System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

Terminal Servers LX Series

NOVEMBER 2016

MN003365A01-A

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a particular system, or may be dependent upon the characteristics of a particular mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003365A01-A	Original release of the *Terminal Servers LX Series* manual	November 2016

This page intentionally left blank.

Contents

List of Figures

This page intentionally left blank.

List of Tables

List of Processes

This page intentionally left blank.

List of Procedures

About Terminal Servers LX Series

This manual provides an introduction to the hardware and software components associated with the LX-4008, 4016, and 4048 S and T series terminal servers. Included are detailed procedures for installation, configuration, and troubleshooting. This booklet is intended to be used by field service managers and field service technicians.

What is Covered In This Manual

This manual contains the following chapters:

- Terminal Server Hardware Description on page 23 provides a high-level description of the terminal server and the function it serves on your system.
- Terminal Server Theory of Operations on page 31 explains how the terminal server works in the context of your system.
- Terminal Server Installation on page 35 details the installation procedures relating to the terminal server.
- Terminal Server Configuration on page 43 details the configuration procedures relating to the terminal server.
- Terminal Server Optimization on page 45 contains the optimization procedures and recommended settings relating to the terminal server.
- Terminal Server Operation on page 47 details the tasks that you perform once the terminal server is installed and operational on your system.
- Terminal Server Maintenance on page 65 describes the periodic maintenance procedures relating to the terminal server.
- Terminal Server Troubleshooting on page 67 provides the fault management and troubleshooting information relating to the terminal server.
- Terminal Server FRU/FRE Procedures on page 71 lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs). It also includes replacement procedures applicable to the terminal server.
- Terminal Server Reference on page 73 contains supplemental reference information relating to the terminal server.
- Terminal Server LX Series Disaster Recovery on page 77 provides references and information that will enable you to recover a terminal server in the event of a failure.
- Configuring the Paradyne Modem on page 83 contains information on configuring the Paradyne COMSPHERE 3810 (V.32), Paradyne COMSPHERE 3810 Plus (V.34), or Paradyne 3920 modem for remote analog access (or out-of-band management at the Demilitarized Zone (DMZ) switch).
- Configuring the Raymar Modem on page 93 contains information on configuring the Raymar V. 3600 Series Modem.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

Refer to the following documents for associated information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This may be purchased on CD **9880384V83** by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Master Site Infrastructure Reference Guide	Covers site-level information required to install and maintain equipment at the ASTRO® 25 system master sites.
Securing Protocols with SSH	Provides information on the implementation and management of the Secure Shell (SSH) protocol for secure transmission of data between devices in ASTRO® 25 systems, including configuration sequences that minimize downtime when adding this feature to a system that is already in operation.
SNMPv3	Provides information relating to the implementation and management of the SNMPv3 protocol in ASTRO® 25 systems.
System LAN Switches	Provides use of Hewlett-Packard (HP) switches in ASTRO® 25 systems, including LAN switches and backhaul switches. In addition to common procedures for installation, configuration, operation, and troubleshooting of the switches, this manual provides information for specific ASTRO® 25 system sites and features that HP switches can support.
Unified Event Manager	Covers the use of Unified Event Manager (UEM) that provides reliable fault management services for devices in ASTRO® 25 systems.
Unified Network Configurator	Covers the use of Unified Network Configurator (UNC), a sophisticated network configuration tool that provides controlled and validated configuration management for system devices including routers, LAN switches, site controllers, and base radios, and is used to set up sites for ASTRO® 25 systems. UNC has two components: VoyenceControl and Unified Network Configurator Wizards (UNCWs).
Virtual Management Server Software	Provides procedures for implementing and managing VMware ESXi-based virtual server hosts on the common Hewlett-Packard hardware platform in ASTRO® 25 systems.

Chapter 1

Terminal Server Hardware Description

This chapter provides a high-level description of the terminal server and the function it serves on your system.

1.1 Terminal Server LX Series Overview

The terminal server supports a Network Management (NM) connection to servers and network transport equipment in the zone. Up to three types of terminal servers may be used. An 8-port, a 16-port, or a 48-port terminal server is installed in the Zone Core to manage various devices. The terminal server provides serial connection to all the managed devices, and Ethernet access by NM clients. A 16-port server is used in systems with Master Site which does not support Multi-Zone Capable configurations. A 48-port server is used in systems with Master Site which supports multiple zones, even though it may consist of only one zone. For more information on Single Zone and Multi-Zone Capable configurations, see “Master Site Architectures” in the *Master Site Infrastructure Reference Guide* manual.

PC clients operating on the Local Area Network (LAN) can connect to the terminal server and access devices from the programmed menu of devices. The terminal server can also be connected to an external modem to allow dial-up access across the Public Switched Telephone Network (PSTN).

The LX-4048, the LX-4016, and the LX-4008 are the three latest terminal server models.

LX-4048:

- 48 ports
- Used for out-of-band management
- Used in the following configurations:
  - One at the Zone Core for M2 systems, if the capacity of an LX-4016 is exceeded
  - One-to-two at the Zone Core for M3 systems, depending on the capacity needs
  - One at the Prime Site
  - One at the Conventional Hub

LX-4016:

- 16 ports
- Used for out-of-band management
- One at the Zone Core for L core and M1 systems
- One at the Zone Core for M2 systems, if the capacity of the LX-4016 is NOT exceeded

LX-4008:

- 8 ports
- Used for Remote Analog Access by PC clients
- Maximum of two LX-4008 used in the Zone Core

1.2

Terminal Servers in the ASTRO 25 System

The diagrams below show terminal servers in various ASTRO® 25 system configurations. In all cases, the terminal server has a direct RS-232 connection to each device.
The devices supported in your system may vary, depending on your system configuration.

For information on where all the VMs reside on the various VMS hosts in the system, see the “Virtual Machine Combinations” appendix in the *Virtual Management Server Software* manual.

Terminal Servers in the Single Zone Non-Redundant Configuration

The diagrams below show the devices that are typically connected and accessible to the remote terminal server in the Single Zone Non-Redundant configuration.

Figure 1: Terminal Server Connections at the Core Site – L1 Single Zone Non-Redundant Configuration

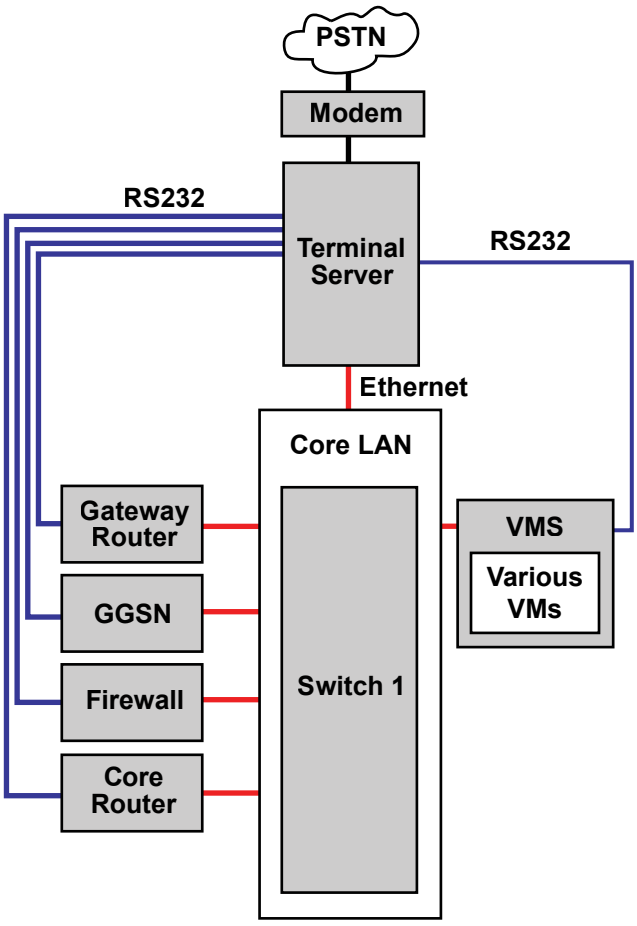
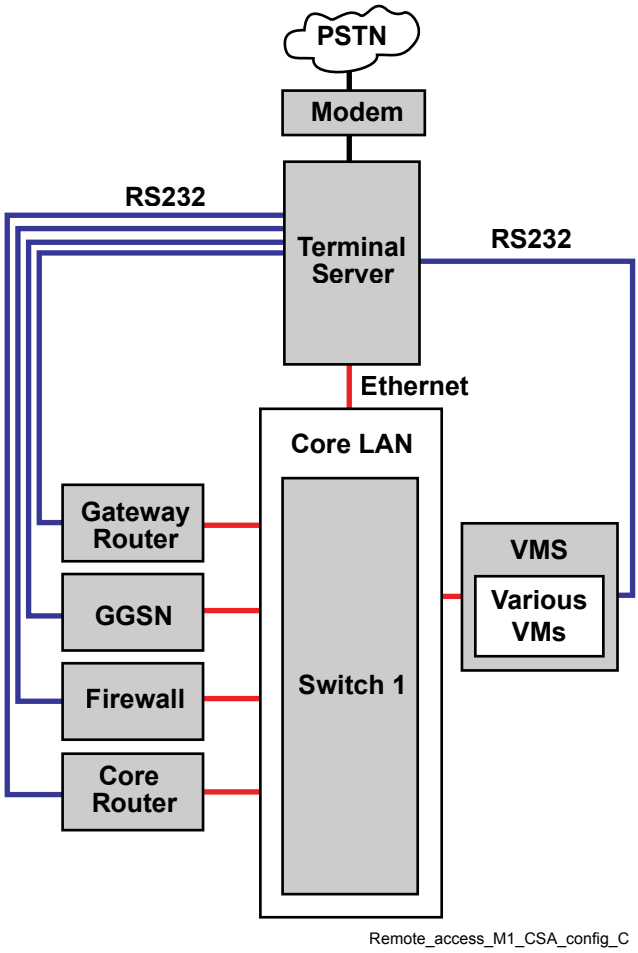


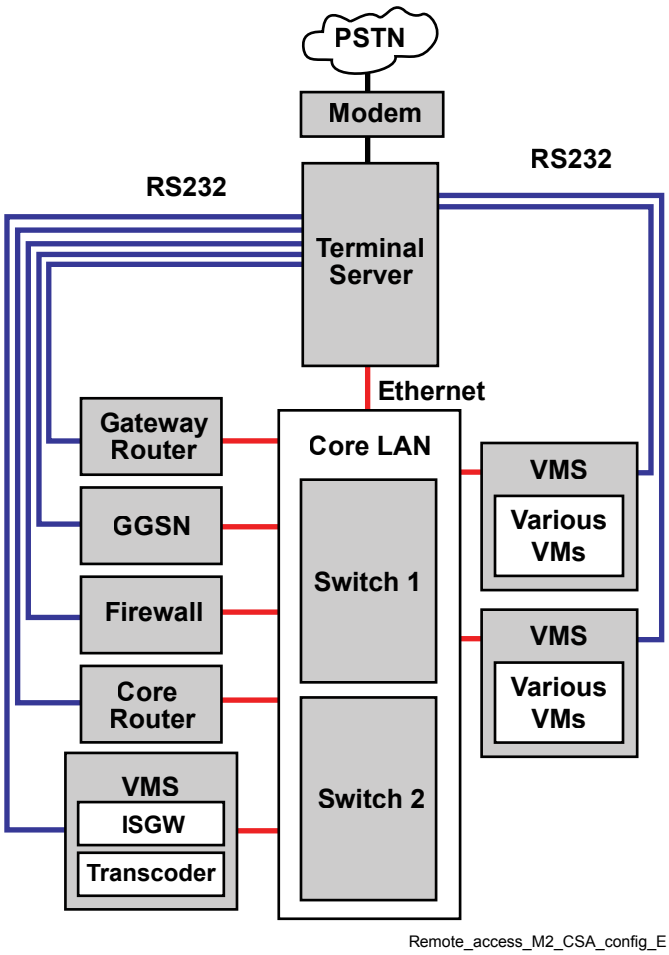
Figure 2: Terminal Server Connections at the Core Site – M1 Single Zone Non-Redundant Configuration



Terminal Server in the Single Zone Redundant Configuration

The diagram below shows the devices that are typically connected and accessible to the remote terminal server in the Single Zone Redundant configuration.

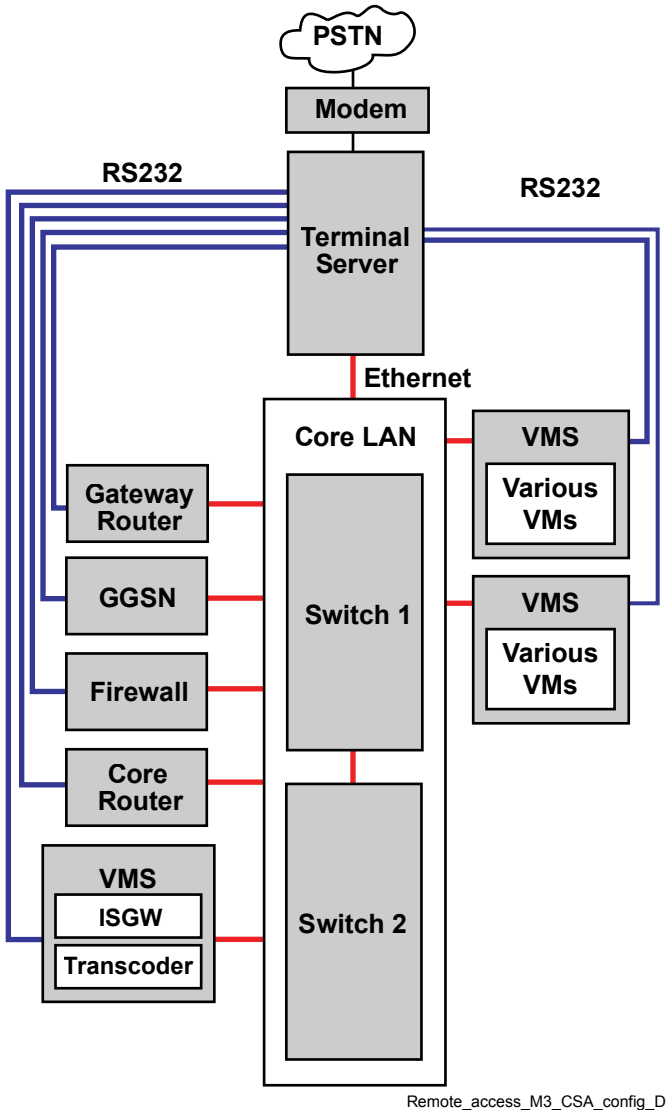
Figure 3: Terminal Server Connections at the Core Site – M2 Single Zone Redundant Configuration



Terminal Server in the Multi-Zone Configuration

The diagram below shows the devices that are typically connected and accessible to the remote terminal server in the Multi-Zone Capable configuration.

