc CREATE

Local>> DEFINE FILTER abc DELETE 2
(Removes the second rule in filter list abc.)
```

In-depth protocol-related examples are given with the sub-commands listed on the following pages.

See Also Define Site Filter, page 13-37; Clear / Purge IP Security, page 13-7; Define Ports Dialback, page 13-15; *Packet Filters and Firewalls*, page 12-22.

13.36.1 Set/Define Filter Any



Specifies that every packet will be allowed or denied passage through the LRS. Using the Any parameter along with either Allow or Deny will affect all packets regardless of any filter specifications that follow. Usually, an Any rule is placed at the end of a filter list to process data packets not specifically identified by the previous rules in the list.

Restrictions You must be the privileged user to use this command.

See Also Define Site Filter, page 13-37; Clear / Purge IP Security, page 13-7; Define Ports Dialback, page 13-15; *Packet Filters and Firewalls*, page 12-22.

13.36.2 Set/Define Filter Generic

Specifies a general filter rule that applies to any packet regardless of protocol. A Generic rule starts at a location *offset* bytes from the beginning of the packet, applies the specified *mask*, and then compares the result with a specified *value*. Multiple generic offset segments can be included in a single rule, subject to the maximum command line length of 132 characters (see the example below).

Restrictions You must be the privileged user to use this command

Parameters

offset
Defines where in the data packet the LRS is to apply the mask. May be a decimal value from 0 to 1500, where 0 indicates the first data position in the packet.

mask
A hexadecimal or decimal number.

operator (GT, GE, EQ, NE, LE, LT)
The available operators are: greater than (GT), greater than or equal to (GE), equal to (EQ), not equal to (NE), less than or equal to (LE), and less than (LT).

value
A hexadecimal or decimal number.

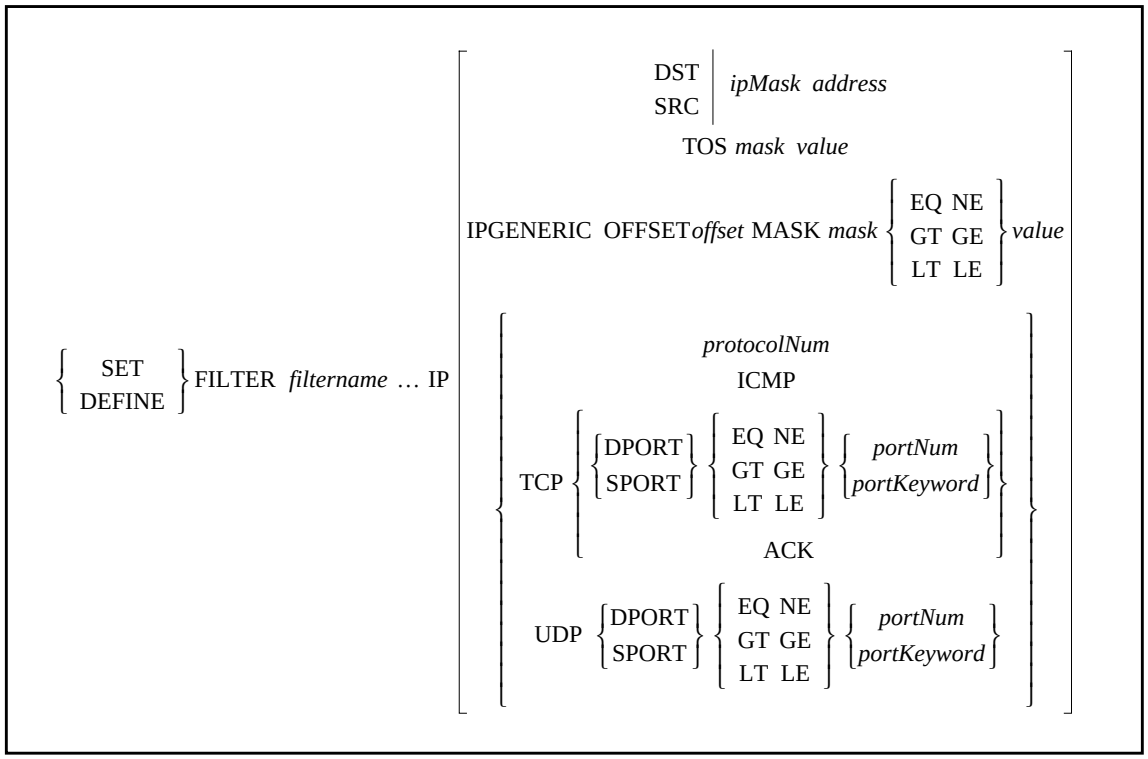
Examples

```
Local>> DEFINE FILTER abc ADD DENY GENERIC OFFSET 0 MASK
0xff000000 GT 0x25000000 OFFSET 8 MASK 0xffffffff EQ
0x12345678
```

(Adds a rule containing two generic segments to filter **abc**)

See Also Define Site Filter, page 13-37; Clear / Purge IP Security, page 13-7; Define Ports Dialback, page 13-15; *Packet Filters and Firewalls*, page 12-22.

13.36.3 Set/Define Filter IP



Creates a rule which will be applied only to IP protocol packets.

Restrictions You must be the privileged user to use this command

Parameters

DST
Allows or denies passage of data packets destined for a specific node on the local area network. Must be used in conjunction with the *ipMask* and *address* parameters.

SRC
Allows or denies passage of data packets that originated from a specific node on the local area network. Must be used in conjunction with the *ipMask* and *address* parameters.

ipMask
An IP address in standard numeric format (for example, 193.0.1.255).

address
An IP address in standard numeric format (for example, 193.0.1.50).

TOS
Builds a rule using the IP Type Of Service field. Must be used in conjunction with the *mask* and *value* parameters. For TOS, the operator EQ is implied.

IPGeneric
Specifies a general IP rule using one set of *offset*, *mask*, *operator*, and *value*. Multiple IPGeneric segments can be included in a single rule (in one command), subject to the maximum command line length of 132 characters.

offset
Defines where in the data packet to apply the mask. May be a decimal value from 0 to 1500, where 0 indicates the first data position in the data packet.

mask
A hexadecimal or decimal number. The *mask* is applied to the data using the operator and the result is compared with the *value*. In the case of TOS, the operator EQ is implied.

operator (GT, GE, EQ, NE, LE, LT)
The available operators are: greater than (GT), greater than or equal to (GE), equal to (EQ), not equal to (NE), less than or equal to (LE), and less than (LT).

value
A hexadecimal or decimal number.

protocolNum
Allows or denies packets of the protocol specified by an IP protocol identifier number between 0 and 65535.

ICMP
Allows or denies Internet Control Message Protocol packets.

TCP
Allows or denies TCP-based packets which match criteria specified by subsequent parameters. Applications that use TCP include Telnet, FTP, and SMTP (Simple Mail Transfer Protocol).

UDP
Allows or denies UDP-based packets which match criteria specified by subsequent parameters. Applications that use UDP include DNS (Domain Name Service), TFTP (a variant of FTP), and BOOTP (used by some computer systems to acquire IP addresses).

DPort
Defines the destination protocol port. Data packets are filtered based on both the protocol and on the protocol port of the data packet. Must be used in conjunction with either the *portNum* or *portKeyword* parameter.

SPort
Defines the source protocol port. Data packets are filtered based on both the protocol and on the protocol port of the data packet. Must be used in conjunction with either the *portNum* or *portKeyword* parameter.

portNum
A TCP or UDP port number.

portKeyword
A keyword corresponding to the TCP or UDP port number. Available keywords are BOOTP, DNS, FINGER, FTP, FTPDATA, HTTP, NNTP, NTP, POP2, POP3, RIP, SMTP, SNMP, SYSLOG, TELNET, and TFTP.

ACK
Allows or denies TCP-based packets in which the ACK (acknowledge) bit is set.

Examples

```
Local>> DEFINE FILTER abc ADD DENY IP
(Adds a rule for all IP traffic to filter abc)
```

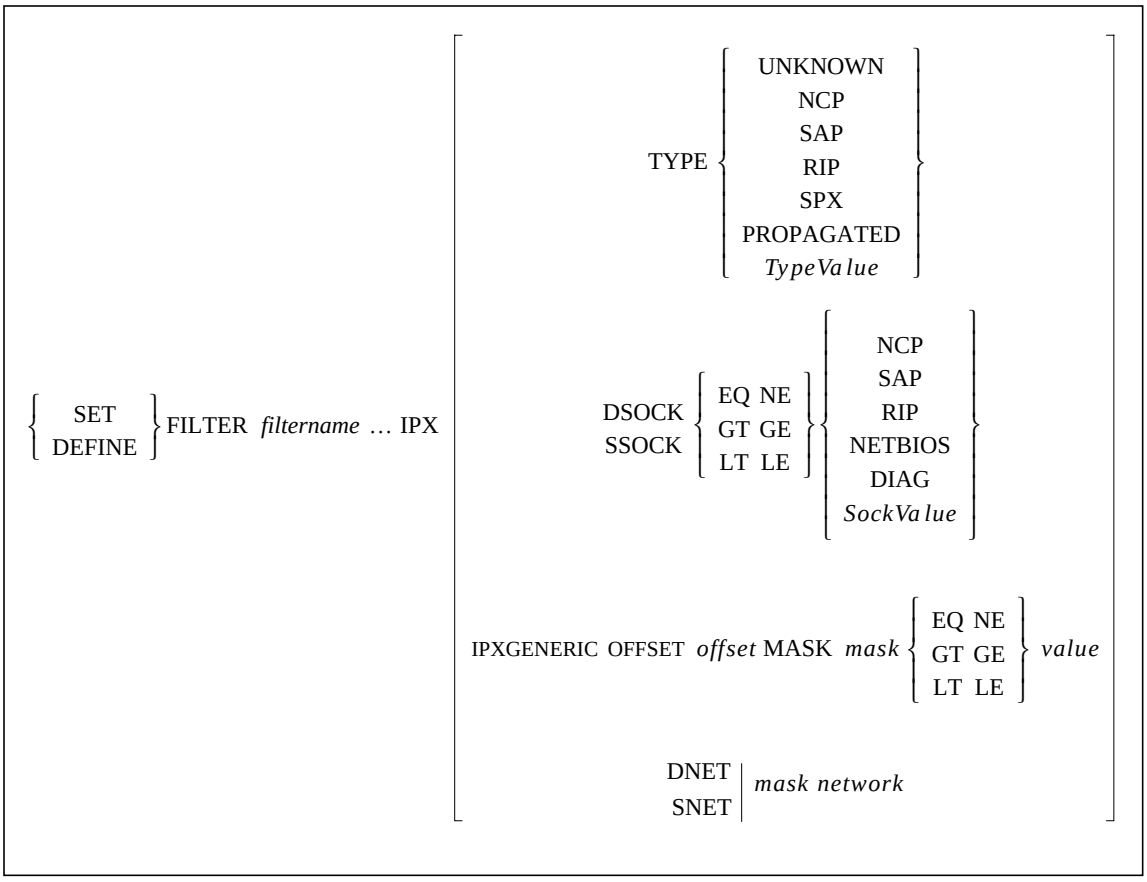
```
Local>> DEFINE FILTER abc ADD ALLOW IPGENERIC OFFSET 4 MASK
0xffff0000 LE 0x78140000 IPGENERIC OFFSET 8 MASK 0xff000000
EQ 0x12000000
(Adds a rule containing multiple IP generic segments to fil-
ter abc)
```

```
Local>> DEFINE FILTER abc ADD ALLOW IP IPGENERIC OFFSET 0
MASK 0xff000000 LT 0x34000000 TCP DPORT EQ TELNET
(Adds a rule containing an IP generic segment and DPORT to
filter abc)
```

```
Local>> DEFINE FILTER abc ADD ALLOW IP SRC 255.255.255.0
192.34.87.0 TCP DSOCK EQ NCP
(Adds a rule containing IP SPORT and SRC to filter abc)
```

See Also
Define Site Filter, page 13-37; Clear / Purge IP Security, page 13-7; Define Ports Dialback, page 13-15; *Packet Filters and Firewalls*, page 12-22.

13.36.4 Set/Define Filter IPX



Creates a rule which will be applied only to IPX protocol packets.

Restrictions You must be the privileged user to use this command

Parameters

Type
Specifies an IPX packet type. Some versions of NetWare don't set the packet type correctly (with the exception of propagated packets); socket values are more reliable in these instances.

Must be used with one of the predefined types (Unknown, RIP, SAP, SPX, NCP, or Propagated) or a hexadecimal *TypeValue*.

Unknown
Specifies the Unknown packet type (0).

NCP
Specifies the NCP packet type (0x11).

SAP
Specifies the SAP packet type (4).

RIP
Specifies the RIP packet type (1).

SPX
Specifies the SPX packet type (5).

Propagated
Specifies the propagated packet type (0x14). Used for Novell NetBIOS.

TypeValue
A hexadecimal value between 0x00 and 0xff.

DSOCK
Specifies the destination socket using predefined socket (NCP, SAP, RIP, NETBIOS, or DIAG) or a hexadecimal *SockValue*. The destination socket will be compared with the designated socket type using an *operator*.

SSOCK
Specifies the source socket using predefined socket (NCP, SAP, RIP, NETBIOS, or DIAG) or a hexadecimal *SockValue*. The source socket will be compared with the designated socket type using an *operator*.

operator (GT, GE, EQ, NE, LE, LT)
The available operators are: greater than (GT), greater than or equal to (GE), equal to (EQ), not equal to (NE), less than or equal to (LE), and less than (LT).

SockValue
A hexadecimal value between 0x0000 and 0xffff.

NCP
Specifies an NCP socket (0x451).

SAP
Specifies a SAP socket (0x452).

RIP
Specifies a RIP socket (0x453).

NETBIOS
Specifies a NetBIOS socket (0x455).

DIAG
Specifies a Diagnostic socket (0x456).

IPXGeneric
Specifies a general IPX rule. Multiple IPXGeneric segments can be included in a single rule (in one command), subject to the maximum command line length of 132 characters.

offset
Defines where in the data packet to apply the mask. May be a decimal value from 0 to 1500, where 0 indicates the first data position in the data packet.

mask
A hexadecimal or decimal number. The *mask* is applied to the data using the operator and the result is compared with the *value*. In the case of TOS, the operator EQ is implied.

value
A hexadecimal or decimal number.

DNET
Specifies the destination network. Must be used in conjunction with the *network* and *mask* parameters, described below. The mask will be used to match a range of addresses.

SNET
Specifies the source network. Must be used in conjunction with the *network* and *mask* parameters, described below. The mask will be used to match a range of addresses.

network
A 4-byte (8-digit) IPX network number in hexadecimal format.

mask
A 4-byte (8-digit) hexadecimal value.

Examples

```
Local>> DEFINE FILTER abc ADD DENY IPX
(Adds a rule for all IPX traffic to filter abc)

Local>> DEFINE FILTER abc ADD ALLOW IPX IPXGENERIC OFFSET 4
MASK 0xffff0000 LE 0x78140000
(Adds an IPX generic rule to filter abc)

Local>> SET FILTER abc ADD ALLOW IPX IPXGENERIC OFFSET 4 MASK
0xffff0000 LE 0x78140000 IPXGENERIC OFFSET 8 MASK 0xff000000
EQ 0x12000000
(Adds a rule containing multiple IPX generic segments to
filter abc)

Local>> SET FILTER abc ADD ALLOW IPX IPXGENERIC OFFSET 0 MASK
0xff000000 LT 0x34000000 TCP DSOCK EQ NCP
(Adds a rule containing an IPX generic segment and DSOCK to
filter abc)

Local>> SET FILTER abc ADD ALLOW IPX SRC 0xffffffff
0x12345678 SSOCK EQ NCP
(Adds a rule containing IPX SSOCK and SNET to filter abc)
```

See Also Define Site Filter, page 13-37; Clear / Purge IP Security, page 13-7; Define Ports Dialback, page 13-15; *Packet Filters and Firewalls*, page 12-22.

13.37 Set/Define Hosts

{ SET / DEFINE } [TELNET]HOSTS *hostname IPaddress*

Associates a TCP / IP *hostname* with an IP address in the local host table, allowing you to use the text name for Telnet connections even if there is no name server to resolve it. If the given host name has already been configured, the new IP address will replace the previous value.

Restrictions You must be the privileged user to use this command.

Errors IP addresses specified in a questionable format will be so noted.

Parameters

hostname
The hostname string you wish to define, limited to 64 alphanumeric characters with only 16 characters between any period delimiters.

IPaddress
Standard, numeric IP address of the machine referred to by the hostname.

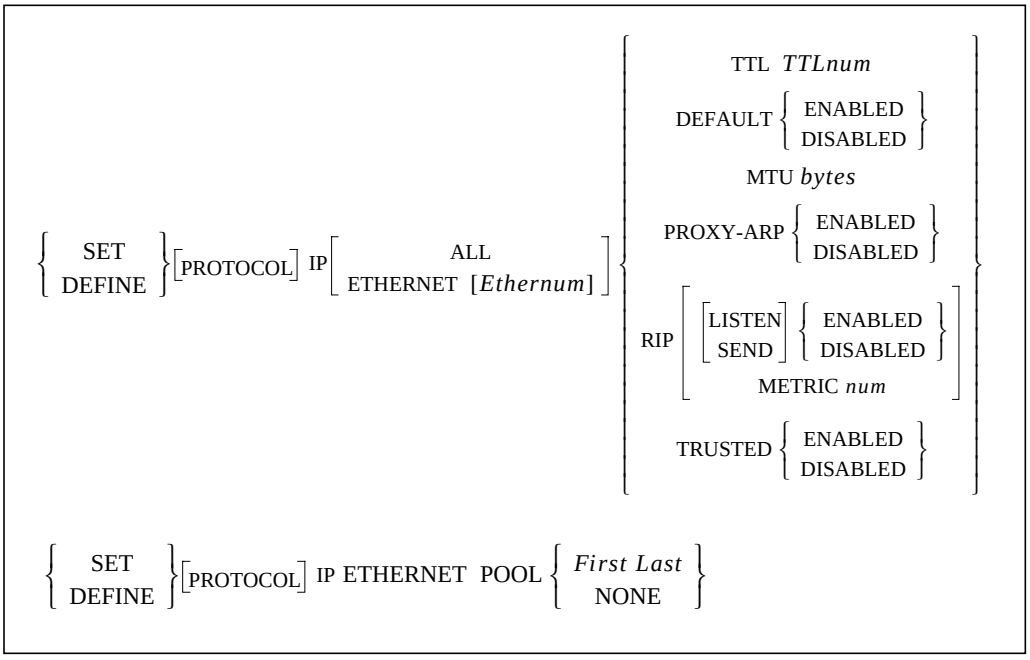
Examples

```
Local>> SET HOST spectre 192.0.1.11
```

See Also Clear / Purge Hosts, page 13-6; Show / Monitor / List Hosts, page 13-149; Show / Monitor / List Telnet Hosts, page 13-162.

13.38 Set/Define IP

13.38.1 Set/Define IP All/Ethernet



Configures all interfaces or an Ethernet interface.

Restrictions You must be the privileged user to use this command.

Parameters

All
Configures all IP interfaces.

Ethernet
Configures an Ethernet interface. To specify the number of the Ethernet, the *num* parameter must be used. If no number is entered, the configuration will affect the primary interface.

NOTE: *Servers with one Ethernet port do not need the optional Ethernet num parameter; when omitted, it defaults to zero.*

Ethernum
Enter the number of a specific secondary Ethernet interface. If a zero is entered, the configuration will affect the primary interface.

TTL
Sets the amount that the IP Time-To-Live value should be decremented by when routed through this interface. The specific amount must be set using the *TTLnum* parameter.

TTLnum
An integer between 1 and 127, inclusive.

Default
If enabled, IP routing updates will advertise this router as the “default” route. Default is commonly used to avoid large routing tables when there is only one possible path to a large number of networks.

MTU
Set the Maximum Transmission Unit, or "packet size" for this interface. Packets larger than this value will be IP fragmented when transmitted. Must be used in conjunction with the bytes parameter, discussed below.

bytes
An integer between 40 and 1500, inclusive.

Proxy-ARP
If enabled, an ARP response will be sent in reply to ARP requests for non-local networks to which the LRS knows a valid path. Commonly used to allow end hosts that don't understand routing or subnet masks to find a router.

Pool
Allocates a pool of IP addresses to dialin users. When Proxy-ARP is enabled, the LRS will respond to ARP requests to all addresses in the pool. Must be used with the *First* and *Last* parameters, or with the *None* parameter.

First
Specifies the start of the range of IP addresses to be used.

Last
Specifies the end of the range of IP addresses to be used.

None
Disables use of the IP address pool.

RIP
Configures the IP Routing Information Protocol (RIP) for this interface. Must be used in conjunction with the *Listen*, *Send*, or *Metric* parameter.

Listen
Enables or disables RIP listening.

Send
Enables or disables RIP sending.

Metric
Configures the cost or "hop-count" of this interface. Routes learned through this interface will have this value added to their metric. The value to be added must be specified using the *num* parameter.

num
An integer between 1 and 16, inclusive. Commonly used to make a given interface less desirable for backup routing situations.

Trusted
When enabled, this interface will only listen to routing updates from routers specified by the Set / Define IP Trusted command. Otherwise, this interface will listen to all routing updates.

Defaults

Ethernet interface number: 0.

TTLNum: 1.

Default, Proxy-ARP, and Trusted: Disabled.

MTU: 1500 bytes.

Listen and Send: Enabled.

Examples

```
Local>> DEFINE IP ALL MTU 1500

Local>> DEFINE IP ETHERNET MTU 1500

Local>> DEFINE IP ETHERNET POOL 192.0.1.50 192.0.1.59
```

See Also Set / Define IP Trusted, page 13-90; Clear / Purge IP Trusted, page 13-8; Show / Monitor / List Hosts, page 13-149; *IP Address Pools*, page 5-15.

13.38.2 Set/Define IP Create

{ SET / DEFINE } [PROTOCOL] IP CREATE ETHERNET 0 *IPaddress Netmask*

Creates a secondary interface—an interface that shares a physical device, such as an Ethernet port, but has a different IP address. The secondary interface is commonly used to allow more than one IP network on a given Ethernet.

Restrictions You must be the privileged user to use this command.

Parameters

0
The number zero represents the primary Ethernet interface for which the secondary interfaces are created. The number zero must be included in the command.

IPaddress
An IP address in standard numeric format (for example, 193.0.1.50).

Netmask
A subnet mask; for example, 255.255.255.0.

Examples

```
Local>> SET IP CREATE ETHERNET 0 192.73.220.183
255.255.255.0
```

13.38.3 Set/Define IP Domain

{ SET / DEFINE } [PROTOCOL] IP DOMAIN { *DomainName* / NONE }

Sets the default domain suffix. This suffix is appended to host names during IP name resolution.

Restrictions You must be the privileged user to use this command.

Parameters

DomainName
A string of up to 64 characters.

None
Clears an existing domain suffix.

Default None (no domain defined).

Examples

```
Local>> SET IP DOMAIN your.domain.com
```

See Also Set / Define IP Nameserver, page 13-86; Show / Monitor / List IP, page 13-149; *Specifying a Default Domain Name*, page 5-6.

13.38.4 Set/Define IP Ethernet

See Set / Define IP All / Ethernet, page 13-82.

13.38.5 Set/Define IP Host Limit

```
{ SET    } [PROTOCOL] IP HOST [LIMIT]{ num  }
{ DEFINE }                           { NONE }
```

Sets the maximum number of TCP / IP hosts that the LRS will add to its host table as a result of Rwho and DNS lookups. Hosts from the preset host table are exempt from this limit.

Restrictions You must be the privileged user to use this command.

Parameters

num
An integer between 0 and 200.

None
Clears any current host limit.

Default Limit: 200 hosts.

See Also Show / Monitor / List IP, page 13-149; *Adding Hosts to the LRS Host Table*, page 5-6.

13.38.6 Set/Define IP IPaddress

```
{ SET    } [PROTOCOL] IP IPADDRESS address
{ DEFINE }
```

Specifies the server's IP address for TCP / IP connections. The address must be specified using the *address* parameter, described below.

Restrictions You must be the privileged user to use this command.

Errors An error is returned if there are active connections to the LRS. An error is returned if the address is in use by another node.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Show / Monitor / List IP, page 13-149; *Setting the LRS IP Address*, page 5-2.

13.38.7 Set/Define IP Loadhost

```
{ SET    }
{ DEFINE } [PROTOCOL] IP [SECONDARY] LOADHOST address
```

Specifies the IP address of the host used for TFTP loading.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Set / Define Server Loadhost, page 13-129.

13.38.8 Set/Define IP Nameserver

```
{ SET    }
{ DEFINE } [PROTOCOL] IP [SECONDARY] NAMESERVER address
```

Specifies the IP address of the local nameserving host for use on IP connections and NetBIOS connections that use IP. The host's address must be specified using the *address* parameter, described below.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Set / Define IP Domain, page 13-84; Set / Define IP NBNS, page 13-86; *Configuring the Domain Name Service (DNS)*, page 5-6.

13.38.9 Set/Define IP NBNS

```
{ SET    }
{ DEFINE } [PROTOCOL] IP [SECONDARY] NBNS address
```

Specifies the address of the NetBIOS Name Server (NBNS) used for NetBIOS over an IP network. NBNS addresses are passed via PPP to remote users who want to locate the name server dynamically. The LRS does not use this information itself.

NOTE: *NBNS is also known as WINS.*

NetBIOS over IP can also use DNS; the nameserver addresses set with the Set / Define IP Nameserver command will also be passed on to remote node users who ask for them.

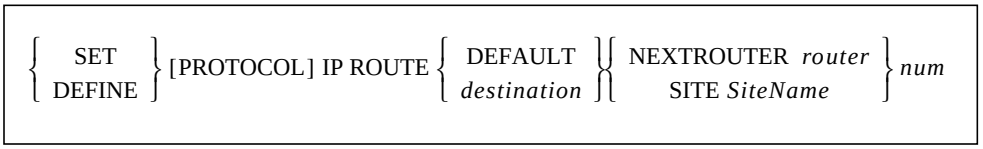
Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Set / Define IP Nameserver, page 13-86; *Configuring the Domain Name Service (DNS)*, page 5-6.

13.38.10 Set/Define IP Route



Configures a static route. Static routes are used to tell the IP router the path toward other IP networks that cannot be learned by a dynamic routing protocol, such as RIP. Static routes commonly point to **sites** (see the Define Site commands, beginning on page 13-31), which represent the best path to the destination. The destination can be an IP network, a subnetwork, or a host.

Restrictions You must be the privileged user to use this command.

Parameters

Default
Configures a default route. If an explicit route to a destination network doesn't exist, the packet will be routed according to the default route.

Static default routes are used when another router is the designated default route. If this router is to advertise itself as the default router, see Set / Define IP All / Ethernet Default on page 13-82.

destination
An IP address in standard numeric form.

Nextrouter
Set the router that packets to the Destination will be sent to.

router
A router name or IP address.

NOTE: *If the route points to a site, use the Site parameter.*

Site
Specifies the site that packets to the Destination will be sent to. When a packet arrives for the destination, a connection will be formed to the specified site, if one does not currently exist.

The site must be defined before a route can be created that points to the site. To configure a site, use the Define Site commands, beginning on page 13-31.

SiteName
A site name of up to 12 characters.

NOTE: *If the next "hop" is a router available on the LAN, use the Nextrouter parameter.*

num
An integer from 1 through 16 representing the metric for this route.

Defaults Metric: 16 (unreachable).

Examples

```
Local>> SET IP ROUTE 198.8.8.0 NEXT 192.0.1.9
```

See Also Clear / Purge IP Route, page 13-7; Set / Define IP Routing; Show / Monitor / List IP Routes, page 13-149; *IP Routing*, page 5-11.

13.38.11 Set/Define IP Routing

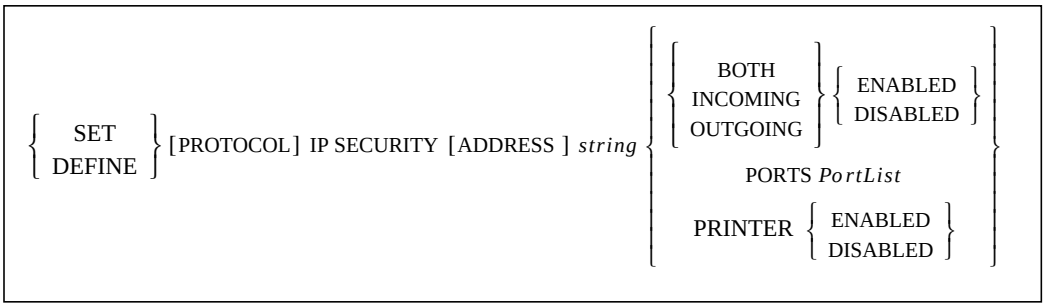
Configures the routing of IP packets. If routing is disabled, any packets requiring routing on the LRS will be rejected. The router will still learn routes via RIP (if enabled) for its own use.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Set / Define IP Route, page 13-87; *IP Routing*, page 5-11.

13.38.12 Set/Define IP Security



This command is used to add or change entries in the IP security table.

Restrictions You must be the privileged user to use this command.

Parameters

address
The IP address to be restricted. The address can be a full IP address, such as 192.0.1.80, to restrict one address; it can also be expressed as a partial address, such as 192.0.1.255, to restrict whole subnetworks.

An address with a 255 in any segment means the restriction applies to all the addresses in that range. Any address with a 0 in any segment implies Incoming and Outgoing Disabled for all ports.

Both
Restricts both logins from the network to the server and Telnet sessions to the network from the server.

Incoming
Restricts logins from the network into the server.

Outgoing
Restricts Telnet sessions to the network from the server.

Ports
A list of ports for which the restriction applies. To specify a port or list of ports, use the *PortList* parameter. If *PortList* is not specified, all physical and virtual ports apply. A port number of 0 is used to apply to the virtual (incoming login) ports.

PortList
A port or series of ports to be logged out. Multiple ports must be specified with a comma; ranges of ports must be specified with a dash (-).

Printer
Enables or disables LPR and RTEL printing from the specified host(s).

Defaults Both Enabled, Printing Enabled.

Examples

```
Local>> SET IP SECURITY ADDRESS 192.0.1.255 INCOMING ENABLED
OUTGOING DISABLED

Local>> SET IP SECURITY 134.0.1.255 Port 3,5-7
```

See Also Clear / Purge IP Security, page 13-7; Show / Monitor / List IP Security, page 13-149; *IP Security*, page 5-10.

13.38.13 Set/Define IP Subnet

{ SET / DEFINE } [PROTOCOL] IP SUBNET [MASK]*address*

Specifies a subnet mask as an IP address. The mask must be specified using the *address* parameter, described below.

Restrictions You must be the privileged user to use this command.

Parameters

Mask
Specifies a subnet mask. Must be used in conjunction with the *address* parameter, discussed below. If a subnet mask isn't specified, a default subnet mask will be inferred from the server's current IP address.

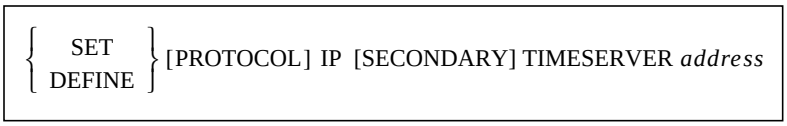
address
An IP address in standard numeric format (for example, 255.255.192.0).

Examples

```
Local>> SET PROTO IP SUBNET MASK 255.255.255.0
```

See Also *IP Addresses*, page 5-1.

13.38.14 Set/Define IP Timeserver



Configures a timeserver for the LRS to use. The LRS has no internal clock. The timeserver's address must be specified using the *address* parameter, described below.

Restrictions You must be the privileged user to use this command.

Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

Secondary
Specifies a backup timeserver.

13.38.15 Set/Define IP Trusted

Configures a list of trusted routers. When Set / Define IP All / Ethernet Trusted is enabled, the LRS will only listen to RIP updates from routers in this list.

Restrictions You must be the privileged user to use this command.

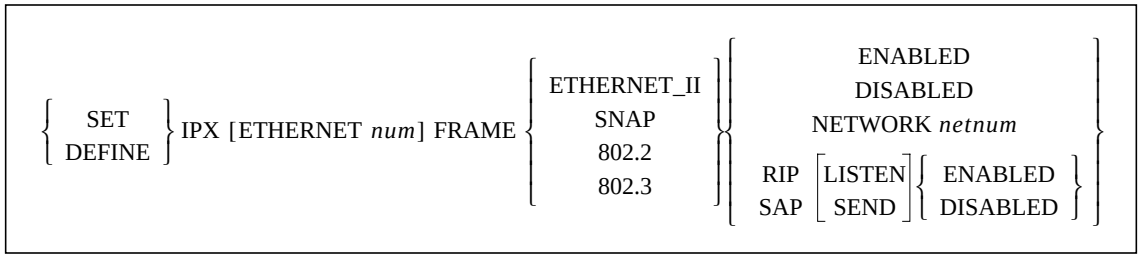
Parameters

address
An IP address in standard numeric format (for example, 193.0.1.50).

See Also Set / Define IP All / Ethernet Trusted, page 13-82; Show / Monitor / List Hosts Trusted, page 13-149; Clear / Purge IP Trusted, page 13-8; *Types of Routes*, page 5-12.

13.39 Set/Define IPX

13.39.1 Set/Define IPX Ethernet Frame



Specifies operations on the Ethernet port.

Restrictions You must be the privileged user to use this command.

Parameters

Ethernet
Configures an Ethernet interface. To specify the number of the Ethernet, use the num parameter. Servers with one Ethernet port do not need the optional Ethernet num parameter; when omitted, it defaults to zero.

num
The number of the Ethernet interface.

Frame
Specifies one of the following encapsulation frame types: Ethernet_II, SNAP, 802.2, or 802.3.

Ethernet_II
Sets the encapsulation frame type to Ethernet_II. Must be used in conjunction with the *Disabled*, *Enabled*, *Network*, *RIP*, or *SAP* parameter.

SNAP
Sets the encapsulation frame type to SNAP. Must be used in conjunction with the *Disabled*, *Enabled*, *Network*, *RIP*, or *SAP* parameter.

802.2
Sets the encapsulation frame type to 802.2. Must be used in conjunction with the *Disabled*, *Enabled*, *Network*, *RIP*, or *SAP* parameter.

802.3
Sets the encapsulation frame type to 802.3. Must be used in conjunction with the *Disabled*, *Enabled*, *Network*, *RIP*, or *SAP* parameter.

Enabled/ Disabled
When used in conjunction with an Ethernet frame type, enables or disables routing on that frame type.

Network
Specifies the IPX network number. Must be used in conjunction with the *num* parameter.

NOTE: *A frame must have a non-zero network number in order to route.*

netnum
A four-byte (8 digit) IPX network number in hexadecimal form. Leading zeroes are assumed; they may be omitted from the command line.

RIP
Configures the Routing Information Protocol (RIP) for the selected frame type. Must be used in conjunction with the *Listen*, *Send*, *Enabled*, or *Disabled* parameter.

SAP
Configures the Service Advertising Protocol (SAP) for the selected frame type. Must be used in conjunction with the *Listen*, *Send*, *Enabled*, or *Disabled* parameter.

Listen
Enables or disables RIP or SAP listening.

Send
Enables or disables RIP or SAP sending.

Enabled/ Disabled
Using “RIP Enabled” or “SAP Enabled” without the Listen or Send parameters will enable both listening and sending. Using “RIP Disabled” or “SAP Disabled” without the Listen or Send parameters will disable both listening and sending.

Defaults Ethernet interface number: 0.

Frame types: all Disabled.

netnum: zero (none defined). There will be no routing until a new netnum is entered.

Listen and Send: Enabled.

Examples

```
Local>> SET IPX ETHERNET FRAME SNAP RIP DISABLED

Local>> SET IPX ETHERNET FRAME ETHERNET_II NETWORK ABCD1234
```

See Also *Routing*, page 6-2.

13.39.2 Set/Define IPX Frame

See Set / Define IPX Ethernet Frame on page 13-90.

13.39.3 Set/Define IPX Netrange

{ SET / DEFINE } [PROTOCOL] IPX NETRANGE *basenumber*

Specifies the base, or first number to assign to connections on serial ports. A port’s IPX network number is the sum of the base and its port number. The netrange includes all numbers from the (base + 1) to the sum of the base and the total number of ports. IPX network numbers in the netrange must be unique on the network.

Restrictions You must be the privileged user to use this command.

Parameters

basenumber
A 4-byte (8-digit) IPX network number in hexadecimal format.

Examples

```
Local>> DEFINE IPX NETRANGE 0x100

Local>> SET IPX NETRANGE 100
```

Default None defined.

See Also *IPX Address Assignment*, page 6-2.

13.39.4 Set/Define IPX Route

{ SET / DEFINE } [PROTOCOL] IPX ROUTE *network* { NEXTROUTER *RouterNet nodeID* / SITE *SiteName* } [*hops* [*ticks*]]

Configures a static IPX route. Static routes are used to tell the IPX router the path toward other IPX networks that cannot be learned by RIP. The route can be specified as a site name, or as an IPX network number in hexadecimal format.

Restrictions You must be the privileged user to use this command.

Parameters

network
A 4-byte (8-digit) IPX network number in hexadecimal format.

Nextrouter
Specifies that there is another router between the LRS and the destination. Must be used with the network and node parameters.

RouterNet
The 4-byte (8-digit) IPX network number of the next router in hexadecimal format.

nodeID
The node id (Ethernet address) of the next router. The format must be *xx-xx-xx-xx-xx-xx*, where each *x* is a hexadecimal digit.

Site
Specifies an existing site through which packets to the network will be sent. Must be used in conjunction with the *SiteName* parameter.

SiteName
Enter a site name of up to 12 characters.

NOTE: *If the next "hop" is a router available on the LAN, use the* ***Nextrouter*** *parameter.*

hops
A number that represents the number of routers between this router and the destination. *hops* must be between 0 and 16; if a value isn't specified, it defaults to 1.

ticks
The time delay it takes to get to the destination network. Units represent 1/18 of a second, and must be between 0 and 255. If a value isn't specified, the tick count will be set to 1.

For routes across sites, PPP adds the site link delay to the tick count value; the specified tick count should be greater than one. The recommended default tick count values are 134 for 2400 bps per second, 21 for 14400 bps per second, 5 for 57600 bps per second, and 1 for 1 Mbps or greater.

NOTE: *The higher the tick count, the less desirable the route.*

Examples

```
Local>> SET IPX ROUTE 1234 NEXTROUT 45af-00-00-ab-12-e2-38.