Figure 4: Terminal Server Connections at Core Site – M3 Multi-Zone Capable Configuration



1.3

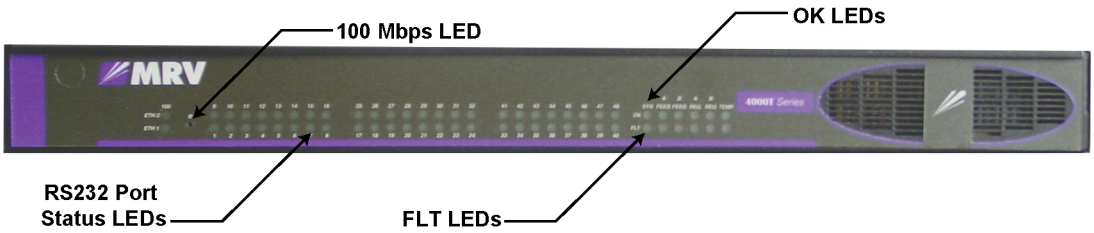
Terminal Server (48-Port) – Front/Rear Views

NOTICE: The T Series Terminal Servers are shown, your model may vary slightly.

This section describes the front view of a 48-Port Terminal Server (LX-4048T). The front panel includes the following features:

- Operating LEDs
- 100 Mbps link LED
- RS-232 port status LEDs (1–48)

Figure 5: LX-4048T Terminal Server Front View



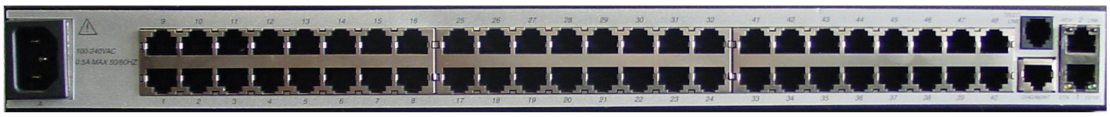
Terminal_Server_48port_front_w_callouts

The 48-port terminal server includes three operational LEDs and 48 port status LEDs. For descriptions of the LED indications, see Terminal Server LED Indications on page 73.

This section describes the rear view of a 48-port Terminal Server. The rear panel includes the following features:

- 120 V power connector
- 48 RS-232 serial ports (RJ45)
- Two 10/100Base-T ports (RJ45) with a link and receive LEDs
- Diagnostic port (RJ45)
- Built-in modem port (RJ-11)

Figure 6: LX-4048T Terminal Server Rear View



Terminal_server_48port_rear

NOTICE: Also, see Cable Connections for the Terminal Server on page 35.

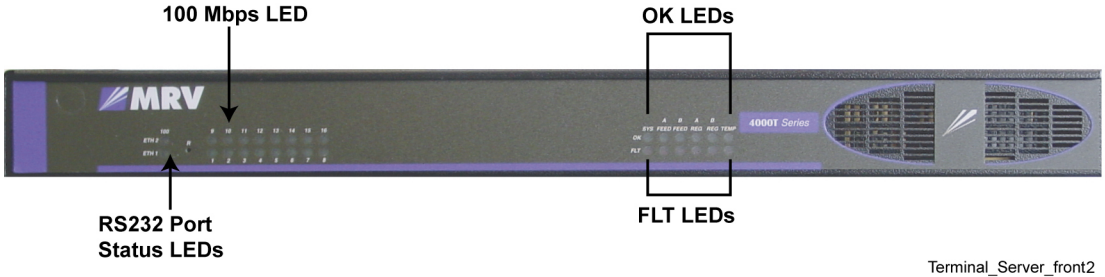
1.4 Terminal Server (16-Port) – Front/Rear Views

NOTICE: The T Series Terminal Servers are shown, your model may vary slightly.

This section describes the front view of a 16-Port Terminal Server (LX-4016T). The front panel includes the following features:

- Operating LEDs
- 100 Mbps link LED
- RS-232 port status LEDs (1–16)

Figure 7: LX-4016T Terminal Server Front View



The 16-port terminal server includes three operational LEDs and 16 port status LEDs. For descriptions of the LED indications, see Terminal Server LED Indications on page 73.

This section describes the rear view of a 16-port Terminal Server. The rear panel includes the following features:

- 120 V power connector
- 16 RS-232 serial ports (RJ45)
- Two 10/100Base-T port (RJ45) with a link and receive LEDs
- Built-in modem port (RJ-11)
- Diagnostic port (RJ45)

Figure 8: LX-4016T Terminal Server Rear View

1.5 Terminal Server (8-Port) – Front/Rear Views

NOTICE: The T Series Terminal Servers are shown, your model may vary slightly.

This section describes the front view of an 8-Port Terminal Server (LX-4008T). The front panel includes the following features:

- RS-232 Port status LEDs (1–8)
- Operating LEDs

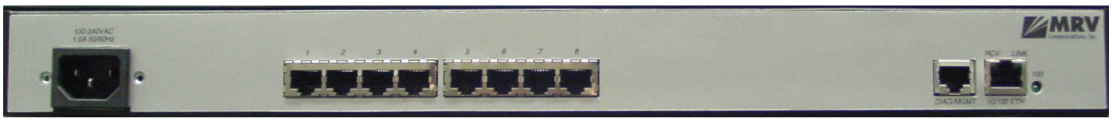
Figure 9: LX-4008T Terminal Server Front View

The 8-port terminal server includes two operational LEDs and eight port status LEDs. For descriptions of the LED indications, see Terminal Server LED Indications on page 73.

This section describes the rear view of an 8-Port Terminal Server. The rear panel includes the following features:

- 120 V Power Connector
- Eight RS-232 serial ports (RJ45)
- One 10/100Base-T port (RJ45) with a link and receive LEDs
- Diagnostic port (RJ45)
- 100 Mbps link LED

Figure 10: LX-4008T Terminal Server Rear View



terminal_server_LX4008_rear

NOTICE: Also, see Cable Connections for the Terminal Server on page 35.

1.6

Terminal Server Technical Specifications

This section lists the technical specifications of the terminal server.

Table 1: Technical Specifications

Specification	Description
Power Specifications	120 VAC - 240 VAC, 50/60 Hz
RS-232 Speeds	34.5 bps – 230 Kbps
Ethernet Interface	10/100 Mbps Auto Sensing
Operating Temperature	0 °C to +40 °C (32 °F to +104 °F)

Chapter 2

Terminal Server Theory of Operations

This chapter explains how the terminal server works in the context of your system.

2.1
Reasons for Using the Terminal Server

The remote terminal server includes several benefits that are not available through a direct telnet connection to a device, such as:

- If you establish a Telnet session directly with a device and fail to log out of the device, you can be locked out of the device and may need to reset the device. In such case, call Motorola Solutions Solution Support Center (SSC).
- A terminal server session can time out, while a direct telnet session with a device does not. Timing out of a session prevents unauthorized access to your devices.
- If you are running telnet sessions directly to a device, a trail of the individual connections can be viewed in the telnet program or the Run dialog box in Windows. Using the terminal server prevents individual connection information (other than the terminal server itself) from being exposed to other people accessing the client.

NOTICE: Terminal Server is available optionally for ASTRO® 25 Express Plus systems.

2.2
Types of Terminal Server Configurations

This section provides the functional configurations of the terminal server.

Table 2: Types of Configurations

Model	Purpose
LX-4048 (48 ports)	Out-of-band management at the master site, Simulcast prime site, and the Conventional Hub
LX-4016 (16 ports)	Out-of-band management at the master site in single zone (both redundant and non-redundant) and Conventional Sub-system configurations.
LX-4008 (8 ports)	Remote Analog Access (also known as Analog Remote Access) or out-of-band management at the Demilitarized Zone (DMZ) Switch

NOTICE: When used to support remote analog access, the terminal server is referred to as the Remote Access Server (RAS). When used to support out-of-band management, the terminal server is referred to as the Out-of-Band Management server.

2.2.1
Out-of-Band Management

Out-of-band management provides serial access to network devices through the console ports for maintenance purposes. The configuration consists of a set of modems and one terminal server, either

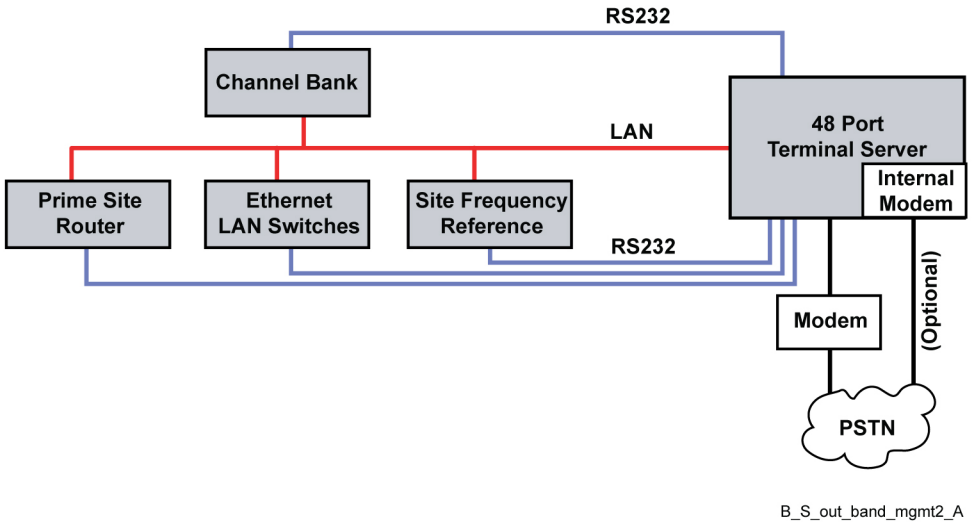
with 48 or 16 ports. Use a 48-port server in configurations with Master Site capable of supporting multiple zones or M2 systems. It is possible to use a 48–port server in a system with only one zone, where the Master Site is Multi-zone Capable. Use a 16-port server in Single Zone Configurations, both Redundant and Non-Redundant, where Master Site is not equipped for multiple zones. The modems allow you to dial into the terminal server connected to the master site LAN. Telnet is supported, as well as connectivity to the serial ports of the routers, switches, servers, and other system equipment. Failure of the terminal server or its links results in loss of the ability to access system devices remotely.

Out-of-band management can be implemented at a master site and a Simulcast prime site (or at the DMZ Switch with the 8-port server), and a Conventional Hub. For the type of terminal server used, see the diagram below.

NOTICE: The model numbers for the terminal servers are the same for both the 115 VAC and the 240 VAC power supply version.

The terminal server is used for out-of-band management at a Simulcast Prime Site or a Conventional Hub to provide serial access to various site components.

Figure 11: Remote Terminal Server Connections — Simulcast Prime Site Implementation



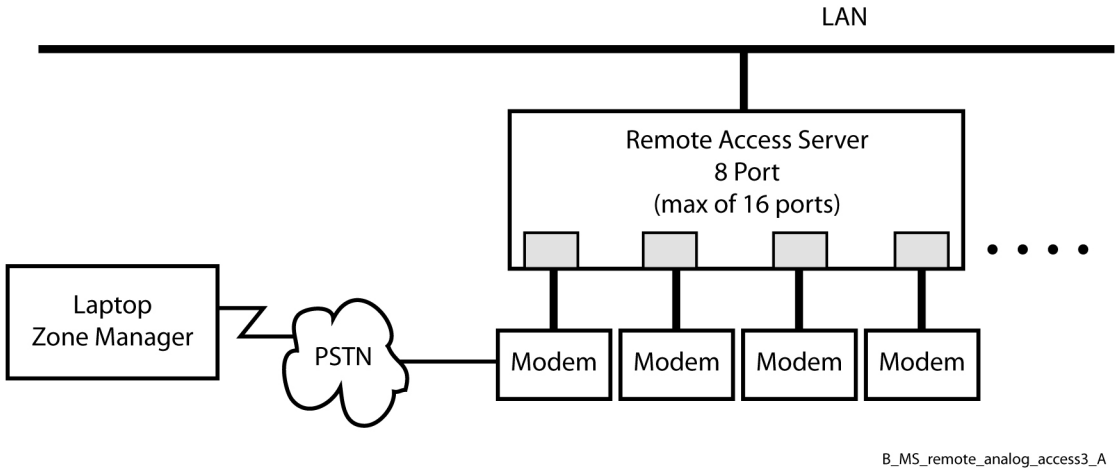
2.2.2
Remote Analog Access

Analog remote access provides network connectivity from a dial-up phone line. The device providing remote analog access for a system is an 8-port Remote Access Server (RAS). You can dial into the network from a properly configured PC, and:

- run NM applications remotely
- make configuration changes
- perform fault management

The Ethernet port of the RAS connects to the Ethernet LAN for remote analog access. Up to 16 ports of analog access are supported. Failure of the terminal server or its links results in loss of the remote dial-up capability.

Figure 12: Remote Analog Access System Diagram – 8-port RAS

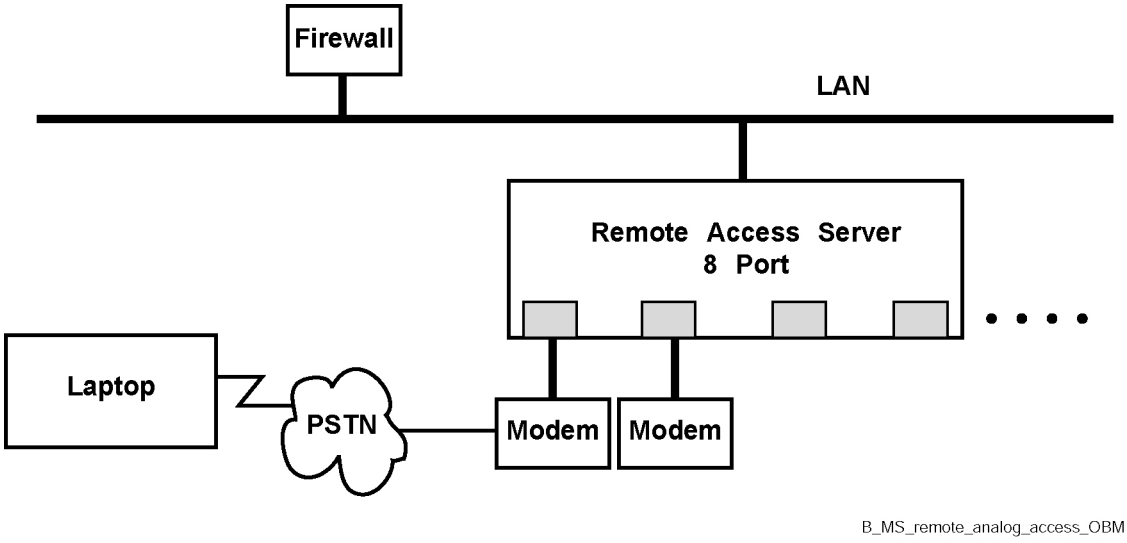


NOTICE: A maximum of two terminal servers can be connected for remote analog access, providing up to 16 ports.

2.2.3
Out-of-Band Management at the DMZ Switch

Out-of-Band Management (OOB) provides access to the Radio Network Interface (RNI) devices at the Demilitarized Zone (DMZ) Switch through a dial-in session through a Virtual Private Network (VPN). The device providing access is an 8-port terminal server. Its configuration, software, and hardware are identical to the 8-port terminal servers used for Remote Analog Access.

Figure 13: Out-of-Band Management Using Terminal Server at DMZ Switch



This page intentionally left blank.

Chapter 3

Terminal Server Installation

This chapter details the installation procedures relating to the terminal server.

3.1 Installing the Terminal Server in a Rack

The terminal server is rack-mounted, for detailed physical installation information, see LX-4000T Series Quick Start Guide (451-0340E) from MRV Communications, Inc.

Prerequisites: Please, see Required Tools and Equipment on page 71

Procedure:

1. Slide the chassis onto the rack.
2. Attach the chassis to the rack with equipment rack screws.

3.2 Cable Connections for the Terminal Server

CAUTION: Use only Category 5 Shielded Twisted Pair or higher cabling and connectors. Motorola Solutions has engineered this system to meet specific performance requirements. Using other cabling and connectors may result in unpredictable system performance or catastrophic failure!

This section lists the terminal server connections. These connections are common to LX-4008, LX-4016, and LX-4048 models.

Table 3: Terminal Server Connections

Connection	Port Type	Description
RS-232 Connections	RJ45	The terminal server supports either 8, 16, or 48 RS-232 ports on the rear side of the chassis. They provide the serial network management connections to the supported devices in the network. **NOTICE:** The 48 RS-232 ports on the LX-4048, or the 16 RS-232 ports on the LX-4016 are used for serial network management. The eight RS-232 ports on the LX-4008 are connected to an external modem for remote analog access or out-of-band management at the Demilitarized Zone (DMZ) switch.
10/100Base-T Ethernet Connection	RJ45	The terminal server provides a 10/100Base-T Ethernet connection to the master site LAN switch. The connection supports all traffic and interfaces for PC clients on the LAN.
Telco Line Connection	RJ-11	The telco line connection provides a V.90/K56flex 56 Kbps modem connection for inbound dial-up access through the

Table continued…

Connection	Port Type	Description
		Public Switched Telephone Network (PSTN). It connects to a regular RJ-11 telephone line. **NOTICE:** The Telco Line connector is available in LX-4048 and LX-4016.
DIAG/MGMT Connection	RJ45	The DIAG/MGMT connection provides local management of the system and the ability to diagnose faults in a failure.
Power Connection	120 V power connector	The standard terminal server accepts a 110/220 VAC input.

3.2.1 Terminal Server Power Connections

The female connector of the power cable connects to the back of the terminal server unit. The male connector of the power cable plugs into a standard 120 V power outlet.

3.3 Out-of-Band Management Connections

With out-of-band management, a second path is available to the managed devices that do not depend on the LAN/WAN. The terminal server has a direct RS-232 connection to each device.

This section explains how to connect to various devices for out-of-band management.

3.3.1 Connecting to the Ethernet LAN Switch

The terminal server's Ethernet port connects to the Ethernet LAN switch for out-of-band management.

See “Destination Device Abbreviation Examples in Port Names and Labels” in the *System LAN Switches* manual for details.

3.3.2 Connecting to PSTN with Internal Modem

The V.90/K56flex internal modem can be used for out-of-band management access. Connect the telephone cable to the Telco Line port on the LX-4048 or the LX-4016 terminal server (if the internal modem is present on the terminal server).

3.3.3 Connecting to External Modem

The Paradyne 3810 Plus or 3920 Plus modem can be used for remote out-of-band management access. Connect the serial port of the modem to serial port 1 on the Terminal Server.

For information on modem configurations, see Configuring the Paradyne Modem on page 83.

3.3.4 Connecting to Terminal Device for Diagnostics

The DIAG port logs system messages during boot-up. You can also use the DIAG port to manage and configure the server once it has booted. The DIAG port is located at the rear of the terminal server unit. The cable used to connect the terminal to the DIAG port is a serial cable provided with the terminal server.

3.3.5
Out-of-Band Management Terminal Server Cabling and Pinout Connections

Cables used to connect a device console port to the terminal server's serial ports vary for each device. The terminal server serial ports are all RJ45 ports. The pinouts required for each device type are listed in Terminal Server and Console Port Interface Cable Pin-outs on page 74.

3.3.6
Identifying LX Series Port Assignments for Network Devices

See Showing Port Layout File on page 55 to obtain port assignment information for network devices connected to the terminal server.

3.4
Remote Analog Access Connections

Remote analog access provides network connectivity from a dial-up phone line.

NOTICE: The connections used for remote analog access can also be used for out-of-band management at the Demilitarized Zone (DMZ) switch.

3.4.1
Connecting Remote Access Terminal Server to Ethernet LAN for Remote Analog Access

The Remote Access Server's Ethernet port connects to the Ethernet LAN for remote analog access.

See “Destination Device Abbreviation Examples in Port Names and Labels” in the *System LAN Switches* manual for details.

3.4.2
Connecting Remote Access Terminal Server to External Modem

The Paradyne 3810 Plus and 3920 Plus modem is used for remote access. Connect the serial port of the modem to a serial port on the Remote Access Server (RAS).

For information on modem configurations, see Configuring the Paradyne Modem on page 83.

3.4.3
Connecting Remote Access Terminal Server for Diagnostics

The DIAG logs system messages during boot-up. Once the system starts, you can also use the DIAG port to manage and configure the server. The DIAG port is located at the rear of the terminal server unit.

The cable used to connect the terminal to the DIAG port is a serial cable provided with the terminal server.

3.5
Common Setup for all LX-4000 Models

The LX-4008, LX-4016, and LX-4048 servers are configured for user ID and password authentication on the ports that connect to the modem for dial-in. If the user ID and password combination is incorrect, you are not able to log in to the LX terminal server. The user ID and password are configured

by system engineers at the staging center for your system. Contact your system administrator for the correct user ID and password.

Pull the terminal server OS files using Unified Network Configurator to archive them. Stored OS versions are used when a replacement terminal server has to have its OS changed.

NOTICE: For the details about pulling configurations, see the “Pulling the Configuration for a Single Device” section in the *Unified Network Configurator* manual.

3.5.1
Setting Up a Laptop/PC for Diagnostic Management

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Connect the DB9 modular adapter and the RJ–45 cable to the serial port of a laptop/PC. Connect the other end of the cable to the DIAG port of the terminal server. (The DIAG port is at the rear of the terminal server unit.)
2. Launch a terminal emulator (for example, HyperTerminal or ProComm) on the laptop/PC with the following settings:
   - Data rate: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow control: Xon/Xoff
3. Press ENTER twice.

   The session starts.
4. Log in through the DIAG port on the terminal server.

3.5.2
Setting Up a Laptop or PC for Out-of-Band Management

Use either HyperTerminal or ProComm Terminal Emulator for Out-of-Band Management.

Procedure:

1. Provide the required information regarding your location, such as your country or region and any special phone dialing rules.
2. Verify that the correct phone number is available and the laptop or PC is connected to an analog phone line.

3.5.3
Setting Up a Laptop or PC for Remote Analog Access Dial-up

This procedure explains how to configure dial-up on a laptop or PC with Windows OS. Use a similar procedure for other operating systems.

NOTICE: This procedure also applies to 8-port terminal servers used for Out-of-Band Management at the Demilitarized Zone (DMZ) switch.

Procedure:

1. Click **Start**, search for the **Network and Sharing Center**, and click it.

2 In the **Network and Sharing Center** window, click **Set up a new connection or network**.

3 In the **Set Up a Connection or Network** window, select **Connect to a workplace** and click **Next**.

4 In the **Connect to a Workplace** window, perform the following actions:

   a Click **Dial directly**.

   b In the **Telephone number** field, enter the telephone number.

   c In the **Destination name** field, enter the name for this connection.

   d Leave the **Use a smart card** checkbox unselected.

   e Select the **Don't connect now** checkbox.

   f Click **Next**.

   g In the **User name** field, enter your user name.

   h In the **Password** field, enter your password.

   i Click **Create**.

5 Click **Start**, search for **View network connections**, and click it.

6 In the **Network Connections** window, right-click the dial-up connection that you created and click **Properties**.

7 On the **Options** tab, select only the following options:

   a Select the **Display progress while connecting** checkbox.

   b Select the **Prompt for phone number** checkbox.

   c **Windows 7 only:** For **Redial attempts**, select **3**.

   d **Windows 7 only:** For **Time between redial attempts**, select **1 minute**.

   e For **Idle time before hanging up**, select **never**.

8 On the **Security** tab, select the **Show terminal window** checkbox.

9 Click **OK**.

   The **Properties** window disappears

10 In the **Network Connections** window, right-click the dial-up connection and click **Connect**.

11 Verify that the correct phone number is available, and that the laptop or PC is connected to an analog phone line.

12 In the **Connection** window, click **Dial**.

   A summary of the connection appears, including the following information:

   - Terminal server name
   - Modem port number
   - Dial-speed used

   The system prompts you to enter your login credentials.

3.5.4
Upgrading the OS Version on the Terminal Server

For information on upgrading the OS version automatically, see “Transferring and Installing OS Images for the MRV LX Terminal Server” in the *Unified Network Configurator* manual.

3.5.5

Downgrading the OS Version on the Terminal Server

Downgrading is supported on LX systems with the OS version 4.0.0 or higher.To check the version of OS running on the terminal server, enter the `show version` command after logging in to the system. For information on downgrading the OS version automatically, see the *Unified Network Configurator* manual.

Prerequisites:

1. Obtain the `ppciboot.img` and `linuxito.img` software files for the required downgrade version.
2. Locate the following information:
   - IP address and subnet mask assignments for your system.
   - Login IDs and passwords for your system

   Contact your system administrator or your system IP plan for this information.
3. Obtain the laptop/PC running TFTP server to transfer the software files to the terminal server.
4. Start the TFTP server on the laptop/PC and configure it to point to the location where the software files are located.
5. If the terminal server has been already configured, it is recommended to restore it to factory default.

IMPORTANT: Read the whole procedure before starting, as the task is dependent on timers.

Procedure:

1. Connect the Terminal Server to the laptop through serial connection using the DB-9 Modular adapter and RJ45 cable.
2. Provide the Ethernet connection using the Ethernet crossover cable.
3. Assign an ***<IP address>*** to the laptop.
4. Launch a terminal emulator (for example, HyperTerminal or ProComm) from the laptop/PC with the following settings:
   - Data rate: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow Control: Xon/Xoff
5. Power cycle the Terminal Server and wait for the PPCiBoot login.
6. In the PPCiBoot main menu, type L to log in and enter the ***<PPCiBoot password>*** at the password prompt.
7. Type 3.
8. In the **IP Configuration** menu, select the options to assign the following to the Terminal Server and to the TFTP server:

   a ***<Terminal Server IP address>***

   b ***<TFTP server subnet mask>***

   c ***<TFTP server IP address>***

   where ***<TFTP server IP address>*** is the IP address of the laptop/PC
9. Verify that the ***<Terminal Server IP address>*** and the ***<TFTP server IP address>*** are in the same subnet.

10 Type `s` to save the configuration.

11 Type `r` to return to the main menu screen.

12 Verify that the **Boot from network** field is set to **Network, Flash**.

13 Type `d` to downgrade PPCiBoot.

This operation resets PPCiBoot and brings up the downgrade version at the default settings.

The Terminal Server reboots.

14 At the password prompt, type `L` to log in and enter the ***<PPCiBoot password>***.

NOTICE: If the boot timer has expired, power cycle the Terminal Server.

15 At the PPCiBoot main menu, reconfigure PPCiBoot to load the downgrade version of `linuxito.img` from your TFTP server.