Local>> SET IPX ROUTE 1234 SITE irvine 2 50
```

See Also Set/Define IP All/Ethernet Frame, page 13-82; Set/Define IPX Routing, page 13-94; *Routing*, page 6-2.

13.39.5 Set/Define IPX Routing

```
{ SET    } [PROTOCOL] IPX ROUTING { ENABLED  }
{ DEFINE }                        { DISABLED }
```

Enables or disables IPX routing. For the LRS to route IPX traffic, this command must be enabled, and at least one frame type must be configured.

Restrictions You must be the privileged user to use this command.

Default Disabled.

See Also Set / Define IP All / Ethernet Frame, page 13-82; Set / Define IPX Route, page 13-93; *Routing*, page 6-2.

13.39.6 Set/Define IPX Service

```
{ SET    } [PROTOCOL] IPX SERVICES ServiceName ServiceType network NodeID socket [hops]
{ DEFINE }
```

Specifies a static IPX service. Static services are used to tell the IPX router information about services that cannot be learned by SAP.

Restrictions You must be the privileged user to use this command.

Parameters

ServiceName
A service name of up to 48 characters.

ServiceType
A hexadecimal value between 0x00000000 and 0xffffffff. Some well-known service types are listed below:

Type	Purpose	Type	Purpose
0000	Unknown	0021	NAS SNA Gateway
0003	Print Queue	0024	Remote Bridge Server
0004	File Server	0027	TCP / IP Gateway
0005	Job Server	002D	Time Synch Server
0007	Print Server	0047	Advertising Print Server
0009	Archive Server	0098	NetWare Access Server
000B	Administration	009E	Portable NetWare
FFFF	Wildcard		

network
A hexadecimal value between 0x00000000 and 0xffffffff.

NodeID
An Ethernet address. The format must be *xx-xx-xx-xx-xx-xx*, where each *x* is a hexadecimal digit.

socket
A hexadecimal value between 0x0000 and 0xffff. Some well-known sockets are listed below:

Socket	Purpose
0451	NetWare Core Protocol (NCP)
0452	Service Advertising Protocol (SAP)
0453	Routing Information Protocol (RIP)
0455	Novell NetBIOS
0456	Diagnostics

hops
A number that represents the number of routers between this router and the destination. *hops* must be between 0 and 16; if a value isn't specified, it will be set to 1.

Examples

```
Local>> DEFINE PROTOCOL IPX SERVICE "comm_server" 4 2c15e830
00-00-00-00-00-01 451 3
```

See Also Set / Define IP All / Ethernet Frame, page 13-82; *Sample LAN to LAN Configuration*, page 6-8.

13.39.7 Set/Define IPX Timeserver

{ SET / DEFINE } [PROTOCOL] IPX TIMESERVER *name*

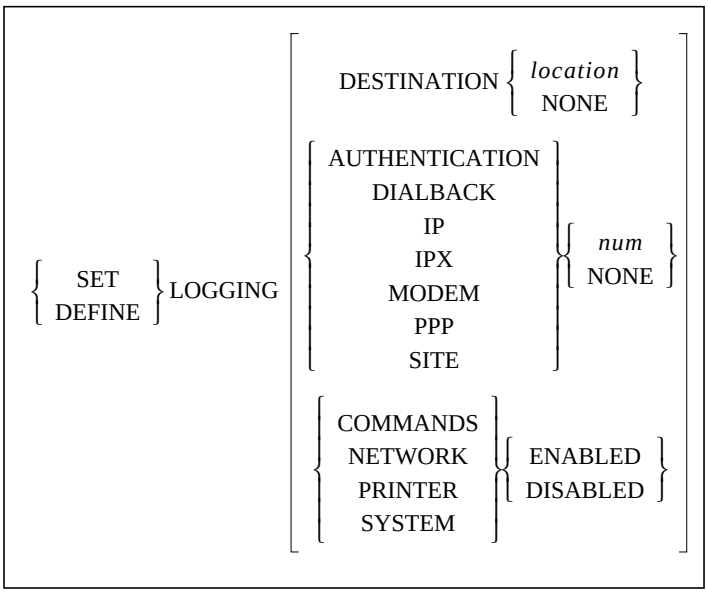
Configures a timeserver for the LRS to use. The LRS has no internal clock. The timeserver must be a NetWare fileserver, specified with the *name* parameter.

Restrictions You must be the privileged user to use this command.

Parameters

name
The name of a NetWare fileserver.

13.40 Set/Define Logging



Controls error and event logging on the LRS. Events can be logged to a network host (via TCP/IP or NetWare) or to a terminal connected to the LRS.

The host must be configured to support logging. If you're using a NetWare host, the LRS name must be added as a print server. If you're using a TCP/IP host, the host's syslog facility must be configured; make sure all priorities equal to or higher than ***.notice** are being logged. The syslog file is typically located in the **/etc** directory; see your host's documentation on syslogd for more information.

NOTE: *Logging levels are cumulative; setting logging to level 4 includes levels 1 through 3 as well. See Chapter 12, Security, for a detailed description of the events that can be logged.*

Restrictions You must be the privileged user to use this command.

Parameters

Destination
Specifies a destination for the logging messages. Must be used in conjunction with the address parameter or the None parameter.

location
A fileserver name, NetWare address, or IP address. This parameter may be specified as one of the following:

String/ Form	Action
hostname:	Specifies a TCP/IP host
hostname \	Specifies an IPX host
CONSOLE	Sends events to the LRS console port
Memory	Saves events in LRS memory

None
Disables logging.

Authentication
Logs events associated with authentication. Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	System Problems
2	Failures and Successes
3	All Logins and Logouts
4	Incorrect Passwords
5	All Passwords, RADIUS Warnings

Dialback
Logs events associated with dialback functionality. Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	Dialback Problems
2	Unauthorized Users
3	Dialback Failures
4	Dialback Successes
5	Dialback Attempts
6	Modem Chat

IP
Traces the activities of the IP router. Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	Errors
2	Packets triggering remote connections
3	Routing table / interface changes
4	Incoming / outgoing RIP packets
5	Resulting routing table (verbose)
6	Contents of all RIP packets (verbose)
7	Routed packets (verbose)

NOTE: *Setting the IP logging level to 2 or greater results in a syslog that prints the source/ destination IP address, protocol, and TCP/UDP source/destination ports.*

IPX
Traces the activities of the IPX router. Must be used with the *num* parameter or the *None* parameter.

Level	Information
2	Critical Conditions
3	Error Conditions
4	Warnings
5	Normal but Significant Conditions
6	Informational Messages
7	Debug-level Messages

NOTE: *At this time, IPX Logging level 1 is inoperative.*

Modem
Logs modem activity, including modem jobs (incoming and outgoing). Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	Problems
2	Call Statistics Dump From Modem
3	Setup

PPP
Logs events associated with PPP. Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	Local System Problems
2	Remote System Problems
3	Negotiation Failures
4	Negotiation Data
5	State Transitions
6	Full Debugging

Site
Logs events associated with sites. Must be used with the *num* parameter or the *None* parameter.

Level	Information
1	Errors
2	State Transitions
3	Chat Scripts
4	Modem Dialing
5	Port Connections
6	Connection Failures
7	Usage Summary

num
An integer that specifies a particular level of logging.

Commands
When enabled, logs all commands users type.

Network
When enabled, logs network events. This is useful for diagnosing network-related problems.

Printer
When enabled, logs printer related events including online / offline conditions and job status at the end of job.

System
When enabled, logs server boots, log file open / closes, and other system related activity.

Defaults

Destination: None.

Logging Options: None / Disabled (logging turned off).

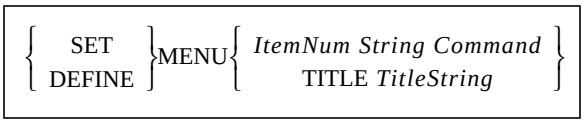
Examples

```
Local>> SET LOGGING AUTHENTICATION 5
```

See Also

Show / Monitor / List Logging, page 13-152; *Event Logging*, page 12-25.

13.41 Set/Define Menu



Configures individual Menu Mode menu choices and the menu's title banner.

NOTE: *It is recommended to add a menu entry that allows users to log out. This can be accomplished by adding a "Logout Port" command to the end of the menu.*

Restrictions You must be the privileged user to use this command.

Parameters

ItemNum
A number (1 through 36) and corresponds to the menu entry you are changing.

String
A text string, up to 32 characters long, that is displayed to users in the menu screen.

Command
A string of text, up to 32 characters long, that is the actual command executed when the user selects this entry.

TitleString
An optional title for the entire menu, up to 48 characters long.

Examples

```
Local>> SET MENU 5 "SHOW NET NODES" "SHOW HOSTS"
```

See Also Show / Monitor / List Menu, page 13-152; Clear / Purge Menu, page 13-10; *Menu Mode*, page 9-18; *Menu Mode*, page 12-20.

13.42 Set/Define NetWare

13.42.1 Set/Define NetWare Access

Configures a list of fileservers the LRS will contact for print jobs. By default, only fileservers on the local network will be queried; this command can be used to query additional fileservers, or only the specified fileserver(s).

Restrictions You must be the privileged user to use this command.

Parameters

All
All fileservers, including those on other networks, will be contacted.

Local
Only fileservers on the local network will be queried.

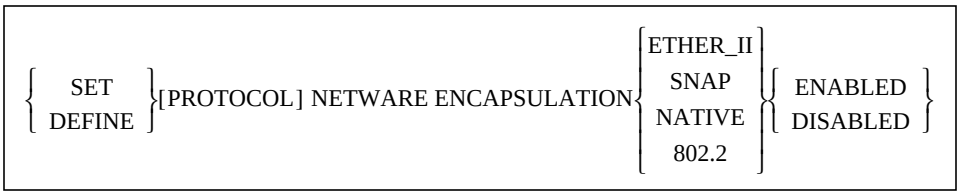
fileserver
An individual fileserver name of up to 8 characters.

Default Local.

Examples
```
Local>> DEFINE NETWARE ACCESS lab_fs4
```

See Also Clear / Purge Protocols NetWare Access, page 13-10; Set / Define Server Software, page 13-135; Show / Monitor / List NetWare, page 13-153.

13.42.2 Set/Define NetWare Encapsulation



Configures the frame types that the LRS will support (accept traffic from and generate traffic for). When routing is enabled with the Set / Define NetWare Routing command on page 13-103, this command will be ignored, as all frame types are accepted in router mode.

Multiple frame types can be enabled at once. This may cause error messages from some NetWare fileservers due to the same network number being on different frame types. To correct this problem, enable NetWare routing.

Restrictions You must be the privileged user to use this command.

Parameters

ETHER_II
Use the Ethernet v2 frame format.

NATIVE
Use the “native mode” NetWare frame format.

SNAP
Use the 802.2 frame type with SNAP SAP.

802.2
Use the 802.2 frame type with NetWare SAP.

Defaults All Enabled.

Examples
```
Local>> DEFINE NETWARE ENCAPSULATION ETHER_II DISABLED
```

See Also Show / Monitor / List NetWare, page 13-153; Set / Define NetWare Routing, page 13-103; *Ethernet Interface*, page 6-6.

13.42.3 Set/Define NetWare Internal

Set NetWare Internal is not a valid command. See Define NetWare Internal on page 13-13.

13.42.4 Set/Define NetWare Loadhost

Specifies the name of the fileserver to download from when the LRS boots.

NOTE: *This command is only useful when configured with the Define command, or with both the Set and Save commands; if it is configured with the Set command alone, it will be cleared at boot time.*

Restrictions You must be the privileged user to use this command.

Parameters **fileserver**
A fileserver name of up to 31 characters.

Examples
```
Local>> DEFINE NETWARE LOADHOST lab_fs4
```

See Also Set / Define Server Software, page 13-135; *Editing Boot Parameters*, page 2-7.

13.42.5 Set/Define NetWare Printserver

Configures the fileserver that the LRS will be dedicated to for Rprinter operation.

Restrictions You must be the privileged user to use this command.

Parameters **fileserver**
A fileserver name of up to 31 characters.

Examples
```
Local>> DEFINE NETWARE PRINTSERVER lab_fs4
```

13.42.6 Set/Define NetWare Reset

Instructs the Print Server module to immediately go to the network and rescan for new connections. This is typically necessary when setting up queues or print servers using PCONSOLE.

Restrictions You must be the privileged user to use this command.

13.42.7 Set/Define NetWare Routing

Configures whether the LRS will act as an internal router if there are multiple NetWare frame types on the LAN. If enabled, the LRS will advertise all its NetWare services as part of an internal network, and will advertise itself as a "router" to that network. If disabled, the LRS will use the setting of Set NetWare Encapsulation to determine which frame types to accept.

Restrictions You must be the privileged user to use this command.

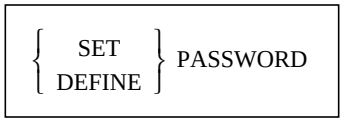
Default Enabled.

See Also Set / Define NetWare Encapsulation, page 13-101; Show / Monitor / List NetWare, page 13-153; *IPX Networks*, page 6-1; *Ethernet Interface*, page 6-6.

13.43 Set Noprivileged

See Set Privileged / Noprivileged, page 13-124.

13.44 Set/Define Password



Changes the current user's password in the local authentication database, provided the user is defined in the local authentication database and is permitted to alter the password. When this command is entered, the user will be prompted for the old password, then prompted to enter and verify a new password.

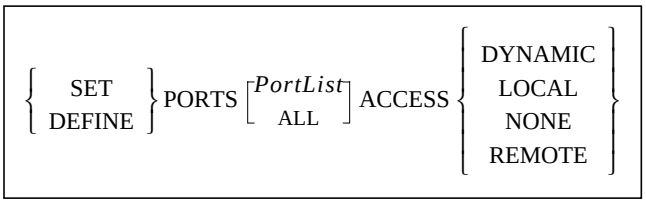
NOTE: *The user has three chances to enter the old password before he or she is logged out of the LRS.*

Restrictions This command **does not** require privileged user status. To prevent users from altering their own passwords, enter the **Set/Define Authentication User Alter Disabled** command.

See Also Set / Define Authentication User, page 13-72; Clear / Purge Authentication, page 13-5; Show / Monitor / List Authentication, page 13-148.

13.45 Set/Define Ports

13.45.1 Set/Define Ports Access



Sets the type of incoming connections allowed through the physical port.

Restrictions You must be the privileged user to use this command.

Errors If a port is active, its access cannot be set.

Autobaud must be disabled for Remote and Dynamic ports.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Dynamic
The ports can receive connection requests from local and remote users.

Local
The ports can only accept connection requests from local users (those connected to the serial ports). No remote logins are permitted.

None
The specified ports are unusable.

Remote
The specified ports accept only network connection requests. No local logins are permitted.

Default Dynamic (LRS versions 1.2 and later).

Examples

```
Local>> DEFINE PORTS ALL ACCESS LOCAL
```

See Also *Accessing a Port*, page 9-1; *Port Access*, page 12-22.

13.45.2 Set/Define Ports Authenticate

When enabled, prompts incoming user for a username and password to be checked against the authentication database(s) set up with the **Set/Define Authentication** commands.

Restrictions You must be the privileged user to use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16.Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also Clear / Purge Authentication, page 13-5; Set / Define Authentication, page 13-62; Show / Monitor / List Authentication, page 13-148; *Port Doesn't Automatically Run PPP or SLIP*, page 3-12; *Port Restrictions*, page 9-9.

13.45.3 Set/Define Ports Autobaud

Enables a port to detect the incoming baud rate and change its own to match at login time. Autobaud must be disabled for Remote and Dynamic port access and for any port offering a service.

NOTE: *When Autobaud is enabled, you may have to press Return twice or more to allow the port to determine the baud rate.*

Restrictions You must be the privileged user to use this command.

Errors Autobaud and Autostart cannot be used together. If you try to configure both options, you will get a message saying that the previously configured option was disabled.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

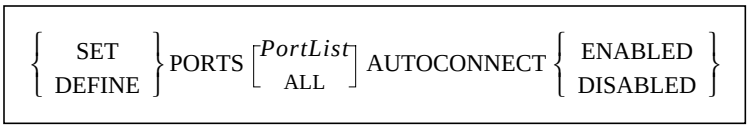
Autobaud works for most baud rates when both ends of the line are the same parity, or when the port is set to 8 bits with no parity and the incoming connection is 7 bits with even parity. Baud rates must be within 3 "steps" of each other; 9600 to 38400 will work, but 9600 to 115200 will not.

Default Disabled.

Examples
```
Local>> DEFINE PORTS AUTOBAUD DISABLED
```

See Also Set / Define Ports Character Size, page 13-109; Set / Define Ports Parity, page 13-115; Set / Define Ports Speed, page 13-120; *Configure Modems*, page 3-15; *Modem Speeds*, page 10-1.

13.45.4 Set/Define Ports Autoconnect



If enabled, the port connects automatically to the preferred service upon login. To exit to character (Local>) mode, the Break command can be used. To attach to other services, the Connect command can be used.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

Examples
```
Local>> SET PORTS AUTOCONNECT ENABLED
```

See Also Set / Define Ports Preferred, page 13-117.

13.45.5 Set/Define Ports Autostart

If enabled, the specified port will not wait for character input before starting.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Errors Autobaud and Autostart cannot be used together. If you try to configure both options, you will get a message saying that the previously configured option was disabled.

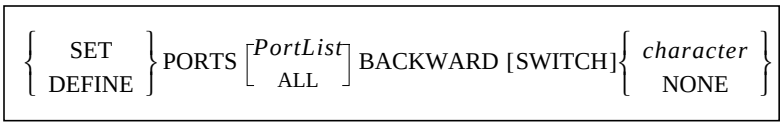
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also *Automatic Start-up*, page 9-2.

13.45.6 Set/Define Ports Backward Switch



Defines a “backward” key. From character (Local>) mode, typing this key functions as if the Backward command was entered; the user may switch to the previous session without entering character mode.

Any key can be specified as a backward key, unless it conflicts with previously-configured break or switch keys. Keys that will be used by a remote operating system or application you will be using, should also be avoided, as the LRS will interpret that key and the remote service will not see it. Line editing characters should also be avoided; these will be interpreted by the LRS.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the *character* parameter.

character
The character to be used as the backward switch. To specify a control character, hold down the control key while typing the letter, or type a caret (^) and the letter.

None
Clears the current switch character.

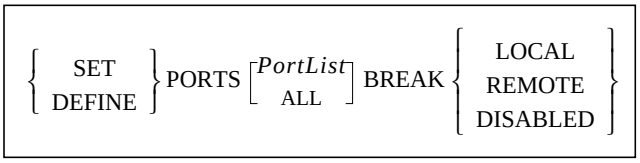
Default None configured.

Examples

```
Local> SET PORT 2 BACKWARD SWITCH ^K
```

See Also Backwards, page 13-3; Set / Define Ports Forward Switch, page 13-112; Set / Define Ports Local Switch, page 13-113; *Switching Between Sessions*, page 9-5.

13.45.7 Set/Define Ports Break



Determines where processing of the Break key will take place.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Local
Pressing the Break key will return to character (Local>) mode.

Remote
The Break key is ignored by the LRS and passed through to the remote service.

Disabled
Pressing the Break key does nothing.

Default Local.

See Also Set / Define Ports Backward Switch, page 13-107; Set / Define Ports Forward Switch, page 13-112; Set / Define Ports Local Switch, page 13-113; *Exiting Sessions*, page 9-5.

13.45.8 Set/Define Ports Broadcast

Enables or disables other users' broadcasts to this port. Broadcasts are typically disabled when extra messages are not desired on the port's output device.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Enabled.

Examples
```
Local>> SET PORTS BROADCAST DISABLED
```

See Also Broadcast, page 13-3; Set / Define Server Broadcast, page 13-125.

13.45.9 Set/Define Ports Character Size

Sets the number of bits per character for the serial port.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Errors Autobaud only works for 8 bits, or for 7 bits with even parity.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Size
Character size must be either 7 or 8 bits.

Default 8 bits.

Examples
```
Local>> SET PORTS CHARACTER SIZE 7
```

See Also Set / Define Ports Autobaud, page 13-105; Set / Define Ports Parity, page 13-115; Chapter 10, *Modems*.

13.45.10 Set/Define Ports Command Completion

Enables or disables the command completion feature. If enabled, the LRS will attempt to complete partially typed command words when the user presses the Space or Tab keys.

Restrictions You must be the privileged user to use this command on ports other than your own.

Errors If the partially-entered command is ambiguous (or if the user is typing an optional string), the LRS sends a beep to the terminal.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

Examples
```
Local>> SET PORTS COMMAND ENABLED
```

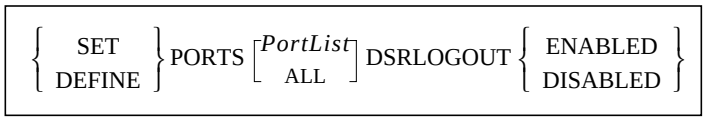
13.45.11 Set Ports Dedicated

Set Ports Dedicated is not a valid command. See Define Ports Dedicated on page 13-14.

13.45.12 Set Ports Dialback

Set Ports Dialback is not a valid command. See Define Ports Dialback on page 13-15.

13.45.13 Set/Define Ports Dsrlogout



When enabled, the port will be logged out when the port's DSR signal is dropped. This usually only occurs when the attached terminal device is powered off or disconnected; it is intended to keep users from switching terminal lines to access other sessions. Any open connections will be closed before logging out.

Restrictions You must be the privileged user to use this command.

Errors Modem Control and Dsrlogout are mutually exclusive.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also *DSR Logouts*, page 9-11; *Serial Signals*, page 9-14.

13.45.14 Set/Define Ports Dtrwait

If enabled, the LRS will not assert the DTR signal on the serial port until a user logs into the port, connects to the port via a service, or connects to the port via a Telnet connect. When the port is idle, DTR will not be asserted.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also Define Ports Modem Control, page 13-20; Set / Define Ports Flow Control, page 13-111; *DTR (Data Terminal Ready)*, page 9-16.

13.45.15 Set/Define Ports Flow Control

Sets the type of flow control on the port.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

None
No flow control will be performed.

CTS
Sets the flow control type to CTS / RTS.

XON
Sets the flow control type to XON / XOFF.

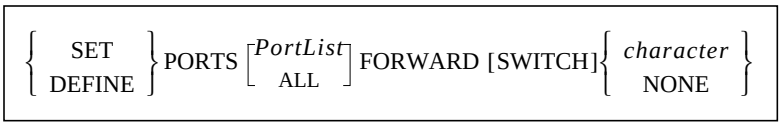
Default XON.

Examples