16 Type 3.

17 In the **IP Configuration** menu, select the options to assign the following to the Terminal Server and to the TFTP server:

a ***<Terminal Server IP address>***

b ***<TFTP server subnet mask>***

c ***<TFTP server IP address>***

where ***<TFTP server IP address>*** is the IP address of the laptop/PC

18 Verify that the ***<Terminal Server IP address>*** and the ***<TFTP server IP address>*** are in the same subnet.

19 Type `s` to save the configuration.

20 Type `r` to return to the main menu screen.

21 Verify that the **Boot from network** field is set to **Network, Flash**.

22 Type `f` to change the **Save the software image to flash when boot from network** option to **yes**.

This operation makes the LX load the image from the TFTP server and writes it into flash in the proper location for this version. The Terminal Server reboots and is ready for use.

This page intentionally left blank.

Chapter 4

Terminal Server Configuration

This chapter contains configuration procedures relating to the terminal server.

Configuration of the terminal server is done by Motorola Solutions. Please contact your Motorola Solutions representative if changes to the terminal server configuration are needed.

4.1 Discovering Terminal Server in UEM

Once the terminal server is installed, it must be discovered in the Unified Event Manager (UEM) application. After discovery is complete, terminal server traps are displayed in UEM. See “Discovering Network Elements” and “Discovering Groups of Network Elements” in the *Unified Event Manager* manual for details.

4.2 Configuring the Terminal Server for SNMPv3 Operation

For details on configuring the LX-T Series terminal servers for SNMPv3 operation see the “Terminal Servers Configuration for SNMPv3” section in the *SNMPv3* manual.

4.3 Configuring the Terminal Server in UNC

For additional ways of configuring terminal servers in the Unified Network Configurator (UNC), see the following sections in the *Unified Network Configurator* manual:

- “Rolling Back the Device Configuration to an Archived Version”
- “Configuring the LX-T Terminal Server with a Configlet”

This page intentionally left blank.

Chapter 5

Terminal Server Optimization

This chapter contains optimization procedures and recommended settings relating to the terminal server.

5.1 Optimization Required

The terminal server does not have any specific procedures for optimization.

This page intentionally left blank.

Chapter 6

Terminal Server Operation

This chapter details the tasks that you perform once the terminal server is installed and operational on your system.

6.1 Logging On to the Terminal Servers

The login and fallback operations covered in the Logging On Using Authentication on page 47 section are common to all Terminal Servers. Provide the correct ID and password/passcode to receive authentication.

NOTICE: If you enter the correct ID but the incorrect passcode/password combination three times, you are logged out and cannot log back in even on providing correct ID and password/passcode combination during the fourth try. The system administrator has to reset the RADIUS server before you can attempt to log on again.

6.2 Logging On Using Authentication

To log in to the terminal server, authenticate using a correct ID and password. Contact your system administrator for the correct ID and password.

Authentication can be accomplished by following Logging On Using RADIUS Authentication on page 47 — managed by the Domain Controller (DC).

NOTICE: See Setting Up a Laptop or PC for Out-of-Band Management on page 38 or Setting Up a Laptop or PC for Remote Analog Access Dial-up on page 38 to dial in to the terminal server with a laptop computer and modem.

6.2.1 Logging On Using RADIUS Authentication

RADIUS authentication occurs through a series of communications between the LX and the RADIUS server, which is located in the Domain Controller (DC). Once RADIUS has authenticated a user, the LX terminal server provides you with access to the appropriate network services.

Prerequisites:
Locate the account logins and passwords for your system before performing this procedure. Contact your system administrator for this information.

Ensure that the **serviceuser** account is enabled on the Domain Controller. See “Enabling User Accounts in Active Directory” in the *Authentication Services* manual.

Procedure:

1. Dial in to the terminal server.

   The login prompt appears along with a message displaying the terminal server information, modem port number, and dial-speed.

```
z001 term001 Remote Access Terminal Server
```

```
Port 49      Speed 57600
Login:
```

NOTICE: This message varies based on your system's terminal server configuration, modem port number, and the dial-speed used.

2 Log on using the correct user ID and password.

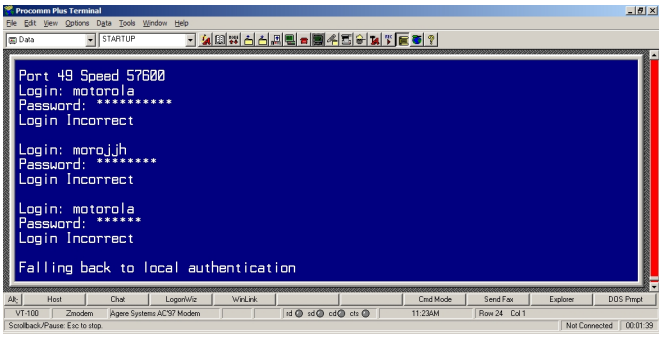
Once the user ID and password combination is authenticated by the RADIUS server, the appropriate menu appears and you can proceed with your tasks.

6.2.2
Fallback Authentication

If primary authentication by RADIUS fails, fallback authentication is used. If both primary and fallback authentication fails, the user must verify their RADIUS credentials and the local terminal server account credentials and try again. This precaution is so the system administrator can log in to the terminal server in case primary authentication fails. Such situation may occur due to the RADIUS server not being available on the network.

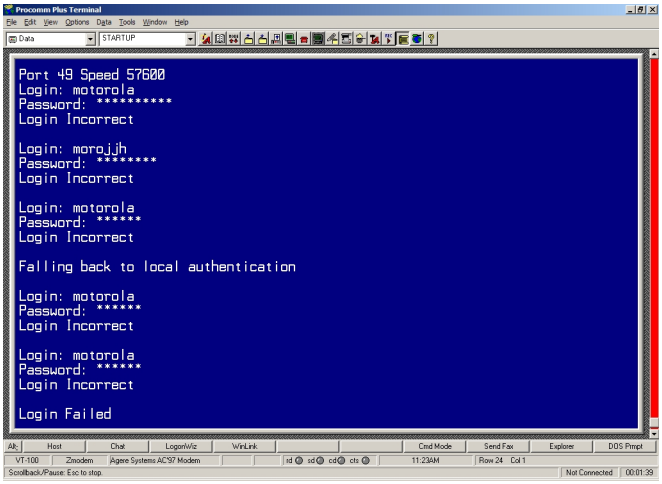
The system uses fallback authentication after three unsuccessful attempts. For each of the three attempts, the `Login` and `Enter Password` prompts appear. After the last failed attempt, the `Login Incorrect` message appears and the system falls back to local authentication.

Figure 14: Fallback Authentication Example



You have two attempts to authenticate using local authentication. If authentication was not successful, the error message `Login Incorrect` appears. After the last failed attempt, an additional message `Login Failed` appears.

Figure 15: Failed Local Authentication



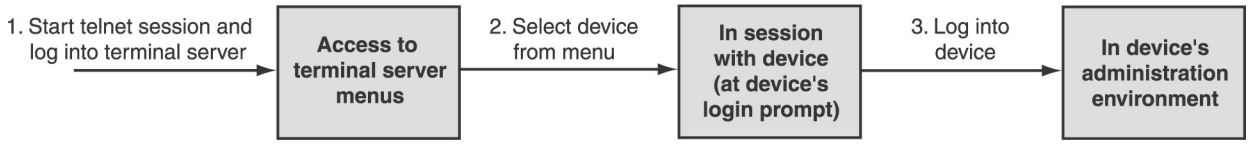
If authentication using the fallback authentication method is successful, the terminal server menu appears.

6.3

Accessing the Out-of-Band Management Terminal Server

The remote terminal server is the access point for all administration with the network management server applications, zone controllers, and other IP devices in the zone. When administrating a device, first connect with the terminal server. Then select the device from the terminal server menus to establish a session with the device. Finally log on to the administration menu of the individual device to manage it. Accessing a device is a three-step process.

Figure 16: Accessing a Device Through the Terminal Server

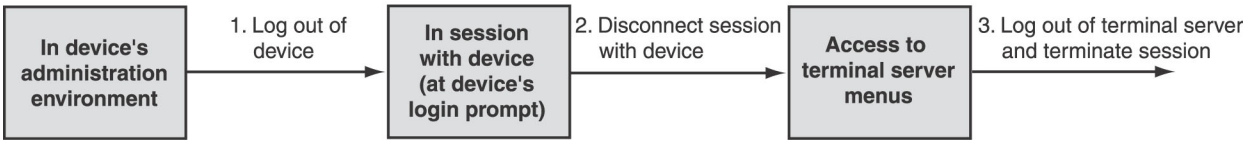


After administrating a device, first log out of the device's administration menu and then disconnect the session with the device.

To exit the terminal server, log out of all device administration environments and disconnect all device sessions. Then log out and disconnect your telnet session with the terminal server.

NOTICE: Telnet is used as an example only. You may dial into a terminal server using a remote laptop/PC and appropriate communication software.

Figure 17: Disconnecting Devices and Logging Out of the Remote Terminal Server



NOTICE:

- These servers are based on nearly identical hardware and share nearly identical procedures for most tasks.
- A maximum of ten sessions can be maintained at a time on your Out-of-Band Management Terminal Server.

6.3.1

Out-of-Band Management Terminal Server Menu Command Keys

This section lists command keys that are used to navigate through the terminal server menus or perform different functions. Several of these commands are used in other terminal server procedures.

Table 4: Remote Terminal Server Commands

Command	Description	When Available
CTRL+F	Moves forward to the next session.	At any time (either within the terminal server menu system or in a session with another device)
CTRL+B	Moves back to the previous session.	At any time (either within the terminal server menu system or in a session with another device)

Table continued…

Command	Description	When Available
CTRL+L	Takes you back to the Local Command Mode.	Move to the originating session (Sess 0), if there is more than one session launched from the menu.
CTRL+Z	Displays the exit prompt.	
SHIFT+Q	Logs out and terminates the session with the terminal server.	Only in the Terminal Server nested menu configuration
SHIFT+R	Refreshes the screen.	
SHIFT+T	Displays the main menu of the terminal server.	
SHIFT+U	Moves to one level up menu.	

6.3.2
Navigating through the Menus in Out-of-Band Management

The terminal server menu in Out-of-Band Management varies depending on where it is connected in the system.

6.3.2.1
Navigating the Menu at the Zone Core

This section describes how to access menu options on the Out-of-Band terminal server at the zone core.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Connect to the terminal device using a terminal display application.
2. At the login prompt, log on using the correct user ID and password.
3. Perform one of the following actions:
   - If the main menu appears, go to step 4.
   - If the CLI appears, enter: `menu`
4. From the main menu, select the required option.

```
 Menu 1 Main Menu
 1 Maintenance Access
 2 Telnet Session to Host
 3 Show users
 4 Ping to user entered IP address
 5 Show logfile
 6 Set Up PPP — Using Windows Dial Up Client
 7 Show port layout file
 8 Router Menu
 9 Switch Menu
10 ZC/Unix Server Menu
11 Data Subsystem Menu
12 Secure Subsystem Menu
13 Channel Bank Menu
14 Misc Device Menu
```

```
Up One Level: U      Top of Menu: T      Refresh: R      Logout: Q
Enter Number of Selection and Press <RETURN> to Continue:
```

NOTICE: Menu options may vary based on your system configuration.

See Using Terminal Server Menu Utilities on page 53 for procedures to access some of the menu options.

6.3.2.2

Navigating the Menu at the Simulcast Prime Site

This section describes how to access the menu options on the Out-of-Band terminal server at the Simulcast Prime Site.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Connect to the terminal device using a terminal display application.
2. At the login prompt, log on using the correct user ID and password.
3. Perform one of the following actions:
   - If the main menu appears, go to step 4.
   - If the CLI appears, enter: `menu`
4. From the main menu, select the required option:

```
 Menu 1 Main Menu
 1 Maintenance Access
 2 Telnet Session to Host
 3 Show users
 4 Ping to user entered IP address
 5 Show logfile
 6 Set Up PPP — Using Windows Dial Up Client
 7 Show port layout file
 8 Router Menu
 9 Switch Menu
10 Simulcast Device Menu
11 Channel Bank Menu
12 Misc Device Menu

Up One Level: U      Top of Menu: T      Refresh: R      Logout: Q
Enter Number of Selection and Press <RETURN> to Continue:
```

NOTICE: The menu options may vary depending on your system configuration.

See Using Terminal Server Menu Utilities on page 53 for procedures you can use to access some of the menu options.

6.3.3

Using the Out-of-Band Management Terminal Server to Access a Device

Once you have logged on to the terminal server and reached the main menu, use this procedure to access devices in the zone.

Prerequisites: Before performing this procedure, contact your system administrator for the correct ID and password for the device you would like to access.

Procedure:

1. At the main menu of the terminal server, select the device category you want to access.

   The submenu for that category appears, showing a list of devices.

2. At the submenu prompt, select the appropriate device from the list.

   NOTICE: Devices can only accept one session at a time. Other users cannot access the device until your session is closed.

   A connection is established with the selected device.

3. Log on and administrate the device according to the instructions for the device.

   NOTICE: See the appropriate device documentation for information about a device login and administration. For example, if you are logging on to the ZDS, see the ZDS documentation.

4. When you have finished managing the device, log out of it.

   IMPORTANT: Always log out of a device before disconnecting the session with the device or before closing out the terminal server session. Otherwise, the next user to log on to the device resumes where the previous session left off. If you fail to log out, the administrative capabilities for the device lock up.

   The initial login prompt appears or the appropriate logout text appears.

5. After logging out of the device press ENTER, press CTRL+Z and then E to disconnect the session to the device from the terminal server.

   NOTICE: Always log out of a device before disconnecting its session.

6.4 Accessing the Remote Access Terminal Server

There are several ways to access the remote terminal server:

- Use HyperTerminal or ProComm (VT100 emulation) to dial in to the terminal server – Provides access to menu options 1 to 5 only.
- For Menu option 6 (PPP), use the Windows After Dial terminal to dial into the terminal server – You cannot use HyperTerminal, ProComm, or telnet for PPP.
- Use telnet to log on to the Terminal Server to access menu options 1 to 5.

6.4.1 Navigating Through the Menu in Remote Analog Access

This section describes how to access the menu options on the remote access terminal server.

NOTICE: This procedure also applies to 8-port terminal servers used for out-of-band management at the Demilitarized Zone (DMZ) switch.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Connect to the terminal device using the **Windows Dial Up Client** application.

2 At the login prompt, log on using the correct ID and password.

3 Perform one of the following actions:

- If the main menu appears, go to step 4.
- If the CLI appears, enter: `menu`

4 From the main menu, select the **Set Up PPP – Using Windows Dial Up Client** option to initiate a PPP link:

```
Menu 1 Main Menu
 1 Maintenance Access
 2 Telnet Session to Host
 3 Show users
 4 Ping to user entered IP address
 5 Show logfile
 6 Set Up PPP — Using Windows Dial Up Client

Up One Level: U      Top of Menu: T      Refresh: R      Logout: Q
Enter Number of Selection and Press <RETURN> to Continue:
```

The `PPP is being started` message appears.

5 Click **Done** to close the **After Dial Terminal** display window.

NOTICE: Options 1 through 5 are applicable in telnet or HyperTerminal/ProComm access only.

6.5 Using Terminal Server Menu Utilities

This section describes the usage of Terminal Server Menu Utilities.

6.5.1 Accessing the Terminal Server through Telnet

This section describes how to access the terminal server through telnet.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

NOTICE: For systems that use Secure Shell (SSH) rather than telnet to access the terminal server, see the section in the *Securing Protocols with SSH* manual for SSH access procedures.

Procedure:

1 Log on to the terminal server.

2 Type the number associated with the **Telnet Session to Host** option. Press ENTER.

The telnet prompt appears.

3 Type the IP address of the device. Press ENTER.

The telnet session is initiated.

6.5.2
Showing Users

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Log on to the terminal server.
2. Type the number associated with the **Show users** option. Press ENTER.

   The list of users and the port number appears.
3. Press ENTER to exit.

6.5.3
Pinging an IP Address

Prerequisites: Locate the following information before performing this procedure:

- IP address and subnet mask assignments for your system
- Login IDs and passwords for your system

Contact your system administrator or your system IP plan for this information.

Procedure:

1. Log on to the terminal server.
2. Type the number associated with the **Ping to user entered IP address** option. Press ENTER.

   The ping prompt appears.
3. Type the `<IP address>` to ping. Press ENTER.

   The ping result appears.
4. Press ENTER to exit.

6.5.4
Showing a Log File

Procedure:

1. Log on to the terminal server.
2. Type the number associated with the **Show logfile** option. Press ENTER.

   NOTICE: This option is used for the maintenance purpose to capture the events for diagnosis.

   The log file appears.
3. Press ENTER to exit.

6.5.5
Setting Up PPP – Using Windows Dial Up PC Client

This procedure describes how to set up Point-to-Point Protocol (PPP) using a Windows Dial Up PC Client.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Log on to the terminal server.
2. Type the number associated with the **Set Up PPP — Using Windows Dial Up Client** option. Press ENTER.

   NOTICE: This option is selected only under Windows After Dial Terminal for PPP link. See Accessing the Terminal Server through Telnet on page 53.

6.5.5.1
Terminating PPP Link Remote Access Terminal Server

Procedure:

1. Right-click the computer icon on the **Windows System Tray**, located in the lower right-hand corner of the screen.
2. Select **Disconnect**.

6.5.6
Showing Port Layout File

Prerequisites: Contact your system administrator for the correct logon ID and password before performing this procedure.

Procedure:

1. Log on to the terminal server.
2. Type the number associated with the **Show port layout file** option. Press ENTER.

   Devices connected to each of the terminal server ports are displayed.
3. Press ENTER to exit.

6.6
Verifying Software Version

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

Procedure:

1. Connect to the terminal server.
2. At the login prompt, enter the `InReach user ID`.
3. At the password prompt, enter the appropriate password.
4. At the `InReach:0>` prompt, enter: `show version`

   The software version information appears.

   - For the S series, the following is displayed:

```
Linux Kernel Version:       X.X.X.X
Linux LX Version:               XXX
Software Version (Runtime):   X.X.X
```

```
Software Version (Flash):     X.X.X
PPCiBoot Version:             X.X.X
```

- For the T series, the following is displayed:

```
Time:               X.X.X.X.X.X.X
Linux Kernel Version:       X.X.X.X
Software Version (Runtime):   X.X.X
Software Version (Flash):     X.X.X
PPCiBoot Version:             X.X.X
```

6.7 Adding Users on the Terminal Server

Use the following procedures to add users on the terminal server. Enter all commands from the super user `InReach>>` prompt.

6.7.1 Accessing the Super User Prompt

To perform this procedure directly from the Unified Network Configurator (UNC), use the Cut-Through method. See “Accessing Devices with the Cut-Through Method” in the *Unified Network Configurator* manual.

The following types of connections to the Terminal Server are available:

Physical

PC/laptop is connected physically by serial connection to the server; both **InReach** and the **serviceuser** accounts can be used (it is local account authentication).

Remote through telnet

When the connection is established remotely and RADIUS authentication is enabled, the **serviceuser** account should be used.

When connection is established remotely but RADIUS authentication is disabled (local account authentication is enabled), **InReach** and **serviceuser** accounts can be used.

Procedure:

1. Connect the DB9 modular adapter and RJ-45 cable to the serial port of a laptop/PC. Connect the other end to the DIAG port on the terminal server.

   The DIAG port is at the rear of the server.

2. Launch a terminal emulator such as HyperTerminal or ProComm from the laptop/PC with the following settings:
   - Data Rate: 9600
   - Data Bits: 8
   - Stop bits: 1
   - Flow Control: Xon/Xoff
3. Press ENTER a few times to activate the session.
4. Log in as the InReach user, and provide the appropriate password.
5. Enter: `enable` and provide the appropriate enable mode password.

   The prompt changes to `InReach:0 >>`.

6.7.2

Adding a New User

This section describes how to add a new user on the terminal server.

Procedure:

1. Acces the Super User Prompt. See Accessing the Super User Prompt on page 56
2. Enter the following command to add a new user: `config subscriber <newuser>`, where **newuser** is the name of the new user account.

   For example, `config subscriber motouser` is the command for the user account **motouser**.

   For more details on how to access the super user prompt, see the “How to Access the Super User Prompt” procedure.
3. Type `exit` twice, to access the `InReach>>` prompt.

   NOTICE: The maximum number of users supported on the LX unit is twice the number of ports. For example, for a 48 port box, the maximum number of users supported is 96.
4. Enter the following commands after the user is created:

   ```
   config subscriber <newuser> security level read
   config subscriber <newuser> idletime 30
   config subscriber <newuser> maxconnections 50
   config subscriber <newuser> maxsessions 10
   config subscriber <newuser> menu name lxuser_menu
   config subscriber <newuser> login mode raw menu
   ```

   NOTICE: The **lxuser_menu** is the name of the menu file. This file is sent to the terminal server through TFTP when initially configured.
5. Enter the following command to configure the password for the newly created user:

   ```
   config subscriber <newuser> password
   ```
6. Enter and re-enter the new password.

6.7.3

Deleting a User

Enter the following command to delete a user on the terminal server: `config no subscriber <newuser>`

For more details on how to access the super user prompt, see Accessing the Super User Prompt on page 56.

6.8

Saving the Configuration

Enter the following command to permanently save any changes made to the Flash configuration:

```
save config flash
```

NOTICE: Enter the `save config flash` command whenever there are changes to the configuration.

6.9 Auditing on the Terminal Server

This section describes how to set up and view auditing on the terminal server.

6.9.1 Setting Up Auditing on the Terminal Server

When the terminal server is configured from the factory, two subscriber accounts, **motorola** and **InReach**, are configured on the server. These accounts may have audit log enabled depending on the security features.

If auditing is required, enter the following command to enable auditing on the new subscriber accounts; `InReach>>config subscriber <username> audit log enable` where **username** is the name of the new subscriber that is created in Adding a New User on page 57.

6.9.2 Viewing Auditing on the Terminal Server

To view auditing, log on as a user that does not have the audit log option enabled. If you log in as a user that has the audit log enabled, log messages are not visible.

Procedure:

1. Log in to the terminal server.
2. Enter the following commands from the `InReach>>` prompt to create a user, only for the audit purpose:
   a. `config subscriber <audituser> security level read`
   b. `config subscriber <audituser> idletime 30`
   c. `config subscriber <audituser> password`

   where **<audituser>** is any valid name
3. Enter the new password and re-enter the password to confirm.

   Once the user is created, you can use telnet to connect to the terminal server and provide the credentials of new user and login.
4. Once logged in, enter the following command to view the audit messages for **Inreach** or **motorola** subscribers, or any new user: `audituser>> show audit log <username>`

   where **<username>** is the name of the subscriber account for which you want to view audit messages

   The audit messages appear.

6.10 Terminal Server Passwords

The following password change procedures are common to all the terminal servers. **Only maintenance personnel can use or change these passwords**. There are four passwords pre-configured by systems engineers responsible for staging and integration on each terminal server.

To change the passwords on the terminal server, log in as the **InReach** user at the console port using Hyper Terminal or ProComm terminal emulator.

CAUTION: Once passwords are changed from the factory default settings and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Set up the laptop/PC for diagnostics management to change user passwords for the terminal server. See Setting Up a Laptop or PC for Out-of-Band Management on page 38 for details.

6.10.1
Setting Read-only User Password for Terminal Server

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

IMPORTANT: Once passwords are changed from the factory default settings and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Procedure:

1. Type the InReach user ID. Press ENTER.

   The password prompt appears.

2. Type the appropriate password. Press ENTER.

   The following prompt appears:

   ```
   InReach:0>
   ```

3. At the `InReach:0>` prompt, type `enable` and provide the privileged password.

   The privileged mode prompt appears.

4. Type the following command. Press ENTER. `InReach:0 >>config subscriber motorola password`

   You are prompted to enter the password.

5. Enter the new password and re-enter it for confirmation.

   The InReach prompt reappears.

6. Type the following command: `InReach:0 >>save config flash` and then press ENTER to save the new password.

   The changed password is saved and the InReach prompt appears.

7. Type `Exit` twice to log out of the terminal server.

6.10.2
Setting Read-Write User Password for Terminal Server

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

IMPORTANT: Once passwords are changed from the factory default settings and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Procedure:

1. Type the InReach user ID. Press ENTER.

   The password prompt appears.

2. Type the appropriate password. Press ENTER.

   The following prompt appears:

   ```
   InReach:0>
   ```

3. At the `InReach:0>` prompt, type `enable` and provide the privileged password.

   The privileged mode prompt appears:

   ```
   InReach:0>>
   ```

4. Type the following command. Press ENTER: `InReach:0 >>config subscriber InReach password`

   You are prompted to enter the password.

5. Enter the new password and re-enter it for confirmation.

   The InReach prompt reappears.

6. Type the following command and then press ENTER to save the new password: `InReach:0 >>save config flash`

   The changed password is saved and the InReach prompt appears.

7. Enter `Exit` twice to log out of the terminal server.

6.10.3
Setting Privilege Mode Password for Terminal Server

This procedure describes how to set the password for the privilege user.

Prerequisites: Contact your system administrator for the correct ID and password before performing this procedure.

IMPORTANT: Once passwords are changed from the factory default settings and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Procedure:

1. Type the InReach user ID. Press ENTER.

   The password prompt appears.

2. Type the appropriate password. Press ENTER.

   The following prompt appears:

   ```
   InReach:0>
   ```

3. At the `InReach:0>` prompt, type `enable` and provide the privileged password.

   The privileged mode prompt appears:

   ```
   InReach:0>>
   ```

4 Enter the following command: `InReach:0 >>config password`

You are prompted to enter the password.

5 Enter the new password and re-enter it for confirmation.

The InReach prompt reappears.

6 Enter the following command. Press ENTER to save the new password: `InReach:0 >>save config flash`

The changed password is saved and InReach prompt appears.

7 Enter `Exit` twice to log out of the terminal server.

6.10.4
Setting PPCiBoot Password for Terminal Server

Prerequisites: Contact your system administrator for the user ID and password before performing this procedure.

IMPORTANT: Once passwords are changed from the factory default settings and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Procedure:

1 Log in as InReach user.

The InReach prompt appears.

2 At the InReach prompt, type `enable` and provide the privileged password.

The privileged mode prompt appears.

3 Type the following command. Press ENTER: `InReach:0 >>config ppciboot password`

You are prompted to enter the password.

4 Enter the current password.

You are prompted to enter the password.

5 Enter the new password and re-enter it for confirmation.

The InReach prompt reappears.

6 Type the following command: `InReach:0 >>save config flash` and press ENTER to save the new password.

The changed password is saved and InReach prompt appears.

7 Enter `Exit` twice to log out of the terminal server.

6.11
Backup and Restore Operations

This section contains procedures for local backup and restore of terminal server configurations.

The interface between the terminal server and the Unified Network Configurator (UNC) does not support secure operation. For systems operating in clear mode, this is not an issue.

For secure backup, the only available option is to back up the terminal server configuration locally using a laptop.

Following are the prerequisites for backing up and restoring the terminal server locally:

- Laptop/PC running 3Com TFTP Server
- Serial connection from the laptop to the terminal server
- Current login password and Privileged mode passwords for the InReach user

6.11.1
Backing Up the Terminal Server Configuration Locally

This section describes how to store the backed up files on the laptop/PC and create a temporary directory (for example, `C:\temp on the laptop/PC`).

Prerequisites: Locate the following information before performing this procedure:

- IP address for TFTP Server
- Account logins and passwords for InReach mode and Enable mode.

Contact your system administrator for this information.

When and where to use: Perform this procedure for maintenance purposes. Lack of the backup configuration files makes it difficult to replace a terminal server when it fails.