```
Local>> SET PORTS FLOW CONTROL CTS
```

See Also Set / Define Ports Dtrwait, page 13-111; *Flow Control*, page 9-12.

13.45.16 Set/Define Ports Forward Switch



Defines a “forward” key. Typing this key from Local mode functions as if the Forward command were entered; the user may switch to the next session without entering character mode.

Any key can be specified as a forward key, unless it conflicts with previously-configured break or switch keys. Keys that will be used by a remote operating system or application you will be using, should also be avoided, as the LRS will interpret that key and the remote service will not see it. Line editing characters should also be avoided; these will be interpreted by the LRS.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the *character* parameter.

character
To specify a control character, hold down the control key while typing the letter, or type a caret (^) and the letter.

None
Clears the current switch character; no switch will be used.

Default None configured.

Examples

```
Local>> SET PORTS ALL FORWARD SWITCH ^X
```

See Also Forwards, page 13-49; Set / Define Ports Backward Switch, page 13-107; Set / Define Ports Local Switch, page 13-113; Set / Define Ports Autostart, page 13-106; *Switching Between Sessions*, page 9-5.

13.45.17 Set/Define Ports Inactivity Logout

Enables automatic logout of the port if it has been “inactive” for a set period of time. Inactive is defined as having no keyboard or network activity on the port. The port’s open connections (if any) will be closed before logging out.

NOTE: *The inactive period is configured using the Set/Define Server Inactivity command.*

This command is ignored for remote networking connections. See the Define Site Idle command on page 13-38.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also Define Site Idle, page 13-38; Set / Define Server Inactivity, page 13-127.

13.45.18 Set/Define Ports Local Switch

Defines a “local switch” key. From a remote connection, typing this key functions as if the Break command was entered; the port will be switched from a remote connection to character (Local>) mode. This is especially useful for connections to the LRS, where a local break key may not be passed to the LRS.

Any key can be specified as a local switch key, unless it conflicts with previously-configured break or switch keys. Keys that will be used by a remote operating system or application you will be using, should also be avoided, as the LRS will interpret the key and the remote service will not see it. Line editing characters should also be avoided; these will be interpreted by the LRS.

The local switch key will be ignored if a session is configured as Passall or Passthru.

Restrictions You must be the privileged user to configure a local switch on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Switch
Defines the control character. Must be used in conjunction with the *character* parameter.

character
The character to be used as the local switch. To specify a control character, hold down the control key while typing the letter, or type a caret (^) and the letter.

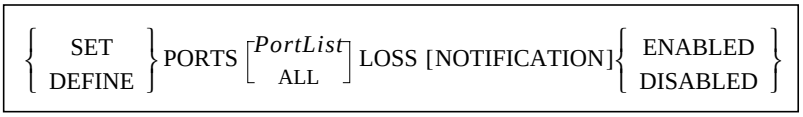
None
No switch is used.

Examples

```
Local>> SET PORTS ALL LOCAL SWITCH ^V
```

See Also Set / Define Ports Break**,** page 13-108; Set / Define Ports Backward Switch, page 13-107; Set / Define Ports Forward Switch, page 13-112; Set Session, page 13-144; *Sessions*, page 9-4.

13.45.19 Set/Define Ports Loss Notification



Sends the terminal device a Ctrl-G (Bell) when a typed character is lost due to a data error or an overrun on the LRS.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Enabled.

See Also *Notification of Character Loss*, page 9-19.

13.45.20 Set/Define Ports Menu

Specifies whether or not the port will be placed in menu mode at login. If Set / Define Ports Menu is disabled, the Local prompt will appear at login. If it is enabled, a menu screen will be displayed; the Local prompt is not accessible.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16.Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also Clear / Purge Menu, page 13-10; Set / Define Menu, page 13-100; Show / Monitor / List Menu, page 13-152; *Menu Mode*, page 9-18; *Menu Mode*, page 12-20.

13.45.21 Set Ports Modem

Set Ports Modem is not a valid command; modem control must be configured with the Define Ports Modem Control commands beginning on page 13-20.

13.45.22 Set/Define Ports Name

Sets a unique name for each port, or a common name for a group of ports. Giving the same name to several ports may be desirable, for example, when you want to label them as modem connection ports or dedicated SLIP / PPP ports.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

portname
A name of up to 16 characters composed of alphanumerics or the underscore (“_”) character. If the name is not enclosed in quotation marks, it will be converted to uppercase.

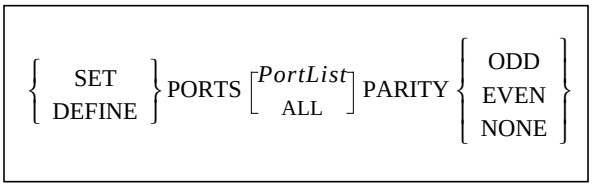
NOTE: *The default portname is Port_n, where n is the port number.*

Examples

```
Local>> SET PORT 2 NAME “highspeed_modem”
```

See Also *Naming a Port*, page 9-18.

13.45.23 Set/Define Ports Parity



Sets the serial port’s parity to Odd, Even, or None (no parity). Note that changing the parity may affect the configured character size.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Errors Autobaud will not work unless the port is using 8 bit characters, or 7 bit characters with Even parity.

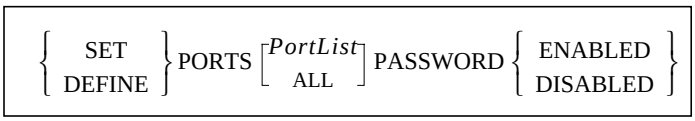
Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default None (no parity).

See Also Set / Define Ports Autobaud, page 13-105; Set / Define Ports Character Size, page 13-109; *Serial Configuration*, page 9-12.

13.45.24 Set/Define Ports Password



Controls whether or not a password is required to log in to the server from this port. The Set Server Login Password command is used to set the password.

Restrictions You must be the privileged user to use this command.

Errors The virtual port (port 0) password must be enabled or disabled with the Define command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

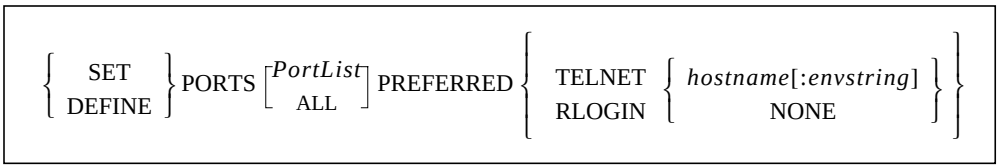
Default Disabled.

See Also Set / Define Server Login Password, page 13-129; *Login Password*, page 9-10.

13.45.25 Set Ports PPP

Set Ports PPP is not a valid command. See Define Ports PPP on page 13-28.

13.45.26 Set/Define Ports Preferred



Specifies a default service for this port. The LRS will attempt to use the preferred service for Auto-connecting, as well as when no service name is specified in a Connect, Telnet, or Rlogin command.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Telnet
Specifies that the service is a default Telnet connection. If there is no local nameserver defined, the host must be specified with a numeric hostname. Must be used in conjunction with the *hostname* parameter.

Rlogin
A synonym for Telnet hostname. Ports set up to use Rlogin will still use Telnet for the connection. Must be used in conjunction with the *hostname* parameter.

hostname
Telnet host name of 40 characters or less, or an IP address in standard numeric format (for example, 192.0.1.3).

envstring
Sets up the connection environment before the session is started. The string is constructed with a sequence of key letters, some of which are prefaced by either “+” or “-.” The key letters are:

D	+D = Backspace mode	-D = Delete mode
E	+E = Local Echo mode	-E = Remote Echo mode
I	I = Interactive mode	
P	+P = Passall mode	-P = Passthru mode
C	+C = CR = CRLF,	-C = CR = LF
T	TCP mode (i.e. uninterpreted data stream)	
R	Rlogin protocol (sets port # to 513 if not already set)	
Q	Queued (i.e. RTEL) connection	
nnn	Optional port number	

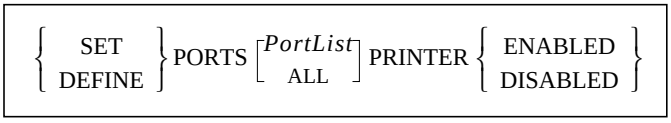
Default None.

Examples

```
Local>> SET PORT 2 PREFERRED TELNET 192.0.1.3

Local>> SET PORT 3 PREFERRED TELNET todd
```

See Also Connect, page 13-12; Rlogin, page 13-56; Set / Define Ports Autoconnect, page 13-106; Define Ports Dedicated, page 13-14; *Setting Session Characteristics*, page 9-6.

13.45.27 Set/Define Ports Printer



If enabled, the server will check to see if the port is online before sending data to it.

Restrictions You must be the privileged user to use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

13.45.28 Set/Define Ports Security

Setting a port to Secure status restricts its access to LRS commands and the ability to get information about other ports using Show / List commands. Privileged commands are not available to secure users. Certain other commands cannot be entered for a port other than the secure user's own port.

Restrictions You must be the privileged user to use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also *Preferred/Dedicated Telnet Hosts*, page 9-9; Chapter 12, *Security*.

13.45.29 Set/Define Ports Session Limit

Limits the number of active sessions on a port. The maximum number of sessions configured for a port cannot exceed the server session limit.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

limit
An integer between 0 and 8.

None
Allows the maximum number of sessions.

Default Limit: 4 sessions.

See Also Set / Define Server Session Limit, page 13-134; *Sessions*, page 9-4.

13.45.30 Set/Define Ports Signal Check

Determines whether or not the DSR signal will be checked for when remote connections to the port are made. If enabled, remote connections to the port will not be permitted unless the DSR signal is asserted.

Restrictions You must be the privileged user to use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

See Also *DSR for Controlling Remote Logins*, page 9-15.

13.45.31 Set Ports SLIP

Set Ports SLIP is not a valid command. See Define Ports SLIP on page 13-31.

13.45.32 Set/Define Ports SLIPdetect

Automatically detects and starts running SLIP. Automatically running SLIP is a potential security hazard.

Restrictions You must be the privileged user to use this command.

Parameters

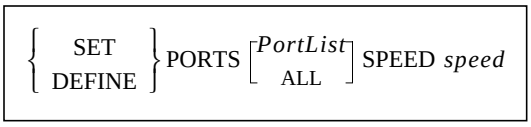
PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Defaults Disabled.

See Also *Starting PPP or SLIP Using Automatic Protocol Detection*, page 3-9.

13.45.33 Set/Define Ports Speed



Specifies the baud rate of the port.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Errors An error is displayed for illegal baud rates.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

speed
One of the following baud rates: 300, 600, 1200, 2400 4800, 9600, 19200, 38400, 57600, 115200.

Default 9600 baud.

Examples
```
Local>> SET PORTS SPEED 2400
```

See Also Set / Define Ports Autobaud, page 13-105; *Modem Speeds*, page 10-1.

13.45.34 Set/Define Ports Stop

Specifies the stop bit count for the port. The default is to use one stop bit.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Errors An error is displayed if an invalid stop bit number is entered.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default 1 stop bit.

13.45.35 Set/Define Ports Telnet Pad

If Telnet Pad is enabled (the default), the server automatically pads carriage returns with null characters for Telnet sessions.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Enabled.

See Also *Padding Return Characters*, page 9-19.

13.45.36 Set/Define Ports TermType

Used to specify a terminal type for the port. The terminal type is reported to the destination node in Telnet and Rlogin sessions. Example terminal types might be VT100 or IBM1000.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

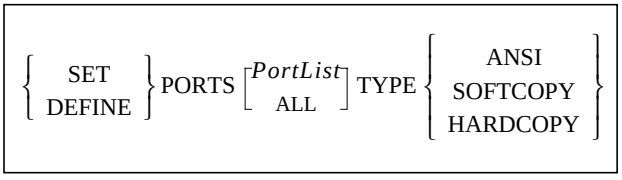
TermString
Enter a string of up to 8 characters in length.

None
Clears the field. There is no terminal type configured by default.

Default None defined.

See Also *Specifying a Terminal Type*, page 9-19.

13.45.37 Set/Define Ports Type



Describes the type of device connected to the port.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

ANSI
VT100 compatible devices.

Softcopy
VT100 without clear screen or cursor controls.

Hardcopy
Deleted characters are echoed between backslashes; there is no cursor movement.

Default Softcopy.

See Also *Setting the Device Type*, page 9-19.

13.45.38 Set/Define Ports Username

Used to specify a username for the port. When the username is defined, you will not be asked for one when logging in to the port.

Restrictions You must be the privileged user to use this command on ports other than your own. Secure users may not use this command.

Parameters

PortList/All
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

username
A name of up to 16 characters in length, converted to all uppercase unless enclosed in quotes.

None
Clears a current username.

Default None.

See Also *Specifying a Username*, page 9-18.

13.45.39 Set/Define Ports Verification

If enabled, the server will issue informational messages whenever a session is connected, disconnected, or switched.

Restrictions You must be the privileged user to use this command on ports other than your own.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Enabled.

See Also *Sessions,* page 9-4.

13.46 Set PPP

Starts PPP on this port using the specified site's configuration.

Parameters **IPaddress**
Defines the non-negotiable remote IP address.

address
An IP address in standard numeric format (for example, 193.0.1.50).

SiteName
A name of 12 characters or less. If no site name is given, a site with the default site characteristics will be used.

Examples

```
Local> SET PPP irvine

Local> SET PPP allison IPADDRESS 191.1.1.1
```

See Also Define Ports PPP, page 13-28; Chapter 8, *PPP*.

13.47 Set Privileged/Noprivileged

Changes the current port's privilege status. Only one port on the server can be privileged at any time. The Override parameter is provided to force your current port to become the privileged port (and the previously privileged port loses the privilege).

When changing your port to privileged status, you will be queried for the privileged password. The factory default privileged password is **system**; this password can be changed with the Set Server Privileged Password command. If the password is forgotten, the server can be reset to factory defaults.

Restrictions

To use Privileged, the user must know the privileged password. Secure users cannot become privileged.

Examples

```
Local> SET NOPRIVILEGED
```

```
Local> SET PRIVILEGED OVERRIDE
Password> ETHERN (not displayed when typed)
```

See Also Set / Define Ports Security, page 13-118; *Privileged Password*, page 2-8.

13.48 Set/Define Protocols

See the Set / Define AppleTalk commands, beginning on page 13-59; Set / Define IP commands, beginning on page 13-82; Set / Define IPX commands, beginning on page 13-90; and Set / Define NetWare commands, beginning on page 13-100.

13.49 Set/Define Server

13.49.1 Set/Define Server BOOTP

Enables or disables querying for a BOOTP host at system boot time.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also LRS **Installation Guide**.

13.49.2 Set/Define Server Broadcast

Enables or disables broadcasts from the server's ports.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Broadcast, page 13-3.

13.49.3 Set/Define Server Buffering

Specifies the size of buffer (in bytes) to use for TCP/IP connections. The size can be increased for large data transfers (file transfers, for example).

Restrictions You must be the privileged user to use this command.

Parameters **buffersize**
Specify the buffer size in bytes between 128 and 8192.

Default 4096 bytes for LRS2 and LRS16, 1024 bytes for LRS1.

Examples
```
Local>> SET SERVER BUFFERING 1024
```

13.49.4 Set/Define Server Clock

Manually sets the date and time information on the server clock.

NOTE: *This command is not available on an LRS1.*

Restrictions You must be the privileged user to use this command.

Parameters **time**
Enter the time in 24-hour **hh:mm:ss** format. Entering seconds is optional.

date
Enter the date in **mm/dd/yyyy** format.

Examples
```
Local>> SET SERVER CLOCK 13:23 03/15/1995
```

See Also Set/Define IP Timeserver, page 13-90; Set/Define IPX Timeserver, page 13-95; Show/Monitor/List Server Clock, page 13-159; Show/Monitor/List Server Timezone, page 13-159; *Setting the Date and Time*, page 2-5.

13.49.5 Set/Define Server Domain

See Set/Define IP Domain, page 13-84.

13.49.6 Set/Define Server Host Limit

```
{ SET    }SERVER HOST[LIMIT]{ limit }
{ DEFINE }                  { NONE  }
```

Sets the maximum number of TCP/IP hosts learned via Rwho that the server will keep information for. Hosts from the preset host table are exempt from this limit. If the new limit is less than the current limit and the host table is full, the limit will be slowly weeded down to the new value.

Restrictions You must be the privileged user to use this command.

Parameters

limit
A value between 0 and 200.

None
No limit is set.

Default 200 hosts.

Examples

```
Local>> SET SERVER HOST LIMIT 6
```

13.49.7 Set/Define Server Inactivity

```
{ SET    }SERVER INACTIVITY[TIMER]limit
{ DEFINE }
```

Sets the period of time after which a port with Inactivity Logout enabled is considered inactive and is automatically logged out.

Restrictions You must be the privileged user to use this command.

Parameters

limit
Enter an inactivity period of 1 to 120 minutes.

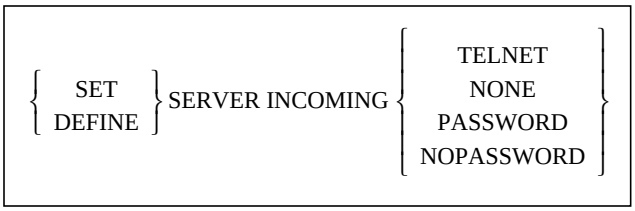
Default 30 minutes.

Examples

```
Local>> DEFINE SERVER INACTIVITY LIMIT 20
```

See Also Set/Define Ports Inactivity Logout, page 13-112.

13.49.8 Set/Define Server Incoming



Allows or denies incoming Telnet connections and enforces password protection if desired. The Show Server command shows the status of incoming connection parameters.

The status of the Incoming Telnet also controls incoming Rlogin sessions from remote hosts— the Set / Define Server Rlogin command controls outgoing Rlogin connections.

Restrictions You must be the privileged user to use this command.

Parameters

Telnet
Enables incoming Telnet connects (logins) to the server.

None
Prevents all login attempts.

Password
Requires incoming Telnet login attempts to supply the server login password before being logged in.

NoPassword
Incoming Telnet logins are permitted and are not prompted for the login password before connecting.

Defaults Telnet, Nopassword.

NOTE: *The default incoming password is "access." See the Set/Define Server Login Password command for more information.*

Examples