Procedure:

1. Open the **3Com TFTP Server** application on the laptop/PC. Point the TFTP root directory to a location where you want to save the backup files, for example, `C:\temp`.
2. From the laptop/PC, launch a terminal emulator, such as HyperTerminal or ProComm with the following settings:
   - Data rate: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow Control: Xon/Xoff
3. Press ENTER a few times to activate the session.
4. At the `Login` prompt, enter: `InReach`
5. At the password prompt, enter: `<InReach password>`
6. At the `InReach:0 >` prompt, enter: `enable`
7. At the password prompt, enter: `<enable mode password>`
8. Enter: `save config network` ***`<filename><tftpIP>`***

   Where:

   `<filename>` is the name of the backup file. Use the `zone`***`<XX>`***`term`***`<YY>`***format, where ***`<XX>`*** is your organization's zone octet number and ***`<YY>`*** is the terminal server number.

   `<tftpIP>` is the IP address of the TFTP server (laptop IP or NM Client IP)

   NOTICE: Configuration files are saved in the specified location with the `.zip` extension.
9. Enter: `exit`
10. Enter: `exit` to logout of the terminal server.

6.11.2

Restoring the Terminal Server Configuration Locally

Prerequisites:
Locate the following information before performing this procedure:

- IP address for TFTP Server
- Account logins and passwords for InReach mode and Enable mode.

Contact your system administrator for this information.

Procedure:

1. Perform the following actions:
   a. Open the **3Com TFTP Server** application on the laptop/PC.
   b. Point the TFTP root directory to a location where the backup files were saved during the backup task.

      The backup file format is `zone`***<XX>***`term`***<YY>***`.zip`, where ***<XX>*** is the zone octet number of your organization and ***<YY>*** is the terminal server number.
2. From the laptop/PC, launch a terminal emulator, such as HyperTerminal or ProComm with the following settings:
   - Data rate: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow Control: Xon/Xoff
3. Press ENTER a few times to activate the session.
4. At the `Login` prompt, enter: `InReach`
5. At the password prompt, enter: ***<InReach password>***.
6. At the In Reach prompt, enter: `enable`
7. At the password prompt, enter: `<enable mode password>`.
8. At the prompt, enter: `config`
9. Enter: `load config from network` ***<tftpIP><zoneXXtermYY>***

   Where:
   <zoneXXtermYY> is the name of the backup file without .zip extension
   <tftpIP> is the IP address of the TFTP server (laptop IP or NM Client IP

   A message to confirm overwriting of current configuration is displayed.
10. Enter: y to confirm overwriting current configuration.

    The Configuration is restored to the terminal server. A message to confirm the reboot appears.
11. Enter: y to confirm the reboot of the terminal server.

    The terminal server reboots for the new configuration to take effect.
12. Restore of configuration is completed.

This page intentionally left blank.

Chapter 7

Terminal Server Maintenance

This chapter contains periodic maintenance procedures relating to the terminal server.

There are no serviceable parts in the terminal server that require maintenance or calibration. If a component fails, send it back to Motorola Solutions for replacement and follow the appropriate FRU/FRE procedure.

7.1 Maintaining the Terminal Server

Clean the exterior of the terminal server using a clean, lint-free cloth, or soft brush periodically.

NOTICE: For detailed descriptions of the status indicators on the terminal servers, see Terminal Server Reference on page 73.

This page intentionally left blank.

Chapter 8

Terminal Server Troubleshooting

This chapter provides the fault management and troubleshooting information relating to the terminal server.

8.1 Terminal Server Failure

Terminal server failure results in loss of out-of-band management capability. While remote and dial-in connectivity to the system becomes unavailable, system functionality is not affected.

8.2 LAN Connection Failure

This section provides troubleshooting for a LAN connection failure. If the LINK LED (also known as the LAN LED) is off, then the terminal server does not detect a connection with the LAN.

Procedure:

1. Remove and visually inspect the cable from the 10/100Base-T Ethernet port. Test the cable for continuity. Reinsert the cable fully into the port.
2. Press the **Reset** button on the terminal server or cycle power to the terminal server.
3. Replace the terminal server or cabling as necessary.

8.3 LAN Activity Failure

This section provides troubleshooting for a LAN activity failure. If the RCV LED is off, then the terminal server does not detect activity on the LAN.

Procedure:

1. Check the condition of the 10/100Base-T Ethernet port. Test the cable for continuity.
2. Check the IP address, subnet mask, and default gateway settings for the terminal server.
3. Remove and visually inspect the cable from the 10Base-T Ethernet port. Test the cable for continuity. Reinsert the cable fully into the port.
4. Press the **Reset** button on the terminal server or cycle power to the terminal server.
5. Reinstall the terminal server software.
6. Replace the terminal server or cabling as necessary.

8.4 POST Test Error Codes

The terminal server software reports status and error messages for different activities that take place. The messages may display a four-digit status or error code, such as `Memory Address Bus Failed Low`. For further information about specific error messages, see Appendix B in *Getting Started with LX-4000 series* (451-0308N) from MRV Communications, Inc.

8.5
General Troubleshooting for the Terminal Server

This section lists general problems of the Terminal Server along with the troubleshooting steps.

Table 5: Terminal Server - General Troubleshooting

Problem	Corrective Action
General connectivity problems	**1** In the network fault management application, check the condition of the Terminal Server and all affected devices and links. **2** Verify that all devices are operating and that all links are physically connected and operational. **3** Check for any sharp bends or kinks in cabling. Test any suspected cabling for noise, continuity, attenuation, and crosstalk. **4** If required, press the **Reset** button on the terminal server or cycle power to the terminal server. **5** If the terminal server still has problems, reinstall the terminal server software or replace the terminal server.
Menu and user access problems	**1** Enter the maintenance access environment and check the menu configuration and password definitions for the terminal server. **2** Update the configuration or restore the configuration from a previous backup copy.
Modem access problems	**1** Verify that the remote client is using the correct phone number and modem configuration. **2** Verify that the phone line is in service and operating normally.
Terminal server not starting up or loading	After initialization, the Run LED should flash slowly and the LAN LED should flash as packets are being received from the network. For information on POST error codes, see “POST Test Error Codes”.

8.5.1
Troubleshooting Terminal Server Using Unified Event Manager

Terminal server is fault-managed by the Unified Event Manager (UEM) application. Check traps displayed in UEM for troubleshooting problems with the terminal server.

See the *Unified Event Manager Online Help* for a list of traps and related definitions.

NOTICE: Terminal Servers must first be discovered in Unified Event Manager before traps can be sent and are visible in the application. For information on discovering devices, see the *Unified Event Manager* manual.

8.6
Restoring Factory Defaults for the LX-4000 Series Terminal Servers

System engineers that are responsible for staging and integration of each terminal server can restore default factory settings.

Prerequisites: If the terminal server's PPCiBoot password is previously configured to a value other than the default value, the updated PPCiBoot password is required to perform factory default settings.

NOTICE: Once passwords are changed from the factory default and are misplaced or forgotten, they cannot be recovered. If this situation occurs, return the terminal server unit to the vendor so it can be reset to its factory defaults.

Process:

1. Set up a laptop/PC for diagnostic management.

   See Setting Up a Laptop/PC for Diagnostic Management on page 38.

2. Restore the terminal server to the factory default settings using the PPCiBoot menu.

   See Restoring the Terminal Server to Factory Default Settings on page 69.

8.6.1 Restoring the Terminal Server to Factory Default Settings

This section describes how to restore the terminal server to the factory default settings using the PPCiBoot menu. Contact your system administrator for the password before performing this procedure.

Prerequisites: Contact your system administrator for the password before performing this procedure.

Procedure:

1. Restart the terminal server by unplugging the power cord and plugging it back.

   The following PPCiBoot menu appears:

```
Welcome to In-Reach PPCiBoot version X.X.X

      [B] Boot System
      [L] Login to System Setup

Booting in    7 seconds...
```

2. Log on to the system setup by typing L before the boot timer expires.

   The PPCiBoot password prompt appears:

```
Enter password:
```

   NOTICE: If the boot timer expires, restart from step 1.

3. Type the PPCiBoot password and press **Enter**.

   PPCiBoot Main Menu appears:

```
                                Main Menu

[1] Boot from network:                      Network, Flash
Image currently in flash:                X.X.X
[f] Save image to flash when boot from network: no
[2] Time Out, in seconds (0=disabled):          8
[3] IP Configuration Menu
[4] Update Ppciboot Firmware
[5] Ethernet Network Link:                      auto
[6] Change PPCiBoot password
[7] FIPS 140-2 Security:                        no
[9] ppciboot image name:                        ppciboot.img
[0] software image name:                        linuxito.img
```

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

Make a choice:

Booting in    4 seconds...
```

4 Type before the boot timer expires. Press ENTER.

The PPCiBoot password prompt appears:

```
Enter current password:
```

NOTICE: If the boot timer expires, restart from step 1.

5 Type PPCiBoot password. Press ENTER.

Unit reset choices are displayed.

```
[1] Reset PPCiBoot configuration
[2] Reset Linux system configuration
[3] Reset PPCiBoot and Linux configurations
!!!Warning: Options 1 and 3 will cause system reset in the end!!!

 Make your choice to proceed or press any other key to return to Main
Menu
```

6 Type the number associated with **Reset PPCiBoot and Linux configurations**.

PPCiBoot and Linux configuration are reset. Status message is displayed and the server restarts.

```
Resetting PPCiBoot configuration ...
.....................................................
Resetting Linux system configuration ...
.....................................................
......
System Reset...
```

After the server restarts, the **Initial Connectivity Setup** message appears.