```
Local>> SET SERVER INCOMING TELNET INCOMING PASSWORD
```
(sets up password protected Telnet logins)

See Also Set / Define Server Rlogin, page 13-134; Set / Define Server Login Password, page 13-129; *Login Password*, page 9-10.

13.49.9 Set/Define Server IPaddress

See Set / Define IP IPaddress, page 13-85.

13.49.10 Set/Define Server Loadhost

Specifies the host to be used for downloads from TCP/IP hosts. The host name must be a numeric IP-style address (that is, it can't be nameserved). The LRS requests its run-time code from this host.

Restrictions You must be the privileged user to use this command.

Parameters **IPaddress**
An IP address in standard numeric format (for example, 193.0.1.50).

Examples
```
Local>> DEFINE SERVER LOADHOST 193.23.71.49
```

See Also LRS **Installation Guide**.

13.49.11 Set/Define Server Lock

Controls whether or not local users are permitted to Lock their ports.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also *Locking a Port*, page 9-9.

13.49.12 Set/Define Server Login Password

Specifies the password that is used to log in to the server from the serial ports or the network. If the password is not given on the command line, the user will be prompted for it and it will not be displayed when typed. Users will only be required to provide this password if their ports also have Password Enabled.

Restrictions You must be the privileged user to use this command.

Parameters **passwd**
Enter a password of 6 or fewer characters.

NOTE: *LRS passwords are case-independent, even when enclosed in quotes.*

Default "access".

Examples

```
Local>> SET SERVER LOGIN PASSWORD
Password> platyp (password will not be displayed)
Verification> platyp
Local>>
```

See Also Set / Define Server Incoming Password, page 13-128; *Login Password*, page 9-10.

13.49.13 Set/Define Server Name

Specifies the name of the LRS. The name string must be in quotes if lowercase characters are used.

Restrictions You must be the privileged user to use this command.

Parameters **ServerName**
16 characters or less, alphanumeric only.

Default LRS_*xxxxxx* where *xxxxxx* represents the last 3 segments of the unit's hardware address.

Examples

```
Local>> SET SERVER NAME "docserver"
```

See Also *Changing the LRS Server Name*, page 2-4.

13.49.14 Set/Define Server Nameserver

Specifies the IP address of the name server (if any) for TCP / IP connections. This host will attempt to resolve text Telnet hostnames into numeric form if the local host table cannot do so.

Restrictions You must be the privileged user to use this command.

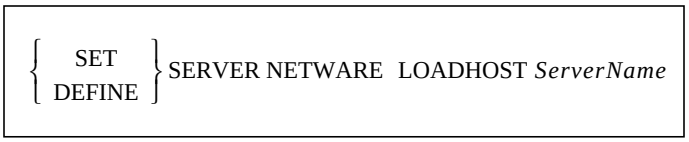
Parameters **IPaddress**
The network address of the nameserving host, in numeric IP format.

Examples

```
Local>> SET SERVER NAMESERVER 192.0.1.49
```

See Also Set / Define IP Host Limit, page 13-85; Set / Define IP Nameserver, page 13-86; *Configuring the Domain Name Service (DNS)*, page 5-6.

13.49.15 Set/Define Server NetWare Loadhost



The loadhost parameter is used to specify name of the NetWare file server to be used for down-loading new software.

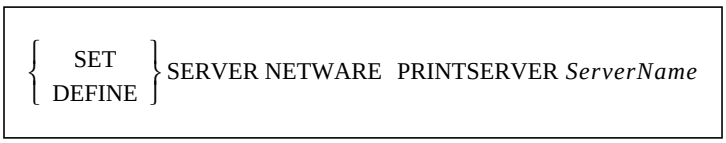
Restrictions You must be the privileged user to use this command.

Parameters **ServerName**
This parameter specifies the name of the file server to be used.

Examples
```
Local>> SET SERVER NETWARE LOADHOST fred
```

See Also LRS **Installation Guide**.

13.49.16 Set/Define Server NetWare Printserver



The Printserver parameter is used to specify name of the print server VAP / NLM running on the NetWare file server. This is used when setting up the LRS as a RPRINTER client.

Restrictions You must be the privileged user to use this command.

Parameters **ServerName**
This parameter specifies the name of the file server to be used.

Examples
```
Local>> SET SERVER NETWARE PRINTSERVER fred
```

13.49.17 Set/Define Server NetWare Reset

This command tells the print server to scan all accessible file servers for queues that it can service and would normally be used after configuring queues on a file server using PCONSOLE.

Restrictions You must be the privileged user to use this command.

Examples
```
Local>> SET SERVER NETWARE RESET
```

13.49.18 Set/Define Server Password Limit

```
{ SET    }
{ DEFINE } SERVER PASSWORD [LIMIT] { limit }
                                   { NONE  }
```

Limits the number of failures allowed when doing a Set Privileged command. After *limit* retries, the port will be logged out. The user can abort the password process by typing Ctrl-Z instead of the password.

Restrictions You must be the privileged user to use this command.

Parameters

limit
A value between 0 and 100. If zero is specified, the port is never logged out for too many password failures.

None
Sets the password limit to the default value.

Default 3 tries.

Examples

```
Local>> SET SERVER PASSWORD LIMIT 10
```

See Also Set Privileged / Noprivileged, page 13-124.

13.49.19 Set/Define Server Privileged Password

```
{ SET    }
{ DEFINE } SERVER PRIVILEGED[PASSWORD][passwd]
```

Sets the password for becoming the “superuser” of the server. If the password is not specified on the command line, the user will be prompted for it, and it will not be displayed on the screen as it is typed.

Restrictions You must be the privileged user to use this command.

Parameters

passwd
Six or fewer alphanumeric characters.

NOTE: *LRS passwords are case-independent, even when enclosed in quotes.*

Default system

Examples

```
Local>> SET SERVER PRIVILEGED PASSWORD “Yodel”

Local>> SET SERVER PRIVILEGED
Password: ok2bin (not echoed)
Verify: ok2bin (not echoed)
```

See Also Set Privileged / Noprivileged, page 13-124; *Privileged Password*, page 2-8.

13.49.20 Set/Define Server Prompt

{ SET / DEFINE } SERVER PROMPT *PromptString*

This command allows the manager to change the prompt that users see from the default **Local_x>** string. A string up to 16 characters long can be configured, and should be enclosed in quotes.

Restrictions You must be the privileged user to use this command.

Parameters **PromptString**
The following parameters can be included in the prompt string:

String	What it does to the prompt
%p	Substitutes the current port's name
%n	Substitutes the current port's number
%s	Substitutes the current server name
%D	Substitutes the product name (LRS2, LRS16, etc.)
%C	Substitutes the company name (Lantronix)
%S	Substitutes the current session name
%P	Substitutes a > if user is currently privileged
%%	Substitutes a percent sign (%)

Default Local_%n%P

Examples (Shown with the prompt that might result on the next line)

```
Local>> SET SERVER PROMPT “Port %n:“
Port 3: SET SERVER PROMPT “%D:%s! “
LRS2:LabServ! SET SERVER PROMPT “%p%S_%n%P%% “
Port_5[NoSession]_5>% SET SERVER PROMPT “Lcl_%n>%P”
Lcl_3>>
```

See Also *Changing the LRS Prompt*, page 2-4.

13.49.21 Set/Define Server RARP

{ SET / DEFINE } SERVER RARP { ENABLED / DISABLED }

Enables or disables querying for a RARP host at system boot time.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also LRS **Installation Guide**.

13.49.22 Set/Define Server Retransmit

Specifies the number of times that an SPX packet will be resent if it is not acknowledged.

Restrictions You must be the privileged user to use this command.

Parameters **LimitNum**
An integer between 4 and 100, inclusive.

Default 50 tries.

13.49.23 Set/Define Server Rlogin

This command restricts the use of the Rlogin command from the server. If Rlogins are disabled, users may not Rlogin to remote hosts. Incoming Rlogin connections may still be permitted, depending on the current Set / Define Server Incoming setting.

Restrictions You must be the privileged user to use this command.

Default Disabled.

13.49.24 Set/Define Server Session Limit

Sets the limit on active sessions per port. Each port can have an individual limit less than or equal to this limit.

Restrictions You must be the privileged user to use this command.

Parameters **limit**
A number between zero and 8.

None
The maximum possible session limit is used (8).

Default 4 sessions.

See Also *Sessions*, page 9-4.

13.49.25 Set/Define Server Software

```
{ SET    }
{ DEFINE } SERVER SOFTWARE filename
```

Specifies the name of the download software file (if any) the server will attempt to load at boot time. For IP-loading hosts, this is the file that will be requested at boot time. This command is only useful if it is Defined; if it is Set, it will be cleared / reset at boot time.

For TFTP loading, the complete path of the file can also be specified if the file is located in a directory other than the default. The path name can be up to 31 characters in length not counting the file name. The full path must be enclosed in quotes to preserve case.

Restrictions You must be the privileged user to use this command.

Parameters

filename
Load file name, 15 characters or less. The server will add the ".SYS" extension to the name.

Examples

```
Local>> DEFINE SERVER SOFTWARE LRS

Local>> DEFINE SERVER SOFTWARE "SYS:\LOGIN\LRS.SYS"

Local>> DEFINE SERVER SOFTWARE "/usr/rich/tscode"
```

See Also Set / Define Server Loadhost, page 13-129; *Editing Boot Parameters*, page 2-7; LRS **Installation Guide**.

13.49.26 Set/Define Server Startupfile

```
{ SET    }                                  [ host:filename[RETRY retrynum] ]
{ DEFINE } SERVER STARTUPFILE               [ NONE                          ]
```

Configures the startup configuration file that the LRS will attempt to download at boot time. This file contains the LRS commands that will configure the server before the users and services are started. If no retry limit is specified in the command, the LRS will retry failed downloads forever; otherwise it will retry that number of times and then boot normally.

Both the Telnet and NCP consoles are available at the time the server attempts to download the startupfile; if there is a problem with the download, you can still log into the server and determine what went wrong.

Restrictions You must be the privileged user to use this command.

Parameters

host
MOP node name or TCP / IP hostname or IP address.

To load from a TCP / IP host via TFTP, use the **host**:**filename** format. If a text hostname is used for TFTP, the name must be resolvable at boot time, otherwise you must use an IP address. To load from a Novell fileserver, use the **node\sys:\login\filename** format.

filename
A startup file name of up to 11 characters.

Retry
Configures the server retry limit. Must be used with the *retrynum* parameter.

retrynum
The number of times to retry the download attempt. The maximum number of retries is 1000.

None
The LRS will continually attempt to download the startup configuration file at boot time.

Default

Startupfile: none specified.

Retries: 5.

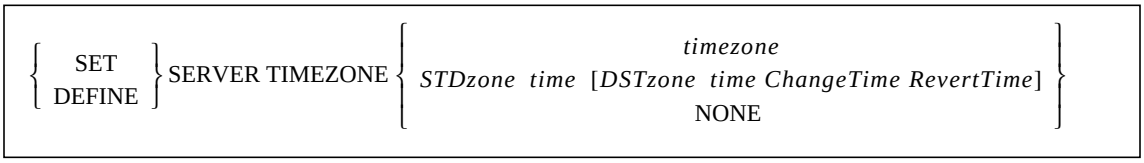
Examples

```
Local>> DEF SERVER STARTUPFILE “bob:start” RETRY 6

Local>> DEFINE SERVER STARTUPFILE
engfs\sys:\login\start.cmd”
```

See Also

Editing Boot Parameters, page 2-7; LRS **Installation Guide**.

13.49.27 Set/Define Server Timezone



Manually sets the LRS’s timezone.

Restrictions

You must be the privileged user to use this command.

NOTE: *This command is not available on the LRS1.*

Parameters

timezone
A pre-configured timezone name. Use the **Show/Monitor/List Timezone** command to see a list of available timezone names.

STDzone
A three-letter timezone name that represents your Standard Time zone (for example, use PST for Pacific Standard Time). Must be used in conjunction with the *time* parameter.

DSTzone
A three-letter timezone name that represents your Daylight Savings Time zone (for example, use PDT for Pacific Daylight Time). Must be used in conjunction with the *time* parameter.

time
The time difference from Greenwich Mean Time, entered as h:mm. Entering the minutes is optional.

ChangeTime
Enter the month, day, and time of day that the change to DST occurs, separating each element by a space (see the examples below). For the month, enter the first three letters of the month. For the day, recognized forms include:

5	the fifth day of the month
lastSun	the last Sunday in the month
Sun>=8	the first Sunday on or after the 8th of the month
Sun<=25	the last Sunday on or before the 25th of the month

For the time of day, use the same format as used for the *time* parameter.

RevertTime
Enter the month, day, and time of day that the timezone reverts to STD. The format is the same as for *ChangeTime*.

None
Specifies that no timezone will be used.

Examples

```
Local>> DEFINE SERVER TIMEZONE AMERICA/EASTERN

Local>> DEFINE SERVER TIMEZONE HST -10

Local>> DEFINE SERVER TIMEZONE MET 1:00 MET-DST 1:00 Mar
lastSun 2:00 Sep lastSun 2:00
```

(In the last example above, MET is the *STDzone*, and MET-DST is the *DSTzone*, both of which are one hour off of Greenwich Mean Time. The change to DST occurs on the last Sunday in March at 2:00, and it reverts back to Standard time on the last Sunday in September at 2:00.)

See Also Set / Define Server Clock, page 13-126; Show / Monitor / List Server Timezone, page 13-159; Show / Monitor / List Timezone, page 13-163.

13.49.28 Set/Define Server UUCP

Enables or disables the UUCP handler on the LRS. If enabled, the LRS will listen to TCP / IP port 540 and attempt to connect any logins there to a service called “UUCP” (typically a serial line with an attached modem). If this service is nonexistent, the connection will be closed.

Restrictions You must be the privileged user to use this command.

Default Disabled.

13.50 Set/Define Service

Creates a new service. For the description and syntax of particular parameters used in conjunction with this command (for example, Set / Define Service Postscript), refer to the individual entries that follow.

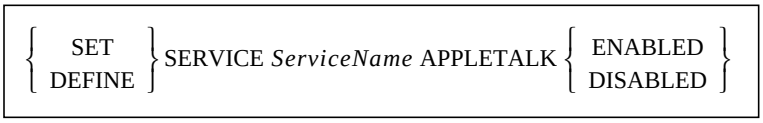
NOTE: *A maximum of 16 services can be created for the LRS.*

Restrictions You must be the privileged user to use this command.

Parameters **ServiceName**
A string of up to 16 alphanumeric characters. Spaces are not permitted.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.1 Set/Define Service AppleTalk



Specifies whether AppleTalk clients will be able to use the service.

Restrictions You must be the privileged user to use this command.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.2 Set/Define Service Banner

Specifies whether the LRS should print a banner page before starting the job. Banners should be disabled (the default) for all PostScript and plotter (binary) data.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.3 Set/Define Service Binary

If the binary characteristic is enabled on a service, character translation (i.e. <cr> to <cr><lf> translation) and tab expansion will be performed on the print data. The binary characteristic should be disabled when printing PCL data.

Restrictions You must be the privileged user to use this command.

Default Disabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.4 Set/Define Service EOJ

Specifies a string to be sent to the attached device at the end of every job regardless of network protocol.

Restrictions You must be the privileged user to use this command.

Parameters

EndString
Any ASCII characters, or non-ASCII characters entered as a backslash and 2 hex digits (for example, \45). The combined length of the SOJ and EOJ strings must not exceed 62 characters.

None
Clears any previously-configured string.

Default No string configured.

See Also Clear / Purge Service, page 13-11; Set / Define Service SOJ, page 13-142; Show / Monitor / List Services, page 13-160.

13.50.5 Set/Define Service Formfeed

If enabled (the default) the LRS will append a formfeed at the end of any LPR print jobs.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.6 Set/Define Service NetWare

Enables or disables NetWare access to the specified service.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.7 Set/Define Service Ports

Specifies a list of ports that will support or offer this service. If Enabled or Disabled is specified, the ports listed will be added to or removed from the current port list, respectively. If neither option is specified, the new port list will replace the old port list. Note that ports offering a service must be in the correct access mode for connections to succeed.

Restrictions You must be the privileged user to use this command.

Parameters **PortList/All**
Specifies a particular port or group of ports, or all ports. Port numbers are specified with integers between 1 and 16. Port numbers should be separated with commas (for lists) or dashes (for ranges).

NOTE: *In the absence of a PortList or the All parameter, the configuration will affect the current port only.*

Default Disabled.

Examples

```
Local>> SET SERVICE lab5 PORTS 3,4,7-8 ENABLED
```

See Also Clear / Purge Service, page 13-11; Set / Define Ports Access, page 13-104; Show / Monitor / List Services, page 13-160.

13.50.8 Set/Define Service Postscript

{ SET / DEFINE } SERVICE *ServiceName* POSTSCRIPT { ENABLED / DISABLED }

If enabled, the LRS will assume there is a PostScript printer attached to the service ports and will try to ensure a job is done before starting another. It will send a Ctrl-D to the attached device and wait for the printer to return a Ctrl-D before starting the job transfer. If this is not done, slower printers may lose new jobs while interpreting the previous job. Setting PostScript mode is strongly recommended for all PostScript queues.

Restrictions You must be the privileged user to use this command.

Default Disabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.9 Set/Define Service PSConvert

{ SET / DEFINE } SERVICE *ServiceName* PSCONVERT { ENABLED / DISABLED }

Controls whether the LRS will place a PostScript wrapper around each job. The LRS will try to detect if it is already a PostScript job, in which case it would not add an additional wrapper.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.10 Set/Define Service RTEL

Enables or disables RTEL access to the specified service.

Restrictions You must be the privileged user to use this command.

Default Enabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.11 Set/Define Service SOJ

Specifies a string to be sent to the attached device at the start of every access regardless of network protocol.

Restrictions You must be the privileged user to use this command.

Parameters

StartString
Any ASCII characters, or a backslash and two hex digits.

None
Clears any previously-configured string. No string is configured by default.

Examples

```
Local>> DEFINE SERVICE myserv SOJ \45
```

See Also Clear / Purge Service, page 13-11; Set / Define Service EOJ, page 13-139; Show / Monitor / List Services, page 13-160.

13.50.12 Set/Define Service SPX

Enables or disables SPX connections to the specified service. By default, SPX is disabled. When enabled, the service name will be advertised via SAP.

Restrictions You must be the privileged user to use this command.

Default Disabled.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.13 Set/Define Service TCPport

Associates a TCP listener socket with the given service. TCP connections to this socket will be connected to the service.

Restrictions You must be the privileged user to use this command.

Parameters

SocketNum
A particular socket. The socket number can be an integer from 4000 to 4999.

None
Clears the current socket number.

Default None.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.50.14 Set/Define Service Telnetport

Associates a TCP listener socket with the given service. TCP connections to this socket will be connected to the service. Unlike the TCPport option, a Telnetport socket will do Telnet IAC negotiations on the data stream.

Restrictions You must be the privileged user to use this command.

Parameters

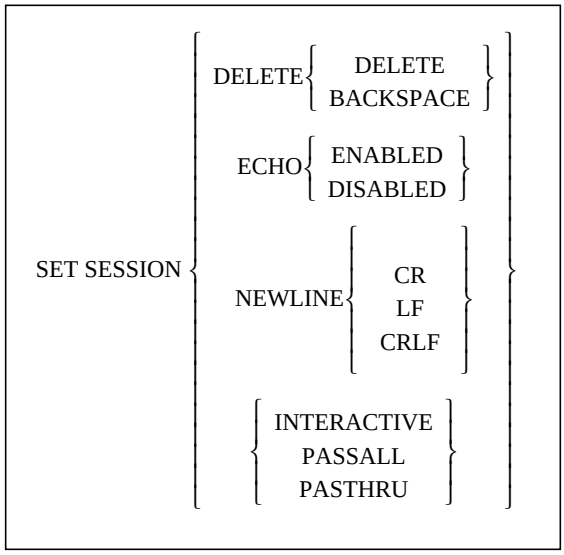
SocketNum
A particular socket. The socket number can be an integer from 4000 to 4999.

None
Clears the current socket number.

Default None.

See Also Clear / Purge Service, page 13-11; Show / Monitor / List Services, page 13-160.

13.51 Set Session



Specifies the characteristics for the current session.

Parameters

Delete
Specifies which character to send as the delete character. Set Session Delete sends a delete character (ASCII 0x7f). This command has no effect if Pasthru or Passall are in effect. This command and the Newline command may be helpful if you are getting odd output from a Telnet session.

Backspace
Set Session Delete Backspace sends a backspace character (ASCII 0x8, or Ctrl-H).

Echo
Enabling asks the LRS to echo for TCP connections. The default is Disabled, on the assumption that the remote host will provide echoing.

Newline
Changes what is sent to the remote service when you press the newline (usually <Return>) key. This command has no effect if Pasthru or Passall (see below) are in effect.

CR
Send carriage returns (ASCII 0xA) only.

LF
Send linefeeds (ASCII 0xD) only.

CRLF
Send both carriage return and linefeed.

Interactive
Allows server-specific keys (i.e. Forward, Backward, and Local) and messages to be interpreted by the LRS.

Passall
Disables server interpretation of switch characters, messages, and XON / XOFF flow control. Used for binary transfers, such as executable files and graphics.

Pasthru
Disables server interpretation of switch characters and server messages, but not XON / XOFF flow control. Used for ASCII file transfers.

Defaults Delete: Delete.

Newline: CR.

Examples

```
Local> SET SESSION DELETE BACKSPACE

Local> SET SESSION NEWLINE CRLF
```

See Also Show / Monitor Sessions, page 13-161; *Sessions*, page 9-4.

13.52 Set Site

Set Site is not a valid command. To configure sites, refer to the Define Site commands beginning on page 13-31.

13.53 Set SLIP

SETSLIP [*SiteName*][IPADDRESS *address*]

Starts SLIP on this port using the specified site's configuration.

Parameters

SiteName
A site name of up to 12 characters. If no site name is given, a site with the default site characteristics will be used.

IPaddress
Defines the non-negotiable remote IP address.

address
An IP address in standard numeric format (for example, 192.75.2.0).

Examples

```
Local> SET SLIP irvine

Local> SET SLIP allison IPADDRESS 192.0.1.221
```

See Also Set / Define Ports SLIPdetect, page 13-120; *PPP and SLIP*, page 3-8.

13.54 Set/Define SNMP

Configures a community name and access mode for SNMP access. Each name has an access restriction associated with it; if an SNMP command comes in with an unknown name or an unauthorized command, an SNMP error reply will be sent. Community names are not case-sensitive.

Restrictions You must be the privileged user to use this command.

Parameters

community
A text name, up to 16 characters long.

Access
Specifies the type of SNMP access. Must be used in conjunction with one of the following parameters: Both, None, or Readonly.

Both
Both read and write requests will be permitted.

None
No SNMP requests are permitted.

Read
Read-only access will be permitted.

Examples

```
Local>> SET SNMP COMMUNITY SUNMAN ACCESS BOTH
```

See Also Show / Monitor / List SNMP, page 13-162; Clear / Purge SNMP, page 13-11; Appendix C, *SNMP Support*.

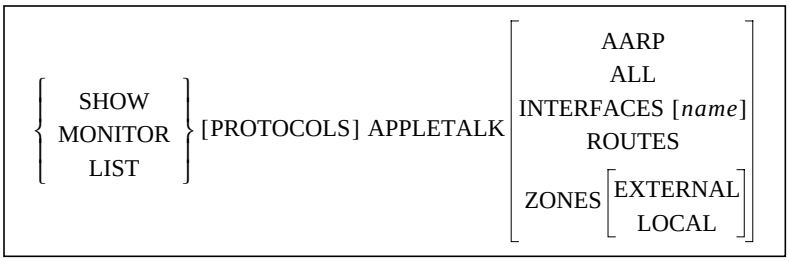
13.55 Set/Define Telnet Hosts

See Set / Define Hosts on page 13-81.

13.56 Show/Monitor/List

For a description of the differences between Show, Monitor, and List commands, see *Show, Monitor, and List* on page 13-1.

13.56.1 Show/Monitor/List AppleTalk



Displays information specific to the AppleTalk protocol. Use the **List** command to see the permanent attributes that will take effect upon reboot/login.

Restrictions You must be the privileged user to use this command.

Errors You cannot list AARP, Interfaces, or Zones External.

Parameters

AARP
Displays the mapping of AppleTalk node names to their addresses. Information includes each node's name, hardware address, and age.

All
Displays all currently-configured AppleTalk information.

Interfaces
Displays information about AppleTalk router interfaces. For more information about a specific interface, add its site *name*.

Routes
Displays AppleTalk routing table (RTMP) information for each zone, including network number, next router needed to get to the zone, metric, state, interface, and zone name.

Zones
Same as Routes, except that the routing table is arranged by zones.

External
Causes the LRS to query another router on the network for its routing table and display the information. For use only when routing is disabled.

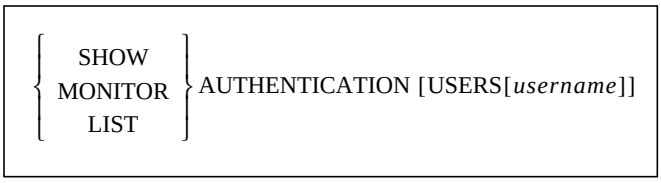
Local
Displays information about known local zones (zones that are at a distance of zero hops from the LRS).

Examples

```
Local>> SHOW APPLETALK INTERFACES
```

See Also Clear/Purge AppleTalk, page 13-4; Set/Define AppleTalk commands, beginning on page 13-59; Chapter 7, *AppleTalk*.

13.56.2 Show/Monitor/List Authentication



Displays the local authentication database.

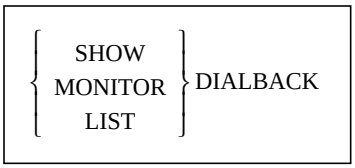
Restrictions You must be the privileged user to use this command.

Parameters **username**
Displays authentication information for the specified user.

Examples
```
Local>> SHOW AUTHENTICATION USER "bob"
```

See Also Set / Define Authentication, page 13-62; *Local (NVR) Database*, page 12-8.

13.56.3 Show/Monitor/List Dialback



Displays the currently configured dialback strings, as well as the number of connect attempts with that string and the number of connect failures.

Restrictions You must be the privileged user to use this command.

See Also Clear / Purge Dialback, page 13-5; Define Ports Dialback, page 13-15; Set / Define Dialback, page 13-73; *Dialback*, page 9-18; *Dialback from Local Mode*, page 12-5.

13.56.4 Show/Monitor/List Filter

Displays the currently configured packet filters. An individual filter may be specified using the optional *filtername* parameter.

Restrictions You must be the privileged user to use this command.

See Also Set / Define Filter, page 13-74; Clear / Purge Filter, page 13-6; *Filter Lists*, page 4-1.

13.56.5 Show/Monitor/List Hosts

Displays either the currently available TCP/IP (Telnet/Rlogin) hosts (Show) or the ones that have been Defined locally in the host table (List). Hosts will be shown with the method of discovery (rwho, connection, host table, etc.) and will also be marked if they are the current nameserver and/or gateway. Specifying a particular host name will show only that host's information. Wildcards for the hostnames are allowed. The All option is the default, and it displays all known TCP/IP hosts.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

hostname
Specifies a particular TCP/IP host.

All
Displays all the TCP/IP nodes that this server currently knows about. These include hosts from the local host table, as well as hosts seen by Rwho broadcasts and those resolved after a Connect/Telnet request.

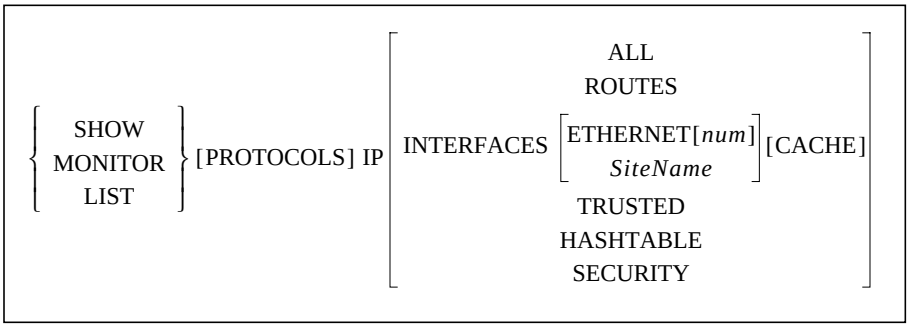
Local
Displays local TCP/IP nodes.

Examples

```
Local> SHOW HOSTS ALL
```

See Also Set/Define Hosts, page 13-81; Show/Monitor/List Authentication, page 13-148; *Adding Hosts to the LRS Host Table*, page 5-6.

13.56.6 Show/Monitor/List IP



Displays the current operating characteristics of the targets. Use the **List** command to see the permanent attributes that will take effect upon reboot/login.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Entering the **Show IP** command without additional keywords will display general IP protocol information, including the following counters.

The Reasons fields show counters in hexadecimal with the rightmost bit being 0. For example, a Connect Failure Reason of 0040 represents 0000 0000 0100 0000 in binary, which means that bit 6 is set. The meaning of each bit is explained in Table 13-1.

Table 13-1: IP Failure and Message Reasons

Bit	Connect Failure Reasons	Invalid Packet Reasons	ICMP Message Reasons
0	Internal failure, should be 0	Data received outside window	Echo message received
1		Connection terminated abnormally	Echo reply received
2	No nameserver defined (for text host name)	Packet received with an invalid data checksum	Destination unavailable; see bits 4-7
3	Attempted name service failed	Packet received with an invalid data header	Unknown ICMP type received
4	No gateway was configured for a non-local connection	RST packet sent to remote node	Network unreachable; usually from a gateway host
5	Attempted ARP failed	Packet received for an unknown local user	Host unreachable
6	Remote host did not answer	Unused, should be 0	Port unreachable; usually due to failed name service
7	Remote host rejected the connection		Protocol unreachable
8-15	Unused, should be 0		Unused, should be 0

All
Displays all defined IP information.

Routes
Displays the IP routing table.

Interfaces
Displays IP router interfaces. To display IP router information about a specific interface, Interfaces may be used in conjunction with one of the following parameters: Ethernet, Cache, or *SiteName.*

Ethernet
Displays information about a particular Ethernet interface. To specify the interface, use the *num* parameter.

num
An integer specifying a particular Ethernet interface.

SiteName
A particular site whose IP information will be displayed.

Cache
Displays cache statistics.

Trusted
Displays trusted IP routers.

Timeserver
Displays the timeserver.

Hashtable
Displays the routing table's hash table statistics.

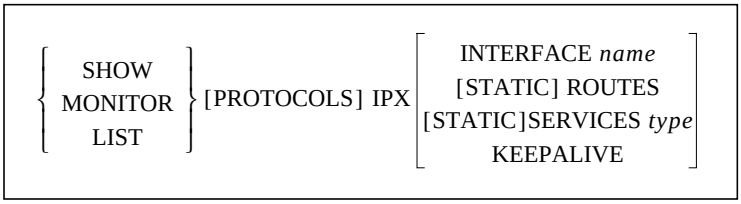
Security
Displays the active (Show, Monitor) or permanent (List) IP security entries.

Examples

```
Local> SHOW IP HASHTABLE

Local>> SHOW IP INTERFACES ETHERNET

Local>> SHOW IP INTERFACES ETHERNET 4
```

See Also Set / Define IP commands, beginning on page 13-84; Chapter 5, *IP*.

13.56.7 Show/Monitor/List IPX



Displays general routing information and routing characteristics.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Interface
Displays currently active IPX routing interfaces. To get more detailed information on a particular interface, specify the interface name with the *name* parameter.

name
Either a site name or an IPX frame type.

Static
Displays static routes or services. Can be used with either the *Routes* parameter or the *Services* parameter.

Routes
Displays all IPX routes, or only static routes if the *Static* keyword is added to the command.

Services
Displays all IPX services, or only static services if the *Static* keyword is added to the command.

type
Specifies a particular service type to display. between 0000 and ffff. For example, type 4 is file servers.

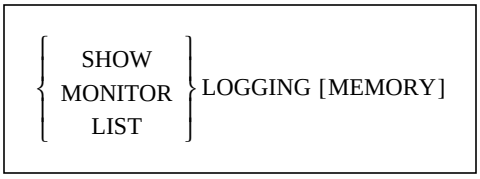
Keepalive
Displays information on spoofed entries.

Examples

```
Local> SHOW IPX STATIC ROUTES
```

See Also Set / Define IPX commands, beginning on page 13-90; Chapter 6, *IPX*.

13.56.8 Show/Monitor/List Logging



Displays the current or saved event logging configuration.

Restrictions You must be the privileged user to use the Monitor command.

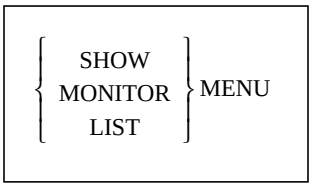
Secure users may not use this command.

Parameters

Memory
Displays the memory log.

See Also Set / Define Logging, page 13-96; *Event Logging*, page 12-25.

13.56.9 Show/Monitor/List Menu

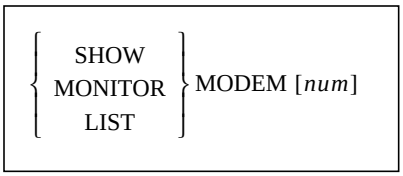


Displays the current or saved Menu entries.

Restrictions You must be the privileged user to use the Monitor command. Secure users may not use this command.

See Also Clear / Purge Menu, page 13-10; Set / Define Menu, page 13-100; *Menu Mode*, page 9-18; *Menu Mode*, page 12-20.

13.56.10 Show/Monitor/List Modem



Displays a list of modem profiles.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

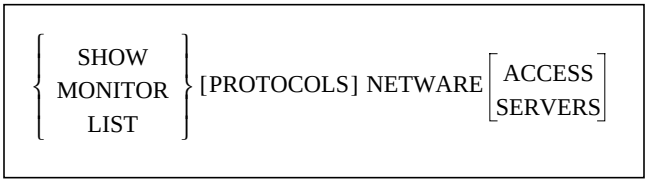
num
A particular modem profile type to display.

Examples

```
Local> SHOW MODEM 3
```

See Also *Modem Profiles*, page 10-2.

13.56.11 Show/Monitor/List NetWare



Displays the current operating characteristics of the targets. Use the **List** command to see the permanent attributes that will take effect upon reboot / login.

Restrictions You must be the privileged user to use the Monitor command.

Parameters Entering **Show NetWare** without any parameters displays detailed counters and status messages specific to the NetWare protocol, including routing and encapsulation information, and packet transfer counters by packet type.

The Error Reasons field shows error counters in hexadecimal with the rightmost bit being 0. For example, an Error Reason of 0040 represents 0000 0000 0100 0000 in binary, which means that bit 6 is set. The meaning of each bit is explained in Table 13-2 on page 13-154.

Table 13-2: IPX Error Reasons

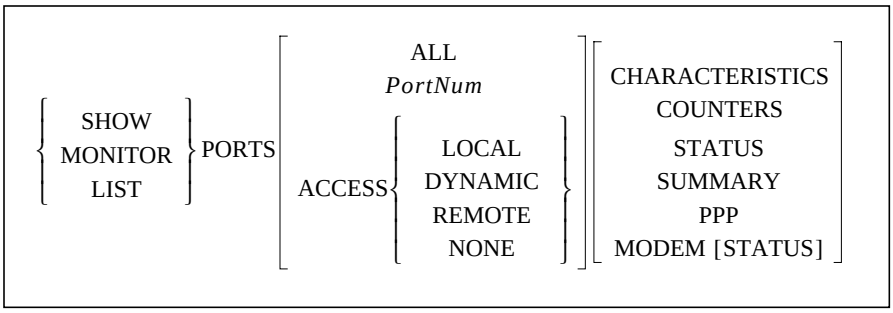
Bit	Meaning	Explanation
0	Received packet for an unknown IPX protocol.	Packet discarded.
1	Received packet for unknown socket.	Packet discarded.
2	Couldn't attach to print queue on file server.	When a printer is found that needs to be serviced, the LRS attaches to the fileserver. If the LRS cannot attach, it can't service the queue.
3	Couldn't connect to a fileserver.	If the LRS hears from a fileserver that matches its own access list, it will try to connect to the fileserver and scan for print queues. If the connection does not go through, there may be security or license limit issues.
4	Couldn't log out of the fileserver.	This bit should never be set.
5	The LRS couldn't get its server name and password credentials from fileserver during login.	Login fails.
6	Fileserver did not accept the LRS server name and password credentials.	If the login password is "access" (the default), the LRS doesn't send a password. Otherwise, the login password has to match the print server password on the fileserver. For example, if the name of the LRS is "BUNDY" and the login password for BUNDY is "shoes," then under PCONSOLE, printserver BUNDY needs to have password "shoes."
7	Couldn't log into the fileserver.	Perhaps the login slots are filled.
8	Check membership call failed.	While scanning for print queues, the LRS checks the memberships of various objects; this is not generally a problem.
9	Couldn't map user to trustee.	This is where the LRS tries to get rights to access the print queue; login fails.
10	Couldn't attach to print queue on fileserver.	Same as bit 2.
11	Couldn't service the print queue or couldn't read the job.	There is a print job on the fileserver, but the LRS cannot access it.
12	Couldn't open a file on the fileserver.	This is not a serious error.
13 +	Unused, should be 0.	

Access
Shows the current NetWare access list.

Servers
Shows the NetWare servers that the LRS can see.

See Also Chapter 6, *IPX*.

13.56.12 Show/Monitor/List Ports



These commands display information about the server's ports. The current port is the default, unless another port number or All is specified. You can also get information about all the local ports having a particular Access value. If no keywords are added to the command, the current port's Characteristics will be shown.

If the port is a virtual port, irrelevant information (such as baud rate, parity, or flow control) will not be displayed. Any List command performed for a virtual port will display the template port's configuration.

Restrictions

You must be the privileged user to use the Monitor command.

Secure ports cannot Show or List ports other than their own.

Errors

Status and Counters parameters are not valid with List.

Counters is not valid for virtual ports.

Parameters

All
Displays information for all ports.

PortNum
Specifies a particular LRS port.

Access
Display ports that match a specified access-type. Must be used in conjunction with the *Local*, *Dynamic*, *Remote*, or *None* parameter.

Local
Displays ports set to Local access. Local access restricts logins on the port to local users.

Dynamic
Displays ports set to Dynamic access. Dynamic access permits local or remote users to log into the port.

Remote
Displays ports set to Remote access. Remote access restricts logins on the port to remote (network) users.

None
Displays ports with access set to None. None prevents all access to the port, including user logins.

Characteristics
Displays information from the operational database about the specified ports, including the port's settings, such as baud rate, parity, preferred services, name, username, and group codes.

Counters
Displays the port's local and remote accesses as well as any communication errors.

Status
Displays information regarding the port's serial connections, including the current flow control state and the state of the DSR and DTR signals.

Summary
Displays a one-line summary of information about the specified ports. The information includes type of access, status, and services offered. The Summary option shows the access type, any offered services, and the login status of the port.

PPP
Displays information about the Point to Point Protocol's Link Control Protocol on the specified ports.

Modem
Displays information about modem control and configuration strings on the specified ports.

Status
The Modem Status option shows the last connect speed of the modem connected to the specified port(s), and the last available Caller-ID information for the port(s). Modem control must be enabled for this command to work.

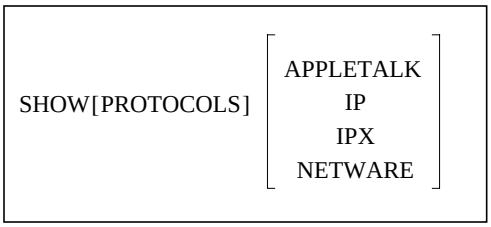
NOTE: *The Modem Status option is of no use for remote access or no access ports.*

Examples