```
This unit has loaded to factory defaults, would you like to run Initial
Connectivity Setup? (y/n) :
```

7 Type n.

The login prompt appears. The server is now ready for use.

Chapter 9

Terminal Server FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the terminal server.

A FRU procedure is the lowest repair level for a device that can be replaced in the field. Once you remove a failed FRU, return it to a Motorola Solutions service facility for repair. A FRE is a device that does not include any field-replaceable subcomponents or subassemblies (such as a router). FRE replacement involves replacement of the entire assembly.

WARNING: The terminal server contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the terminal server and remove the power cabling before servicing this equipment.

IMPORTANT: Power down the terminal server before replacement. Powering down the terminal server causes any terminal connection services to be lost until the unit is replaced. Local or remote terminals connected to master site resources through the terminal server lose their connection until the terminal server is available again. Terminals have to establish a new connection when the terminal server becomes available again.

NOTICE: After servicing the equipment, always verify that the equipment is operational before leaving the site.

9.1 Required Tools and Equipment

The following items should be taken to the replacement site when replacing any equipment in the terminal server:

- Electrostatic discharge (ESD) strap (Motorola Solutions part number RSX4015A, or equivalent)
- Laptop PC with Trivial File Transfer Protocol (TFTP) server application installed
- Crossover cable
- Phillips and slotted screwdrivers
- Set of TORX drivers

9.2 List of Field Replaceable Entities for the Terminal Server

This section lists each FRE available for the terminal server along with its part number. Use the part number for the item when ordering.

Table 6: Terminal Server Field-Replaceable Entities

Component Type	Part Number
LX Terminal Server 48 Ports with modem	CLN8489A
LX Terminal Server 16 Ports with modem	T7385A
LX Terminal Server 8 Ports no modem	TT2022A

9.3

Replacing a Terminal Server

This section provides instructions to replace a failed terminal server.

Prerequisites:

WARNING: Shock Hazard. The terminal server contains dangerous voltages which can cause electrical shock or damage to equipment. Turn off the terminal server and remove the power cabling when servicing this equipment.

CAUTION: Wear an ESD strap and connect its cable to a verified good ground. Wear this strap throughout this procedure to prevent ESD damage to any components.

IMPORTANT: Power down the terminal server before replacement. Powering down the terminal server causes terminal connection services to be lost until the unit is replaced. Local or remote terminals connected to master site resources through the terminal server lose their connection until the terminal server is again made available. The terminals have to establish a new connection when the terminal server is available.

For more information on how to back up or restore the LX4000 series Terminal Server configuration, see Terminal Server Operation on page 47.

Procedure:

1. Disconnect the power cable from the rear of the terminal server.
2. Remove the terminal server:
   a. Label and disconnect all communication cabling from the rear of the Terminal Server.
   b. Disconnect the grounding cable from the rear of the chassis
   c. Remove the four screws securing the terminal server to the rack and remove the terminal server.
3. Remove the mounting brackets from the terminal server and secure the brackets to the replacement terminal server.
4. Install the replacement terminal server:
   a. Secure the replacement terminal server to the rack.
   b. Connect the grounding cable to the rear of the chassis.
   c. Reconnect the communication cabling to the rear of the terminal server.
5. Connect the power cable to the rear of the terminal server.

   The terminal server powers up.
6. Verify that the terminal server is operating properly.

Chapter 10

Terminal Server Reference

This chapter contains supplemental reference information relating to the terminal server.

10.1 Terminal Server LED Indications

This section provides the LED status for the terminal server.

Table 7: Terminal Server LED Indications

LED	Description	Indication	Status
FLT LED	The FLT LED shows the terminal server has experienced a fault condition. Will also remain on during POST.	Red	The terminal server has experienced a fault condition or it requires maintenance.
OK LED	The OK LED shows the system voltages are normal and it passed the POST.	Green	The terminal server has passed POST and is normal.
LINK LED	The LINK LED shows the status of the LAN connection.	Green	The terminal server is connected to the LAN.
		Off	The terminal server does not detect a connection with the LAN.
RCV LED	The RCV LED indicates LAN activity.	Flashing Yellow	The terminal server is receiving data. Rapid flashing indicates heavy network traffic.
100 Mbps LED	The 100 Mbps LED indicates the speed of the LAN connection.	Solid Green	The terminal server connection is at speed of 100 Mbps.
		Off	The terminal server connection is at speed of 10 Mbps.
Port Status LEDs (1-48)	During initialization, the ports indicate self-test processes, and if any self-test fails, they indicate an error code. When the terminal server is running, the port status LEDs show activity on their designated ports.	Green	During initialization, the ports indicate self-test processes. When terminal server is running, the port status LEDs show activity on their designated ports.

10.2

Terminal Server and Console Port Interface Cable Pin-outs

The cables and associated pin-outs required to connect a terminal server's serial port (8 pin RJ45) to the console port on each device will vary based on the type of device. The following tables define the pin-out requirements for each type of device specified.

NOTICE: To locate cable part numbers, see the system-specific configuration documentation provided by Motorola Solutions shipped with your system.

The following devices based on a CompactPCI platform require pin-out configurations shown in Table 9: Terminal Server to CompactPCI Console Ports on page 74 to interface these devices to the terminal server:

- Zone Controller – CompactPCI console port
- Zone Database Server – CompactPCI console port
- Unified Event Manager Server – CompactPCI console port
- System Statistics Server – CompactPCI console port

Table 8: Terminal Server to EsxServer Console Ports

Terminal Server Serial Port RJ45	Device Console Port DB-9F
3 - Tx	2 - Rx
Tx Rx GND 4 5	GND 5
6 - Rx	3 - Tx

Table 9: Terminal Server to CompactPCI Console Ports

Terminal Server Serial Port RJ45	Device Console Port DB-9F
3 - Tx	2 - Rx
Tx Rx GND 4 5	GND 5
6 - Rx	3 - Tx

Table 10: Terminal Server to TeNSr Channel Bank

Terminal Server Serial Port RJ45	Device Console Port RJ45
3 - Tx	6 - Tx
4 - Tx GND	4 - GND
6 - Rx	5 - Rx

Table 11: Terminal Server to HP ProCurve 2620 Switch and Serial Port to Serial Port (Rollover Cable)

Terminal Server Serial Port RJ45	Device Console Port RJ45
1	8
2	7

Table continued...

Terminal Server Serial Port RJ45	Device Console Port RJ45
3 - Tx	6 - Rx
4 - Tx GND	5 - GND
5 - Tx GND	4 - GND
6 - Rx	3 - Tx
7	2
8	1

Table 12: Terminal Server to Paradyne 3810 Plus or 3920 Plus Modem

Terminal Server Serial Port RJ45	Modem DTE Port DB-25M
1 - CTS	5 - CTS
2 - DTR	20 - DTR
3 - Tx	2 - Tx
Tx & Rx GND 4 & 5	GND 7
6 - Rx	3 - Rx
7 - DCD	8 - DCD
8 - RTS	4 - RTS

Table 13: Terminal Server to TRAK 9100

Terminal Server Serial Port RJ45	Device Console Port DB-9M
3 - Tx	3 - Tx
Tx Rx GND 4 5	GND 5
6 - Rx	2 - Rx

You need a cable to access the console of either the MCP820 PDR or the MCPN905 RNG through the Out-of-Band Management server. Connect this cable to the front of the MCP820 or MCPN905 card and to the Out-of-Band Management server. Do not use the RJ45 connections located in the back of the chassis.

Table 14: PDR to Out-of-Band Management Server Cable Connection Pinout Chart

Out-of-Band Management Server	PDR
3 (TX)	5 (RX)
4 (TX GND)	3 (GND)
6 (RX)	4 (TX)

Table 15: Terminal Server to ASTRO-TAC™ Receiver

Terminal Server Serial Port RJ45	Device Console Port DB-9M
3 - Tx	2 - Rx
Tx Rx GND	GND
4 5	5
6 - Rx	3 - Tx

Table 16: Terminal Server to IDS, Exit Router, and Netra 240

Terminal Server Serial Port RJ45	Device Console Port RJ45
1	8
2	7
3 - Tx	6 - Rx
4 - Tx GND	5 - GND
5 - Rx GND	4 - GND
6 - Rx	3 - Tx
7	2
8	1

Chapter 11

Terminal Server LX Series Disaster Recovery

This chapter provides references and information that will enable you to recover a Terminal Server LX Series in the event of a failure.

11.1 Recovery Sequence for Terminal Server

Prerequisites: Maintain a backup of the terminal server configuration. See Backing Up the Terminal Server Configuration Locally on page 62.

Process:

1. Replace the terminal server.

   See Replacing a Terminal Server on page 72.

2. Restore factory defaults.

   See Restoring Factory Defaults for the LX-4000 Series Terminal Servers on page 68.

3. Log in using default passwords and then set new passwords.

   See Terminal Server Passwords on page 58.

   The factory default passwords are as follows:

   - Login: InReach
   - Password: access
   - InReach:0> enable
   - Password: system
   - InReach:0>>

4. Assign an IP address:

   a. Enter the ***<InReach User ID>***.

   b. At the password prompt, enter the appropriate password.

   c. At the `InReach:0>` prompt, type: `enable` and provide the privileged password.

   d. At the privileged mode prompt, enter:
   `InReach:0 >>config interface 1 address` ***<IP address of the terminal server>*** `mask 255.255.255.0`

   Where the ***<IP address of the terminal server>*** depends on the type of terminal server. Terminal servers located in the zone core have different IP addresses from terminal servers at a site or conventional hub site.

   e. Enter: `InReach:0 >>save config flash`

   f. Verify by entering: `InReach:0>>show interface 1 status`.

5. Verify the software version.

   See Verifying Software Version on page 55.

IMPORTANT: Ensure that the software version is in accordance with your ASTRO® 25 system release.

6 Upgrade/downgrade software, as needed.

See:

- Load Terminal Server Operating System from UNC to the Terminal Server – Network Connectivity to UNC is Available on page 78
- Load Terminal Server Operating System and Software files to the Terminal Server – Network Connectivity to UNC is NOT Available on page 79

7 Restore the terminal server configuration locally.

See Restoring the Terminal Server Configuration Locally on page 63.

8 Before connecting the HP switch port with the terminal server port, disable MAC port lockdown on the HP Switch Port.

See “Disabling MAC Port Lockdown with an HP Switch Service Port” in the *MAC Port Lockdown* manual.

9 Connect the HP switch port to the terminal server port.

10 Enable MAC Port Lockdown on the HP switch port.

See “Performing MAC Port Lockdown on HP Switches” in the *MAC Port Lockdown* manual.

11 Optional: Depending on security policies of your organization, configure SNMPv3 parameters.

See “Terminal Servers Configuration for SNMPv3” in the *SNMPv3* manual.

11.2 Load Terminal Server Operating System from UNC to the Terminal Server – Network Connectivity to UNC is Available

When and where to use: Use this procedure to load the Terminal Server Operating System (OS image) from the UNC to the terminal server. This procedure assumes that the appropriate terminal server operating system is available from the UNC and that UNC is available to “push” the OS image from the UNC to the Terminal Server. For more details on how to load OS Images from CD or DVD media to the UNC Server, see the *Unified Network Configurator* manual.

Procedure:

1 Log on to the UNC from the PNM Client:

a Double-click the Internet Explorer icon on the desktop.

b In the Internet Explorer window, in the Address field, enter: `https://ucs-unc<Y>.ucs`

Where **<*Y*>** is the number of the UNC server (01 for primary core UNC server and 02 for backup core UNC server).

The UNC client launches and a login dialog box appears.

c Type an administrator username in the **Username** field.

d Type an appropriate password in the **Password** field.

e Click **OK**.

The **Dashboard** window appears.

2 Open the list of available Terminal Servers:

a Select **ASTRO 25 Radio Network** from **Networks** in the navigation pane.

The list of options expands.

b Select **Views** from the navigation pane.

c Double-click **Terminal Servers** from the navigation pane.

The list of options expands.

3 Select the terminal server to which you want to upgrade the new OS.

4 Right-click the selected terminal server.

A pop-up menu appears.

5 Select **Update OS Image** from the menu.

6 In the **Select OS Image** dialog box, select the version of the OS image for the terminal server you have selected and click **Next**.

7 In the **Update OS Image** dialog box, select and start files:

a Select the terminal server to which you want to load the OS.

b Click **Schedule**.

The **Schedule Push Job** dialog box appears.

8 In the Schedule Push Job dialog box, type a name for the job in the **Job Name** field and click **Approve & Submit**.

NOTICE: By default, all jobs are scheduled to Run upon approval. To refresh the window with any updates, press F5.

The Terminal Server View appears in the window.

9 Press F7.

NOTICE: The OS push to the device takes approximately 8 minutes to complete. The state for the device appears as Completed and a green dot appears next to the device when the push is complete. If the push fails and the state shows Failed, a red dot appears next to the device. If the dialog box does not automatically refresh, click F5.

The **Schedule Manager** dialog box appears.

10 Double-click **Terminal Server** in the navigation pane.

The **Terminal Server View** window appears.

11 To refresh the **Terminal Servers View** window, press F5.

12 Verify that the OS has been upgraded on the selected Terminal Server.

11.3 Load Terminal Server Operating System and Software files to the Terminal Server – Network Connectivity to UNC is NOT Available

When and where to use: Use this procedure to load the Terminal Server Operating System (OS image) and Software files to the terminal server when the UNC is not available. This procedure assumes that the appropriate terminal server operating system and software files are available on a

client laptop or client PC that can interface with the terminal server to load the OS image and software files from the local client to the Terminal Server.

Procedure:

1. Open the TFTP server on the laptop and configure it to point to the location where the ppciboot.img and linuxito.img are located.

   NOTICE: Ensure that the TFTP server is on the laptop.

2. Connect the terminal server to the laptop via serial connection using the DB-9 Modular adapter and RJ-45 cable.
3. Provide the Ethernet connection using the Ethernet crossover cable into the Eth 1 10/100 port located on the rear side of the Terminal server.
4. Assign an IP address to the Laptop in the same subnet as the terminal server.
5. From the laptop, launch a terminal emulator such as HyperTerminal or ProComm with the following settings:
   - Data rate: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow Control: Xon/Xoff
6. Cycle power on the terminal server and wait for the ppciboot login.

   The ppciboot login prompt appears.

7. At the ppciboot login prompt, do the following:

   a Type L and press ENTER.

   b Type the ppciboot password (the default password is access) at the prompt and press ENTER.

   NOTICE: If boot timer has expired, power cycle again and start over.

   The ppciboot Main Menu appears.

8. Type 3 and press ENTER.

   The IP Configuration Menu appears.

9. Choose the options to enter the IP address of the terminal server, subnet mask and IP address of the TFTP server and press ENTER.