```
Local> SHOW PORT ALL SUMMARY

Local> LIST PORT ACCESS DYNAMIC COUNTERS
```

See Also
Define Ports commands beginning on page 13-14; Set / Define Ports commands beginning on page 13-104; Chapter 9, *Ports*.

13.56.13 Show/List Protocols



When the Show Protocols command is used without any parameters, a summary screen of all protocols will be displayed. General figures, such as packet counts and error status, will be shown.

To displayed information about a particular protocol, use the AppleTalk, IP, IPX, and NetWare parameters. To display detail about these protocols, refer to the alphabetical listing for the protocol. For example, to see detail on the IPX protocol, refer to Show / Monitor / List IPX.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

AppleTalk
Displays detailed counters specific to the AppleTalk protocol, including those for the Datagram Delivery Protocol (DDP), AppleTalk Transmission Protocol (ATP), and Printer Access Protocol (PAP).

IP
Displays detailed counters and status messages specific to the TCP / IP protocol, including configured nameservers and gateways, the default domain name, packet information, and ICMP counters.

IPX
Displays detailed counters specific to the IPX protocol, including routing and encapsulation information, the netrange and timeserver, and the status of RIP and SAP for each IPX interface.

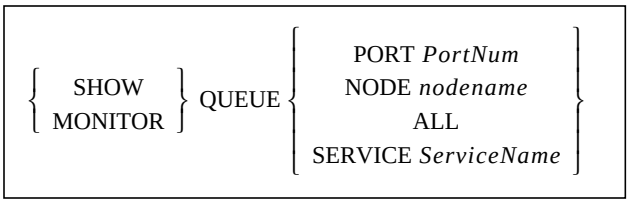
NetWare
Displays information and counters and status messages specific to the NetWare protocol, including routing and encapsulation information, and packet transfer counters by packet type.

Examples

```
Local> SHOW PRINTER STATUS
```

See Also Netstat, page 13-52; Chapter 5, *IP*; Chapter 6, *IPX*.

13.56.14 Show/Monitor Queue



Show Queue will display the entries in a connect queue, if it exists. Particular sets of queues or entries can be selected with the Port, Node, or Service parameters. All can also be specified to show all entries.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Port
Displays information for all queue entries that can be served by the specified port. Must be used in conjunction with the *PortNum* parameter.

PortNum
Specifies a particular LRS port.

Node
Displays information for all queue entries requested from the specified node. Must be used in conjunction with the *nodename* parameter.

nodename
Specifies a particular node.

All
Displays information for all ports and nodes.

NOTE: *All is the default setting for Show/Monitor Queue.*

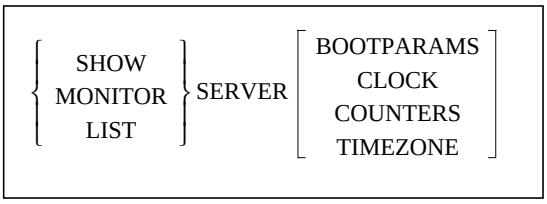
Service
Displays information for all queue entries for the local service specified with the *ServiceName* parameter.

ServiceName
Specifies a service name of up to 16 characters.

Examples

```
Local> SHOW QUEUE Port 6

Local> MONITOR QUEUE SERVICE lab5
```

13.56.15 Show/Monitor/List Server



This command is used to display the global attributes or counters for the server itself.

NOTE: *The Clock and Timezone options are not available on the LRS1.*

Restrictions You must be the privileged user to use the Monitor command. The List Server command can only be used with the Bootparams parameter.

Parameters

Bootparams
Displays parameters related to rebooting the unit and reloading the software file.

Clock
Displays the local time and date and the UTC (GMT) time and date.

Counters
Counters can be reset to zero with the Zero Counters All command. Displays the accumulated error counters for the Ethernet and TCP/IP protocols. The four-digit bit position numbers represent one of the network error reasons listed below:

Table 13-3: Server Failure Reasons

Bit	Send Failure Reason	Receive Failure Reason
0	Unused, should be 0	Unused, should be 0
1	Unused, should be 0	Packet received with CRC error
2	At least one collision has occurred while transmitting	Received packet did not end on byte boundary
3	Transmit aborted due to excessive (more than 16) network collisions	FIFO overrun: Could not write received data before new data arrived
4	Carrier sense was lost during transmission	Receive packet could not be accommodated due to lack of receive buffers
5	FIFO underrun: Ethernet controller could not access transmit data in time to send it out	Received a packet larger than the maximum Ethernet size (1536 bytes)
65	CD heartbeat not received after transmission	Unused, should be 0
7	Out-of-window collision detected	
8-15	Unused, should be 0	

Timezone
Displays the timezone if a timezone has been specified.

Examples

```
Local> SHOW SERVER BOOTPARAMS
```

See Also Set / Define Server Clock, page 13-126; Set / Define Server Timezone, page 13-136; *Setting the Date and Time*, page 2-5.

13.56.16 Show/Monitor/List Services

This command is used to display the characteristics of the services on the network. Remember that this list is masked by the services that this port is eligible to see—users will not see services they cannot connect to.

Restrictions You must be the privileged user to use the Monitor command.

Parameters

Local
Displays those services local to this server, whether available or not.

service
Specifies a particular LRS service. Numbers and wildcards are permitted.

All
Displays all known services usable by the current port.

Characteristics
Displays information about the known (local and remote) services. Information includes service rating, group code, and if the service is local, the service ports and service flags (such as Queueing and Connections).

Summary
Displays one-line summary information for the specified services.

Status
Displays full information for the specified services including network address, protocol version, and other services that node offers.

Examples

```
Local> SHOW SERVICE lab5_prtr STATUS

Local> MONITOR SERVICE LOCAL SUMMARY
```

See Also Set / Define Service, page 13-138.

13.56.17 Show/Monitor Sessions

Displays information about the specified sessions.

Restrictions You must be the privileged user to use the Monitor command.

Secure users cannot specify Port or All.

Parameters

PortNum
Specifies a particular LRS port.

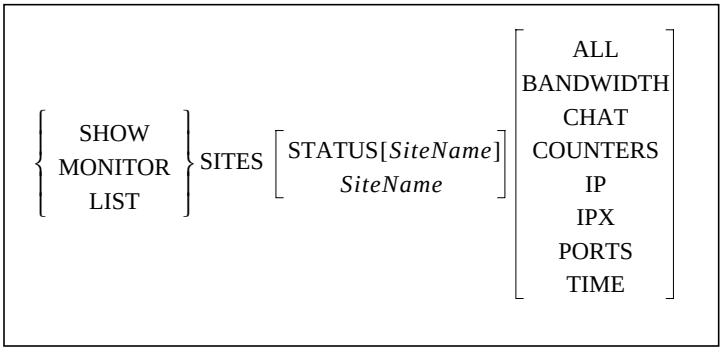
All
Displays the sessions currently running on all ports.

Examples

```
Local> SHOW SESSION

Local> SHOW SESSION PORT 5
```

See Also Set / Define Ports Security, page 13-118; *Sessions*, page 9-4.

13.56.18 Show/Monitor/List Sites



In general, displays information about a specified site. The **All** keyword is a special case, as described below.

Restrictions You must be the privileged user to use this command.

Parameters

SiteName
A particular site name of up to 12 characters.

All
Displays all accumulated statistics for all sites that have started since the LRS was last booted, not just those that are running.

Bandwidth
Displays the specified site's bandwidth configuration and related statistics.

Chat
Displays a site's chat script.

Counters
Displays a site's counters.

IP
Displays a site's IP configuration.

IPX
Displays a site's IPX configuration.

Ports
Displays a site's ports.

Time
Displays time configuration for the specified site, including.

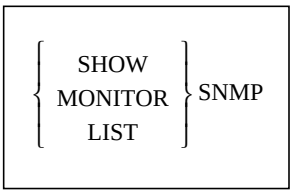
Status
Displays statistics for sites that have been active since booting.

Examples

```
Local> SHOW SITE irvine CHAT

Local> SHOW SITE irvine IP
```

See Also Define Site, page 13-31.

13.56.19 Show/Monitor/List SNMP



Displays the current or saved SNMP security table entries.

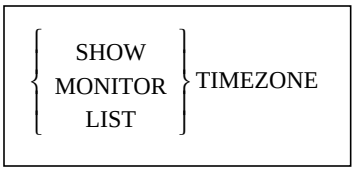
Restrictions You must be the privileged user to use this command.

See Also Clear / Purge SNMP, page 13-11; Set / Define SNMP, page 13-146; Appendix C, *SNMP Support*.

13.56.20 Show/Monitor/List Telnet Hosts

See Show / Monitor / List Hosts on page 13-149.

13.56.21 Show/Monitor/List Timezone

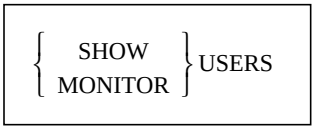


Displays a table of timezone abbreviations which can be used to select a timezone for the server.

Restrictions You must be the privileged user to use the Monitor command.

See Also Set / Define Server Timezone, page 13-136; *Setting the Date and Time*, page 2-5.

13.56.22 Show/Monitor Users



Displays the current users logged onto the server. For each user, the LRS displays the port username and current connection information.

Restrictions You must be the privileged user to use the Monitor command.

Errors List Users will cause an error.

13.56.23 Show Version

Displays the current version of the LRS software.

See Also *Reloading Operational Software*, page 2-7.

13.57 Source

SOURCE *host*:*filename*[VERIFY]

Source attempts to download a configuration file from a TFTP or NetWare host. The file is assumed to be lines of server commands which will be executed. The Source command is most useful for trying out a configuration file before using the Set/Define Server Startupfile command (page 13-135). To use TFTP, use the **hostname:filename** format. For NetWare, use the **hostname\sys:\login\filename** format. Note that files to be downloaded via NetWare must be in the login directory on the fileserver, due to access restrictions.

Restrictions You must be the privileged user to use this command.

Parameters

host
Either a NetWare fileserver name or a TFTP host (text host name or IP address).

filename
The download path and filename, 22 characters maximum.

NOTE: *If filename contains lower-case letters, it must be enclosed in quotation marks.*

Verify
Displays each command from the configuration file before executing it.

Examples

```
Local> SOURCE "labsun:start.com"

Local> SOURCE LABFS4\SYS:\LOGIN\LRS.COM
```

See Also Set/Define Server Startupfile, page 13-135.

13.58 Telnet

Telnet is a shorthand for the Connect Telnet command. For a description of the command, see Connect on page 13-12.

13.59 Test

13.59.1 Test Port

TEST PORT [*PortNum*][POSTSCRIPT] [COUNT *lines* | WIDTH *characters*]

Tests a serial port's connection by sending a continuous stream of ASCII alphabetic characters until the number of lines specified by Count is reached. You can stop the test by pressing any key.

Restrictions

Non-privileged users may only test their own port.

Virtual and multisession-enabled ports can only be tested by the user on that port.

Parameters

PortNum
Specifies a particular LRS port.

PostScript
Sends a PostScript test page to the port instead of ASCII data.

Count
Specifies the number of test lines to be sent, or if in postscript mode, the number of pages to print. Any character will terminate the test. Must be used in conjunction with the *lines* parameter.

lines
The number of lines to be sent to the port. There is no line limit.

Width
The number of characters per line in the test pattern. Must be used in conjunction with the *characters* parameter.

characters
Enter an integer between 1 and 132, inclusive.

Examples

```
Local> TEST PORT
```

```
Local> TEST PORT 4 WIDTH 45 COUNT 5
```

13.59.2 Test Site

TEST SITE *SiteName*

Tests a site without having to force packet traffic. When the command is issued, the LRS will attempt a connection to the site and return basic status. The site must then be shut down manually.

Errors

An error will be returned if the site is unavailable. For more detailed information, use the Logging feature.

See Also

Define Site, page 13-31; Set / Define Logging, page 13-96; *Setting Up Sites*, page 3-3.

13.60 Unlock Port

UNLOCK PORT *PortNum*

Unlocks a locked port, which may be necessary if the user has locked the port and forgotten the password. The command does nothing if the port is already unlocked.

Restrictions You must be the privileged user to use this command.

Parameters

PortNum
The number of the locked LRS port.

Examples

```
Local> UNLOCK PORT 6
```

See Also Lock, page 13-51; *Locking a Port*, page 9-9; *Locking a Port*, page 12-19.

13.61 Zero Counters

ZERO COUNTERS [ALL | ETHERNET | PORT *PortNum*]

This command is used to reset the counters for errors and other network and server events.

Restrictions You must be the privileged user to zero some other port (or All).

Parameters

All
Zeroes all Ethernet, TCP/IP, SLIP, and serial port counters.

Ethernet
Zeroes only Ethernet counters.

Port
Zeroes only the counters for events associated with a single serial port.

NOTE: *In the absence of a PortNumber or the All or Ethernet parameters, the configuration will affect the current port.*

Examples

```
Local> ZERO COUNTERS Port 6
```

A - Technical Support

A.1 Lantronix Problem Report Procedure

If you are experiencing problems with the LRS or have suggestions for improving the product, please contact Lantronix Technical Support at (800) 422-7044 or (714) 453-3990. We are also reachable via Internet email at support@lantronix.com.

If you are submitting a problem, please provide the following information:

- Your name, company name, address, and phone number
- Product name
- Unit serial number
- Software version (available by issuing the **Set/Define Telnet Hosts** command)
- Network configuration including the output from a **Netstat** command
- Description of the problem
- **Debug** report (stack dump) if applicable
- Product status when the problem occurred; please try to include information on user and network activity at the time

15353 Barranca Parkway, Irvine, CA 92618 USA • 714/453-3990 • Fax: 714/453-3995
North American Direct Sales: 800/422-7055 • North American Reseller Sales: 800/422-7015
North American Sales Fax: 714/450-7232 • Internet: sales@lantronix.com
International Sales: 714/450-7227 • International Sales Fax: 714/450-7231
Internet: ww@lantronix.com
Technical Support: 800/422-7044 or 714/453-7158
Technical Support Fax: 714/450-7226 • Internet: support@lantronix.com

B - Updating Software

The latest version of the Lantronix LRS software and its associated release notes can be downloaded directly from Lantronix via dial-in modem or using anonymous FTP through the Internet.

Comments or requests for help via e-mail are welcome - send them to **support@lantronix.com** and they will be routed appropriately. Questions or comments regarding the FTP / download process itself can be sent to **ftp@lantronix.com**. Mail can also be sent from within the Lantronix BBS system.

B.1 Updating Using FTP

The LRS operational software resides on the Lantronix FTP server (ftp.lantronix.com). The current IP address of the server is 192.73.220.84. The address is subject to change at any time, therefore the text name should be used if at all possible. The files are stored in normal and UNIX compress formats (filename.Z); if you have access to the UNIX uncompress utility, get the compressed versions. These files are binary data, so the binary option must be used when transferring the files.

To log into the FTP server, use a username of **anonymous** and enter your full email address as the password. If the FTP server cannot verify the username or email address, you will be denied access. The machine issuing the FTP command must be resolvable via the INADDR.ARPA DNS record for the connection to succeed. If access is denied, try using a “known” machine such as a gateway or nameserver.

When connected to the Lantronix FTP server, the following text will be displayed:

Figure B-1: Lantronix FTP Session

```
230-Welcome to the Lantronix FTP Server.
230-
230-IMPORTANT: Please get the README file before proceeding.
230-IMPORTANT: Set BINARY mode before transferring executables.
220-
230-Direct questions to support@lantronix.com or 1.800.422.7044
230-Questions about this ftp account only to ftp@lantronix.com
230-
230-
230 Guest login ok, access restrictions apply.
Remote system type is UNIX. [your type will be displayed here]
Using binary mode to transfer files.
ftp>
```

All released files are in the **pub** directory. Always download the README file in the pub directory before downloading anything else; it contains a directory of available versions.

B.2 Updating Using a Modem

The Lantronix system supports the following modems for the physical connection: v.32, v.42, v.42bis, and 9600 / 2400 / 1200 / 14400 baud. The following software is supported for the file transfer: KERMIT, xmodem, ymodem, and zmodem. The modem phone number is USA (714) 367-1051. The account name is **ets** and the password is **server**.

Remember that the download files (*.SYS) and executable files are image data and should only be transferred in binary mode. If binary mode is not used, the files will be corrupted.

When you have finished downloading files, type “g” to logout of the bulletin board system.

Figure B-2: Lantronix BBS System, New User Entries

```
SunOS UNIX (nexus)
login: ets
Password: server (not echoed)
Last login: Mon Jun 5 13:21:13 from company.com
SunOS Release 4.1.3_U1 (NEXUS) #2: Fri Dec 2 10:08:39 PST 1994
Welcome to the Lantronix BBS. Type ‘h’ for help
userid (‘new’ for new user): new
Welcome, new user! Enter a userid, 1-12 characters, no spaces.
Userid: bob
Enter Passwd: platypus (not echoed)
Confirm Passwd: platypus (not echoed)
User Name: bob
Terminal type (default=vt100):
Email address, if any: bob@widgets.com
```

Figure B-3: Lantronix BBS System, Introduction Screen

```
Welcome to the “NEW” Lantronix Bulletin Board System.
To access the files menu, type ‘f’ at the main menu.
At the files menu, type ‘p’ to select a download protocol
(a=ascii, k=kermit, x=xmodem, y=ymodem, z=zmodem)
At the files menu, type ‘l’ to list available software directo-
ries.
Select the board name by entering its number.
At any menu, press ‘h’ to receive additional help.
Press [Return] to continue:
```

B.3 Reloading LRS Software

The LRS stores software which controls the initialization process, the operation of the LRS, and the processing of commands in Flash ROM. The contents of Flash ROM can be updated by downloading a new version of the operational software.

LRS software can be reloaded using EZCon, or from network hosts using IPX, TFTP, or MOP. If EZCon is used, refer to the accompanying EZCon documentation for reloading instructions.

If an IPX, TFTP, or MOP host is used, the following points are important:

- The Flash ROM software is contained in a file called LRS16.SYS. These files are provided with the LRS on CD-ROM. The appropriate Flash ROM file for your unit must be accessible when updating Flash ROM.
- The LRS16.SYS download file should be world-readable on the host, regardless of which download method is being used. In addition, there is a 31 character length limit for the path name and a 15 character limit for the filename.
- Define commands are used in the examples on the next few pages because configurations made with Set commands are cleared when the LRS boots. Use the **List Server Boot** command to check the LRS settings before using the Initialize Reload command.

NOTE: *If you experience problems reloading Flash ROM, refer to Troubleshooting Flash ROM Updates on page B-5.*

B.3.1 IPX

The LRS16.SYS file should be placed in the login directory on the NetWare file server. The LRS cannot actually log into the file server (since it knows no username / password); it can only access files in the login directory itself. On the LRS, specify the file server name, filename and path:

Figure B-4: Reloading LRS16 Flash ROM From IPX

```
Local> SET PRIVILEGED
Password> SYSTEM (not echoed)
Local>> DEFINE SERVER NETWARE LOADHOST fileserver
Local>> DEFINE SERVER SOFTWARE “SYS:\LOGIN\LRS16.SYS”
Local>> LIST SERVER BOOT
Local>> INITIALIZE RELOAD
```

NOTE: *Check the LRS settings before using the Initialize Reload command to ensure that you are reloading the correct software file.*

B.3.2 TFTP

Downloading uses TFTP (Trivial File Transfer Protocol) and optionally BOOTP. The LRS will perform a BOOTP query each time it boots. If a host provides BOOTP support, it can be used to set the LRS's IP address and loadhost information. Add the LRS's name, IP address, Ethernet address, and download path and filename to the BOOTP file (usually **/usr/etc/bootptab**).

Some BOOTP and TFTP implementations require a specific directory for the LRS16.SYS file; in this case the path is not specified in the bootptab file and the file must be placed in that directory. If BOOTP cannot be used to configure the LRS's IP parameters, configure them manually using the following commands:

Figure B-5: Reloading LRS16 Flash ROM From TFTP

```
Local> SET PRIVILEGED
Password> SYSTEM (not echoed)
Local>> DEFINE IP ADDRESS 192.0.1.220
Local>> DEFINE SERVER SOFTWARE "/path/LRS16.SYS"
Local>> DEFINE SERVER LOADHOST 192.0.1.210
Local>> LIST SERVER BOOT
Local>> INITIALIZE RELOAD
```

The path and filename are case-sensitive and must be enclosed by quotation marks. Booting across an IP router requires that the router be configured to perform proxy ARPing for the LRS.

B.3.3 MOP

Copy the LRS16.SYS file to the MOM$LOAD directory. The LRS16.SYS filename is the only parameter that the LRS needs to reload via MOP. Make sure the service characteristic is enabled on the host's Ethernet circuit, and then reload the server using the following commands:

Figure B-6: Reloading Flash ROM From MOP

```
Local> SET PRIVILEGED
Password> system (not echoed)
Local>> INITIALIZE RELOAD
```

B.3.4 Reloading Sequence

If BOOTP or RARP are enabled on the LRS they will request assistance from a BOOTP or RARP server before starting the download attempts. The LRS will then try TFTP, NetWare, and MOP booting (in that order) provided that it has enough information to try each download method.

Downloading and rewriting the Flash-ROM will take approximately two minutes from the time the Initialize command is issued. If more than two minutes have elapsed and the server has still not successfully booted, connect a terminal to the console port. The displayed error message should explain what is happening.

If the download file cannot be found or accessed, the LRS can be rebooted with the code still in the Flash-ROMs. As noted in the Installation section, the OK / Activity LED will blink quickly while the LRS is booting (and reloading code) and then slowly when it returns to normal operation.

B.4 Troubleshooting Flash ROM Updates

Many of the problems that occur when updating Flash ROM can be solved by completing the following steps:

NetWare Make sure the file is in the login directory. Since the LRS cannot actually log into the file server, it has limited access to the server directories.

TFTP Check the file and directory permissions. Make sure the loadhost name and address are specified correctly and that their case matches the case of the filenames on the host system. Ensure that the host has TFTP enabled; several major UNIX vendors ship their systems with TFTP disabled by default.

MOP The Ethernet circuit must have the **service** characteristic enabled. Verify that the MOM$LOAD search path includes the directory containing the LRS16.SYS file.

C - SNMP Support

SNMP is an abbreviation for Single Network Management Protocol. SNMP commands enable users (usually system administrators) to get information from and control other nodes on a local area network.

Information about SNMP can be obtained in RFCs (Request For Comments) which can be obtained via anonymous FTP from **nisc.jvnc.net**. To obtain a specific RFC, use the pathname **pub/RFC/ rfc*nnn***, where ***nnn*** is the name of the desired RFC. To obtain the RFC index, use the pathname **pub/RFC/rfc-index.txt**.

The extent to which other nodes may be controlled and / or queried for information is documented in Management Information Bases (MIBs). The MIBs and SNMP in general are documented in RFCs 1066, 1067, 1098,1317, 1318, and 1213.

The following MIBs are supported:

MIB-II (RFC 1213):	System, Interface, Address Translation, IP, ICMP, TCP, and UDP. They do not support the EGP group.
RS-232 MIB (RFC 1317):	All objects (RS-232-style objects).
Character MIB (RFC 1318):	All objects (character-oriented devices).

C.1 LRS SNMP Support

- The LRS will respond to queries for unknown MIBs with a “not in MIB” error to the requesting host.
- The LRS has a local SNMP security table to restrict or prevent unauthorized SNMP configuration.
- The LRS will also generate limited forms of 3 of the SNMP **traps**. Traps are sent to a host when an abnormal event occurs on the LRS.

Currently, the LRS will generate a Coldstart trap when it first boots, and will send a Linkup trap when the startupfile (if any) has been read from a host and normal operation commences. If a startupfile has been configured but the download fails, the LRS will send an Authentication trap. In all 3 cases, the trap will be directed to the IP address of the loadhost for the LRS. If a loadhost has not been specified (Flash ROM based units, for example), the traps will not be sent. The LRS will not generate traps other than the cases listed here.

C.2 SNMP Security

Because SNMP can be used to change security settings, the LRS provides a security mechanism for restricting SNMP access to the unit. The security mechanism is linked to the SNMP community name. By default, the only allowed community name is **Public**, which is given only Read privilege.

To change, add, or delete community names in the table, **Set/Define SNMP** and **Clear/Purge SNMP** are used. Set SNMP requires specification of a community name and an access type. Available access types are Readonly, Both (allows read and write), or None. Clear SNMP requires either a community name to remove a single entry or the **All** parameter to clear the entire table. **Show/Monitor/List SNMP** commands require privileged access to prevent unauthorized users from seeing the allowed community names.

The LRS sends an error message when it receives SNMP queries or Set requests that are not permitted for the current user.

D - Boot Troubleshooting

This Appendix discusses the symptoms that may be encountered, and diagnoses possible errors.

D.1 Diagnosing the Error

To properly diagnose an error, connect a terminal to the console port. Take note of any error message displayed on the terminal. Table D-1 lists each error message, and problems that don't necessarily display a message. If the terminal displays an error message that isn't listed in the following table, try to match the message with one discussed in the table. If none match, contact your dealer or Lantronix Technical Support.

Table D-1: Error Messages

Problem	Error	Remedy
Terminal doesn't display information. No prompt is displayed.	The terminal's setup is incorrect or there is a connection error.	Check the terminal setup and physical connections. Try another terminal or cable, or try cycling power on the LRS.
Terminal displays a Boot> prompt rather than a Local> prompt	No network is present.	Specify the correct Ethernet interface using the **Set Server Ethernet command**. Reboot the LRS.
	Init Noboot was issued at the Local> prompt.	Configure and reboot the LRS. Use the **Set Server Hardware xx-xx-xx** command to set the correct address.
	The Ethernet address is invalid.	Reboot the LRS.
Request BOOTP: no valid reply received	The BOOTP request has failed.	The unit will still boot. Check the BOOTP server's configuration. See page D-2 for more information.
Request RARP: no valid reply received	The RARP request has failed.	The unit will still boot. See your host man pages for rarpd information.
Attempting NetWare boot: failed	The flash is invalid	Reload the code. Make sure that the LRS is using the proper fileserver name, and that the fileserver is running properly. Both devices must be on the same network.
		Make sure that the LRS is using the complete and correct loadfile pathname, including the drive name. Verify that the loadfile is in the login directory and is world-readable.
	The flash needs to be replaced.	Contact your dealer or Lantronix Technical Support for assistance.

Table D-1: Error Messages, cont.

Problem	Error	Remedy
Attempting TFTP boot: failed	The flash is invalid.	Reload the code.
	The TFTP request has failed.	See the LRS Reference Manual for TFTP troubleshooting information.
	The flash needs to be replaced.	Contact your dealer or Lantronix Technical Support for assistance.
File server *xxxxxx* not found	The NetWare boot has failed.	Make sure that the LRS is using the proper fileserver name, and that the fileserver is running properly. Both devices must be on the same network.
File not found	NetWare or TFTP could not locate the appropriate boot file.	Make sure that the LRS is using the complete and correct loadfile pathname, including the drive name. Verify that the loadfile is in the login directory and is world-readable.

NOTE: *See Appendix A for Lantronix contact information.*

D.2 BOOTP Troubleshooting

BOOTP failure does not disable the unit from booting. If the BOOTP request fails and you have configured your host to respond to the request, there are a few areas you can check quickly:

- BOOTP must be an uncommented line in the **/etc/services** file as a real TCP / IP service.
- The LRS must be in the loadhost's **/etc/hosts/** file for the host to answer a BOOTP or TFTP request.
- The download file must be in the correct directory and be world-readable. Specify the full pathname for the download file in the BOOTP configuration file or, a default pathname may be added to the download filename.
- Some hosts do not allow BOOTP replies across IP networks. Use a host running a different operating system, put the LRS on the same IP network as the host, or some routers allow turning BOOTP gatewaying on.

E - Supported RADIUS Attributes

This appendix lists and explains the RADIUS attributes currently supported by the LRS. The LRS transmits these attributes whenever they are appropriate for the given connection.

LRS users cannot directly specify which attributes the LRS will transmit—this is negotiated for each connection based on the connection type and requirements. For example, CHAP-Challenge packets are only needed for PPP connections that authenticate via CHAP.

E.1 Authentication Attributes

E.1.1 Access-Request

For Access-Request packets, the LRS can transmit the following attributes.

User-Name

User-Password

CHAP-Password Either a User-Password or CHAP-Password will be sent.

CHAP-Challenge

NAS-Identifier The NAS-Identifier is the LRS's name string configured with the **Set/ Define Server Name** command.

NAS-Port

NAS-Port-Type

Service-Type The Service-Type will be either **Login** or **Framed** (PPP / SLIP).

Framed-Protocol When the Service-Type is **Framed** or **Callback-Framed**, this value denotes which of the framed protocols (PPP or SLIP) is being used for the connection.

Calling-Station-ID When Caller-ID is enabled on the port and a phone number is found in the modem's response string, the LRS will report this value.

NOTE: *For more information about Caller-ID, see the Caller-ID section on page 10-12.*

E.1.2 Access-Accept

The LRS interprets reply attributes based on the Service-Type received in the Access-Accept. Supported service types include:

Login The user is connected to a specific host.

Framed A PPP or SLIP connection is started.

Callback-Login The user is disconnected and called back, then connected to a host.

Callback-Framed The user is disconnected and called back, then begins a PPP or SLIP mode connection.

Prompt The user is provided with a command line prompt on the LRS from which it is possible to enter privileged commands.

Table E-1 shows the additional attributes that can be used in Access-Accept packets sent by the RADIUS server. Items marked with plus signs (+) are only valid when the Service-Type is Login or Callback-Login. Items marked with asterisks (*) are only valid when the Service-Type is Framed or Callback-Framed.

Table E-1: Access-Accept Attributes

Attribute	Supported Values (if any)
Framed-Protocol*	PPP SLIP
Framed-IP-Address*	See *Framed-IP-Address*, page E-3
Framed-Routing*	Send Listen Send & Listen None
Filter-ID*	See *Filter-ID*, page E-3
Framed-MTU*	
Framed-Compression*	None Van-Jacobson TCP/IP Header Compression IPX Header Compression
Login-IP-Host+	See *Login-IP-Host*, page E-3
Login-Service+	Telnet Rlogin TCP-Clear (raw TCP connection)
Login-TCP-Port+	
Reply-Message	
Framed-IPX-Network*	
Session-Timeout	
Idle-Timeout	
Framed-AppleTalk-Link*	
Framed-AppleTalk-Network*	

NOTE: *To use both Van-Jacbson TCP/IP header compression and IPX header compression, send the Framed-Compression value twice (once for each type).*

E.1.2.1 Framed-IP-Address

Using this attribute is equivalent to setting the remote address range of a site to "undefined." Two values are available:

- 255.255.255.255 (0xFFFFFFFF) allows the user to choose and IP address
- 255.255.255.254 (0xFFFFFFFE) assigns the user an address from the LRS IP address pool

If an IP address pool is defined for the LRS and the incoming user asks for an address, one will be assigned from the pool. If the user asks for a specific address, the user will be given the address, provided it is available. In the absence of an address pool, the user will be given any address that he requests.

E.1.2.2 Filter-ID

The LRS renames filters by appending suffixes based on the filter type. For example, a filter named "dallas" configured on the LRS will be renamed "dallas.in" (for an incoming filter), "dallas.out" (for an outgoing filter), "dallas.idl" (for an idle timeout filter), and "dallas.st" (for a startup filter).

NOTE: *The maximum filter name length is 12 characters, but should be limited to 8 characters to account for the added suffix.*

To understand how the Filter-ID attribute works, imagine that user **irvine** is trying to make a PPP connection using RADIUS authentication. When the connection is initiated, the LRS starts a copy of the default site.

During the authentication phase, RADIUS looks in NVR for a site that has the same name as the user. If RADIUS finds a match, this site becomes the **base site**. If the LRS does not find a match, RADIUS will use the default site as the base site. RADIUS uses the attributes passed from the RADIUS server during authentication to modify the base site.

If the Filter-ID attribute is present and has the value "irvine," RADIUS examines NVR for a filter named **irvine.in**. If it finds the filter, it uses that filter as the incoming filter for the site. If it doesn't find the filter, the incoming filter from the base site, if any, is used. If no incoming filter is defined for the base site, no incoming filter is used. RADIUS then repeats the process for the other three filter types (outgoing, idle, and startup). As long as RADIUS finds at least one filter matching the Filter-ID value, the connection will succeed.

However, if the Filter-ID attribute is present and no filters are found matching the Filter-ID value, the connection is refused. This prevents a potential security hole created when a user is allowed to connect without the intended restrictions being enforced.

NOTE: *Because startup filters only apply to outgoing sites, which RADIUS doesn't handle, there is no need to define a startup filter for a RADIUS user.*

E.1.2.3 Login-IP-Host

If the Service-Type is Login or Callback-Login and the Login-Ip-Host value is not set or is set to 0.0.0.0, the preferred Telnet host will be used. If the Service-Type is Login or Callback-Login and this value is set to 255.255.255.255, the user will be prompted to enter the name of the host to use for the connection, including normal LRS environment strings. If present, the Login-TCP-Port value will override the user-entered environment.

If Login-Service is Rlogin and the Login-IP-Host value is not set, the LRS makes an Rlogin connection to the preferred Telnet host.

E.2 Accounting Attributes

For all Accounting packets, the LRS transmits Acct-Status-Type (On, Off, Start, or Stop) and the LRS's NAS-Identifier. For individual Accounting-Start and Accounting-Stop packets, the LRS can also transmit the attributes listed in Table E-2.

NOTE: *Items marked with* ***** *are only sent when the Service-Type value is Framed or Call-back-Framed.*

Table E-2: Accounting Packet Attributes

Accounting-Start	**Accounting-Stop**
Acct-Session-ID	Acct-Session-ID
Acct-Delay-Time	Acct-Delay-Time
User-Name	User-Name
NAS-Identifier	NAS-Identifier
NAS-Port	NAS-Port
NAS-Port-Type	Class
Calling-Station-ID	Acct-Input-Octets
Class	Acct-Output-Octets
Service-Type	Acct-Input-Packets*
Framed-Protocol*	Acct-Output-Packets*
Framed-IP-Address*	Acct-Session-Time
Framed-Routing*	Acct-Terminate-Cause (if known)
Filter-ID*	
Framed-MTU*	
Framed-Compression*	
Framed-IPX-Network*	
Framed-AppleTalk-Network*	
Idle-Timeout	
Session-Timeout	

E.3 Examples

The following examples can be used as templates for the public domain Merit RADIUS server available via anonymous FTP at **ftp.merit.edu**. The examples will also work with the public domain Livingston RADIUS server available via anonymous FTP at **ftp.livingston.edu**.

If you are using a different server, please note that the file format for the Merit and Livingston RADIUS servers are of following form:

```
username        check-item1, check-item2, ..., check-itemN
                reply-item1,
                reply-item2,
                ..,
                reply-itemN
```

Check-items are attribute / value pairs that must be received from the authentication client (for example, the LRS) for authentication to occur. Reply-items are attribute / value pairs that will be returned to the client upon authentication. Note that the Merit and Livingston Password attribute may be used to match either User-Password or CHAP-Password.

NOTE: *Please read your RADIUS server's documentation for more information about how to configure your RADIUS server.*

E.3.1 Configuring Basic Authenticated PPP Connections

The following entry allows user **april** to gain access to a LAN via PPP using the IP address 192.0.1.58:

```
april           Password = "fools"
                Service-Type = Framed,
                Framed-Protocol = PPP,
                Framed-IP-Address = 192.0.1.58
```

This user may be authenticated via PPP PAP, PPP CHAP, or via the local mode username and password prompts. If authenticated by the latter, the user will automatically be forced to execute the command **Set PPP** *sitename;* **Logout** where *sitename* is the name of the site dynamically created by the LRS for this user.

NOTE: *All settings in the default site other than the IP address will apply for this user.*

Here is a more complicated example for a dialback PPP user who is not allowed to perform a local mode login:

```
april           Password = "fools", Service-Type = Framed, Framed-Protocol = PPP
                Service-Type = Callback-Framed,
                Framed-Protocol = PPP,
                Framed-IP-Address = 192.0.1.233,
                Callback-Number = "555 1234"
```

E.3.2 Forcing a Telnet Connection to the Preferred Host

The following example shows a local mode user that is forced to Telnet to the LRS's preferred Telnet host:

```
froggy          Password = “ribbit”
                Service-Type = Login
```

The **Telnet; Logout** command is forced as soon as authentication is complete. To force the user to make an Rlogin to connect to the preferred Telnet host, add “Login-IP-Service = Rlogin” to the reply-item list.

E.3.3 Forcing a Telnet Connection to a Specific Port

To force the user to Telnet to a particular port on the specified host, add the Login-IP-Port attribute:

```
froggy          Password = “ribbit”
                Service-Type = Login,
                Login-IP-Host = 192.0.1.155,
                Login-IP-Service = Telnet,
                Login-IP-Port = 1000
```

The **Connect Telnet 192.0.1.155:1000** command is forced as soon as authentication is complete. Remember that if a user connects via PPP and is authenticated by the RADIUS server with Service-Type set to Login or Prompt, the LRS RADIUS client code will reject the user because a user cannot be made to fall out of PPP mode into local (character) mode.

E.3.4 Preventing RADIUS Authentication

You may wish to prevent the user from being authenticated by the RADIUS server in the first place. If so, enter the following:

```
froggy          Password = “ribbit”, Service-Type = Login
                Service-Type = Login,
                Login-IP-Host = 192.0.1.88,
                Login-IP-Service = Telnet,
                Login-IP-Port = 1000
```

In this case, if the LRS sends an authentication request for the user froggy with the Service-Type set to Framed, the authentication request will be rejected by the RADIUS server.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors which may appear in this guide.

DEC, thickwire, thinwire, VMS, VT100, and ULTRIX are trademarks of Digital Equipment Corporation. UNIX is a registered trademark of AT&T. Ethernet is a trademark of XEROX. NetWare is a trademark of Novell Corp. AppleTalk, Chooser, and Macintosh are trademarks of Apple Computer Corp. Windows NT and Windows for Workgroups are trademarks of Microsoft Corporation. Security Dynamics and SecurID are registered trademarks and PASSCODE, PINPAD and ACE/Server are trademarks of Security Dynamics Technologies Inc.

The revision date for this manual is January 11, 1997.

Part Number: 900-072
Rev. B

WARNING

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against such interference when operating in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with this guide, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause interference in which case the user, at his or her own expense, will be required to take whatever measures may be required to correct the interference.

Warning: Changes or modifications to this device not explicitly approved by Lantronix will void the user's authority to operate this device.

Cet appareil doit se soumettre avec la section 15 des statuts et règlements de FCC. Le fonctionnement est subjecté aux conditions suivantes:

(1) Cet appareil ne doit pas causer une interférence malfaisante.

(2) Cet appareil doît accepter n'importé quelle interférence reìue qui peut causer une opération indésirable.