   NOTICE: IP address of the TFTP server is the IP address of the laptop. Ensure that the IP address of the terminal server and IP address of the laptop are in the same subnet.

10. Type S and press ENTER.

    The configuration is saved.

11. Type R and press ENTER.

    The main menu appears.

12. Type 1 and press ENTER.

    NOTICE: Keep typing 1 until the result is [1] Boot from: Network, Flash Result: The Boot from Network field appears as Network, Flash.

13 Type 4 and press ENTER.

This upgrades the ppciboot version. Once the upgrade is done, ppciboot menu appears again.

14 Type S to save and press ENTER.

15 Type F and press ENTER to save the image to flash when booted from the network.

Terminal server loads the image from the TFTP server and (this time only) writes it to flash in the proper location for this version.

16 Type B to boot (Starts booting process automatically and loads the Linuxito file into flash).

Once the image is downloaded, the terminal server finishes the boot process. The login prompt appears.

17 At the login prompt, do the following:

a Type `InReach` and press ENTER.

b Type the appropriate password and press ENTER.

The prompt appears.

18 Type the following command and press ENTER: `show version`.

The version number appears.

19 Verify that the version matches with the upgraded version.

This page intentionally left blank.

Appendix A

Configuring the Paradyne Modem

This appendix contains information on configuring the Paradyne COMSPHERE 3810 (V.32), Paradyne COMSPHERE 3810 Plus (V.34), or Paradyne 3920 modem for remote analog access (or out-of-band management at the Demilitarized Zone (DMZ) switch).

IMPORTANT: Paradyne 3920 modems are approved for use in countries outside the United States. Although you can use the 3810 Plus or 3920 outside of the USA, the 3920 is recommended because it is homologated in more countries. The programming parameters are the same (set up any country-specific parameters when in the destination country). The configuration for 3810 Plus and 3920 is common for both models of modem.

When used for remote analog access or for out-of-band management at the DMZ, the Paradyne COMSPHERE 3810 modem connects to a terminal server device to provide dial-up access to the ASTRO® 25 Local Area Network (LAN).

Review the following to configure the Paradyne COMSPHERE 3810 modem for remote analog access or for out-of-band management at the DMZ switch.

A.1 Configuring the Paradyne Modem for Remote Access

For remote access, dial in to the system network through a remote access server or terminal server. This section provides the necessary steps and parameters for configuring the Paradyne modem for remote access.

NOTICE: A terminal server used for remote analog access can also be referred to as a remote access server.

A.1.1 Powering Up the Paradyne Modem

Procedure:

1. Plug the modem power supply into an appropriate power source (normally 110 V, 60 Hz).
2. Plug the power supply into the modem.
3. Turn on the toggle switch near the power plug in the back of the modem.

   The Paradyne modem is now powered up.

A.1.2 Returning Paradyne Modem to Factory Default Settings

Follow this procedure to ensure that these default settings are loaded before configuring other Paradyne modem parameters. In this procedure, F_ is used to indicate the function key (F1, F2, or F3) that is directly under the option that you want to select.

Prerequisites:

NOTICE: In the procedure, F_ is used to indicate the function key (F1, F2, or F3) that is directly under the option that you want to select.

Procedure:

1. Press **Scroll Forward (>)**, on the front panel of the modem, several times until the **Configure** option appears.

   The Configure option appears in the LED screen.

2. Press the **F_** key under the Configure option to select it, where **F_** is the key directly under the **Configure** option.

   The configure option is selected.

3. At the `Ld EditArea frm>` prompt, press **>** to scroll through the configure options until you see the **Factory** option.

   The factory options appear.

4. Press **F1** under the **Factory** option to select it.

   The factory default settings are saved.

5. Press **>** to scroll through the main menu until the Async_Dial option appears in the LED screen.

   The Async_Dial Option appears on the LED screen.

6. Press **F1** to select the **Async_Dial** option.

   The Async Dial option is selected.

7. Press **>** until the **Save Edit Area to Activ (Saved)** option appears in the LED screen.

   (Saved) option appears in the LED screen.

8. Press **F1** to select **Save Edit Area to Activ (Saved)**.

   The Activ prompt is displayed and saved.

9. Press the **Main Menu** double **^** button to move back to the top-most menu.

   The Top menu appears.

A.1.3
Configuring the Modem Parameters

In the procedure, F_ is used to indicate the function key (F1, F2, or F3) that is directly under the option that you want to select.

Procedure:

1. Press **Scroll Forward (>)** until the **Configure** option appears in the LED screen.

   The Configure option appears in the LED screen.

2. Press the **F_** key under the **Configure** option to select it.

   The Configure option is selected.

3. Press **F1** to select the **Activ (Operating)** option.

   The Activ (Operating) option is selected.

4. Press **F1** to select the **Edit** option.

   The Edit option is selected.

A.1.4
Configuring the DTE Interface Strap Group

In this procedure, F_ is used to indicate the function key (F1, F2, or F3) that is directly under the option that you want to select.

Procedure:

1. Press **F1** to select the **DTE_Interface** option.

   The Configure option appears in the LED screen.

2. Set/Verify the parameters in the order shown in the tables found in the Configuration Parameter Settings for Remote Access — Paradyne 3810 Plus Modem on page 86 or Configuration Parameter Settings for Remote Access — Paradyne 3920 Modem on page 89 sections. At the end of each Strap Group, an **END** option appears. Press **F1** to select the **END** option, and then scroll to the next parameter group using the **>** key.

   The Configure Option is selected.

A.1.5
Configuring Other Parameters

This section provides the steps for how to configure the other Paradyne modem Strap/Group parameters.

Procedure:

1. From the **Main** menu, select each Parameter Group Name (for example, DTE_Interface, DTE_Dialer, or Line_Dialer), enter the values shown in the tables in the Configuration Parameter Settings for Remote Access — Paradyne 3810 Plus Modem on page 86 or Configuration Parameter Settings for Remote Access — Paradyne 3920 Modem on page 89 sections.

   Each Strap Group choice appears and may be selected.

2. Save the configuration as described in Saving the Configuration for All Parameters on page 85.

   Set values are saved.

3. Repeat until all parameters are set and verified.

   The modem is correctly configured.

A.1.6
Saving the Configuration for All Parameters

Use this procedure to save the configuration for all Paradyne modem parameters.

Procedure:

1. When all changes in a given parameter set have been made, press the **^** key once, press **F3** to select the **SAVE** option.

   The SAVE option is selected.

2. Press **F1** to select the **Save Edit/Area to Activ (Saved)** option.

   The values in the parameter set are saved.

3 Use the configuration parameters shown in the tables found in the Configuration Parameter Settings for Remote Access — Paradyne 3810 Plus Modem on page 86 and the Configuration Parameter Settings for Remote Access — Paradyne 3920 Modem on page 89 sections.

The modem is correctly configured when all parameters have been entered, saved, and verified.

A.1.7

Configuration Parameter Settings for Remote Access — Paradyne 3810 Plus Modem

DTE_Interface Operating Parameters

This table lists the Active (Operating) parameters for the DTE_Interface.

Table 17: Paradyne 3810 Plus Modem – DTE_Interface Operating Parameters

DTE_Interface Setting	Value
Async / Sync Mode	Async
Async DTE Rate	38400
#Data Bits	8
Parity Bit	None
#Stop Bits	1
DTR Action	Standard RS232
DSR Control	Standard RS232
RTS Action	Standard RS232
CTS Control	Standard RS232
RTS/CTS Delay	0 msec
LSD Control	Standard RS232
CT111_Rate Cntl	Disable
DTE_Rate=VF	Disable

DTE_Dialer Operating Parameters

The table lists the Active (Operating) parameters for the DTE_Dialer.

Table 18: Paradyne 3810 Plus Modem – DTE_Dialer Operating Parameters

DTE_Dialer	Value
DTE Dialer Type	Disable

Line_Dialer Settings

This table lists the Line_Dialer settings.

Table 19: Paradyne 3810 Plus Modem – Line_Dialer Settings

Line_Dialer Setting	Value
AutoAnswerRing#	1
Dialer Type	Tone
DialTone Detect	Enable
Busy Tone Detect	Enable
"," Pause Time	2 seconds
NoAnswer Timeout	45 seconds
Fast Disconnect	Enable
Long Space Disc	Enable
No Carrier Disc	2 seconds
No Data Disc	Disable
MakeBusy ViaDTR	Disable

Dial_Line Settings

This table lists the Dial_Line settings.

Table 20: Paradyne 3810 Plus Modem – Dial_Line Settings

Dial_Line Setting	Value
Modulation	V34
Dial Line Rate	33600
Automode	Enable
Autorate	Enable
Dial Tx Level	Permissiv (-9)
V22b Guard Tone	Disable
Train Time	Long
Asymmetric Rate	Enable
Proacte Retrain	Enable
Fall Fwd Delay	Disable

V42/MNP/Buffer

This table lists the V42/MNP/Buffer settings.

Table 21: Paradyne 3810 Plus Modem – V42/MNP/Buffer

V42/MNP/Buffer	Value
Error Control Mode	V42/MNP_or_Buffer

Table continued…

V42/MNP/Buffer	Value
V.42bis Compress	Enable
MNP5	Enable
EC Negotiat Bfr	Enable
EC Fallbk Char	ASCI
Flw Cntl of DTE	CTS_to_DTE
Flw Cntl of Modem	RTS_To_Mdm
Mdm/Mdm FlowCtl	Disable
Break Buffr Cntl	Keep_Data
Send Break Cntl	Data_First
Tx Buff Disc Delay	10 seconds
Rx Buff Disc Delay	Disable
Max Frame Size	256
BfrSizeLnBfrMode	Normal

Test Values

This table lists tests and the corresponding values.

Table 22: Paradyne 3810 Plus Modem – Test Values

Test	Value
DTE RL (CT140)	Disable
DTE LL (CT141)	Disable
Test Timeout	Disable
Rev RemoteLoop	Enable
V54 Address	Disable

Misc. Settings

This table lists the Misc. settings.

Table 23: Paradyne 3810 Plus Modem – Misc. Settings

Misc.	Value
StrapsWhenDisc	No_Change
Speaker Control	OnUntilCarr
Speaker Volume	Medium
Access frm Remt	Disable
RemAccessPasswrd	00000000
Dir#1_Callback	Disable
NetMngmtAddress	256
NMS_Call_Msgs	Call Cact & Prg

Table continued…

Misc.	Value
NMS DTR Alarm	Disable

Security Settings

This table lists Security settings.

Table 24: Paradyne 3810 Plus Modem – Security Settings

Security	Value
NMS Reporting	00
Answer_Secur	No_Answer_Sec
Originate_Secur	No_Orig_Sec

A.1.8

Configuration Parameter Settings for Remote Access — Paradyne 3920 Modem

DTE_Interface Operating Parameters

This table lists the Active (Operating) parameters for the DTE_Interface.

Table 25: Paradyne 3920 Modem – DTE_Interface Operating Parameters

DTE_Interface Setting	Value
Async / Sync Mode	Async
Async DTE Rate	38400
#Data Bits	8
Parity Bit	None
#Stop Bits	1
DTR Action	Standard RS232
DSR Control	Standard RS232
RTS Action	Standard RS232
CTS Control	Standard RS232
RTS/CTS Delay	0 msec
LSD Control	Standard RS232
DTE_Rate=VF	Disable
DTE Alarm Mask	Disable
Extend Main Ch.	Disable

DTE_Dialer Operating Parameters

This table lists the Active (Operating) parameters for the DTE_Dialer.

Table 26: Paradyne 3920 Modem – DTE_Dialer Operating Parameters

DTE_Dialer	Value
DTE Dialer Type	Disable

Line_Dialer Settings

This table lists the Line_Dialer settings.

Table 27: Paradyne 3920 Modem – Line_Dialer Settings

Line_Dialer Setting	Value
AutoAnswerRing#	1
Dialer Type	Tone
DialTone Detect	Enable
Busy Tone Detect	Enable
"," Pause Time	2 seconds
NoAnswer Timeout	45 seconds
Fast Disconnect	Enable
Long Space Disc	Enable
No Carrier Disc	2 seconds
No Data Disc	Disable
MakeBusy ViaDTR	Disable

Dial_Line Settings

This table lists the Dial_Line settings.

Table 28: Paradyne 3920 Modem – Dial_Line Settings

Dial_Line Setting	Value
Modulation	V34
Dial Line Rate	33600 (V34)
Automode	Enable
Autorate	Enable
Dial Tx Level	-10 dBm
V22b Guard Tone	Disable
Train Time	Long
V.34 Symbol Rate	Automatic
V.34 Precoder	Disable
Asymmetric Rate	Enable

Table continued…

Dial_Line Setting	Value
Proacte Retrain	Enable

V42/MNP/Buffer

This table lists the V42/MNP/Buffer settings.

Table 29: Paradyne 3920 Modem – V42/MNP/Buffer

V42/MNP/Buffer	Value
Error Control Mode	V42/MNP_or_Buffer
V.42bis Compress	Enable
MNP5	Enable
EC Negotiat Bfr	Enable
EC Fallbk Char	013 ASCI
Flw Cntl of DTE	CTS_to_DTE
Flw Cntl of Modem	RTS_To_Mdm
Mdm/Mdm FlowCtl	Enable
Break Buffr Cntl	Keep_Data
Send Break Cntl	Data_First
Buff Disc Delay	10 seconds
Max Frame Size	256
BfrSizeLnBfrMode	Disable

Test Values

This table lists tests and the corresponding values.

Table 30: Paradyne 3920 Modem – Test Values

Test	Value
DTE RL (CT140)	Disable
DTE LL (CT141)	Disable
Test Timeout	Disable
Rev RemoteLoop	Enable
V54 Address	Disable

Misc. Settings

This table lists the Misc. settings.

Table 31: Paradyne 3920 Modem – Misc. Settings

Misc.	Value
StrapsWhenDisc	No_Change

Table continued…

Misc.	Value
Speaker Control	OnUntilCarr
Speaker Volume	Medium
Access frm Remt	Disable
RemAccessPasswrd	00000000
Dir#1_Callback	Disable
SpecialSecurity	Disable
NMS_Call_Msgs	Call Cact & Prg
Network Position	Tributary
Diag Connection	Modem (DC)
Link Delay (sec)	0

Security Settings

This table lists Security settings.

Table 32: Paradyne 3920 Modem – Security Settings

Security	Value
Answer_Secur	No_Answer_Sec
Originate_Secur	No_Orig_Sec

Appendix B

Configuring the Raymar Modem

This appendix contains information on configuring the Raymar V.3600 Series Modem.

NOTICE: The Raymar modem can be used as a replacement for the Paradyne Modem

The Raymar-Telenetics V.3600 Series Modem provides synchronous, asynchronous, and fax capabilities for data communications or facsimile links between a local computer and a remote computer, fax, or data terminal equipment (DTE) located anywhere a standard or cellular telephone can reach. Data can be transmitted over standard dial-up lines, private leased telephone lines, or wireless communication. A high-level security feature allows secure operation of the modem, both locally and remotely.

B.1
Configuration of the Raymar Modem

Table 33: Modem Option Parameters

NOTICE: The following configuration applies only when used in conjunction with LX Terminal server dialup access.

Option	Parameter
DIAL LINE	(DEFAULT)
MODULATION	AUTOMODE
DCE MAX RATE	33600
DCE MIN RATE	DISABLED
V.34 RATE THRESH	HIGH BER
V.34 ASYM	ENABLED
V.22 GUARD TONE	DISABLED
V.32B FAST TRAIN	ENABLED
AUTO RETRAIN	ENABLED
SQ AUTO RATE	DISABLED
CLOCK	INTERNAL
DIAL TX LEVEL	-10DBM
RING FREQ LIMIT	DISABLED
LINE CURRENT DIS	LONG
LONG SPACE DISC	ENABLED

Table 34: Protocol Option Parameters

Option	Parameter
LAPM PROTOCOL	DISABLED

Table continued…

Option	Parameter
MNP PROTOCOL	ENABLED
PROTOCOL FALLBACK	ENABLED
DATA COMPRESSION	NORMAL
DTE SPEED	CONSTANT
DTE FLOW CONTROL	RTS
DCE FLOW CONTROL	CTS
XON/XOFF PASSTHRU	DISABLED
INACTIVITY TIMER	OFF
BREAK OPTION	#5
V.42 FAST DETECT	ENABLED

Table 35: DTE Option Parameters

Option	Parameter
DATA	ASYNC
DTE RATE	38400
CHAR SIZE	8 BIT
PARITY	NO
DIALER	ASYNC
AT COMMAND SET	DISABLED
DTR STATE	DISCONNECTS
DSR STATE	FORCE HIGH
DCD STATE	NORMAL
CTS STATE	FOLLOWS RTS
RTS-CTS DELAY	0 MS
DTE FALLBACK	DISABLED
OPTIONS AT DISC	RETAINED

Table 36: Test Option Parameters

Option	Parameter
BILAT DIGITAL	DISABLED
DTE LOCAL TEST	DISABLED
DTE REMOTE TEST	DISABLED
REMOTE COMMANDED	ENABLED
TEST TIMEOUT	OFF

Table 37: Dial Line Option Parameters

Option	Parametr
DIAL TYPE	TONE
AUTO DIAL	#1
DIAL TONE	WAIT FOR DIAL TONE
WAIT DELAY	(DEFAULT)
PAUSE DELAY	2 SEC
CALL TIMEOUT	30 SEC
AUTO ANSWER RING	1
AUTOCALLBACK	DISABLED

Table 38: Speaker Operation Parameters

Option	Parameter
VOLUME	LOW
SPEAKER CONTROL	ON UNTIL CARRIER DETECT

Table 39: Load or Store Option Set

Option	Parameter
LOAD FACTORY OPTION SET	NO
LOAD FROM USER OPTION SET	NO
STORE PRESENT OPTIONS	YES
STORE TO USER OPTION SET #1	YES
ARE YOU SURE	YES
USER OPTION	NO

NOTICE: TX LEVEL (-10)dB Microwave (0)dB Leased Line. These levels are approx. and vary from system to system.

This page intentionally left blank.