



L357 Gigabit Ethernet Service Unit User Manual



This product may contain a laser diode emitter operating at a wavelength of 1300 nm - 1600 nm. Use of optical instruments (for example: collimating optics) with this product may increase eye hazard. Use of controls or adjustments or performing procedures other than those specified herein may result in hazardous radiation exposure.

Under normal conditions, the radiation levels emitted by this product are under the Class 1 limits in 21 CFR Chapter 1, Subchapter J.

ATTENCION!

Cet équipement peut avoir une diode laser émettant à des longueurs d'onde allant de 1300nm à 1600nm. L'utilisation d'instruments optiques (par exemple : un collimateur optique) avec cet équipement peut s'avèrer dangereuse pour les yeux. Procéder à des contrôles, des ajustements ou toute procédure autre que celles décrites ci-après peut provoquer une exposition dangereuse à des radiations.

Sous des conditions normales, le niveau des radiations émises par cet équipement est en dessous des limites prescrites dans CFR21, chapitre 1, sous chapitre J.



This device contains static sensitive components. It should be handled only with proper Electrostatic Discharge (ESD) grounding procedures.

NOTE!

Cet équipement contient des composants sensibles aux décharges électro-statiques. Il doit absolument être manipulé en respectant les règles de mise à la terre afin de prévenir de telles décharges.

NOTICE

Canoga Perkins has prepared this users manual for use by customers and Canoga Perkins personnel as a guide for the proper installation, operation and/or maintenance of Canoga Perkins equipment. The drawings, specifications and information contained in this document are the property of Canoga Perkins and any unauthorized use or disclosure of such drawings, specifications and information is prohibited.

Canoga Perkins reserves the right to change or update the contents of this manual and to change the specifications of its products at any time without prior notification. Every effort has been made to keep the information in this document current and accurate as of the date of publication or revision. However, no guarantee is given or implied that the document is error free or that it is accurate with regard to any specification.

CANOGA PERKINS CORPORATION

20600 Prairie Street Chatsworth, California 91311-6008 Business Phone: (818) 718-6300 (Monday through Friday 7 a.m. - 5 p.m. Pacific Time) FAX: (818) 718-6312 (24 hrs.)

> Web Site: www.canoga.com Email: fiber@canoga.com

Copyright © 2004 - 2005 Canoga Perkins Corporation All Rights Reserved

> EdgeAccess[®] Universal Chassis System L357 Gigabit Ethernet Service Unit User Manual Model Number L357-UM Part Number 6912590 Rev. C 01/2008

To reference Technical Advisories and Product Release Notes, go to Canoga Perkins' website.

Table of Contents

Chap	oter 1 Overview	1-1
1.1	L357 Series	1-1
1.2	L357 Hosts	1-2
Chap	oter 2 Set-up and Installation	2-1
2.1	Set Up and Install the L357	2-1
2.2	Install the Cables	2-3
2.3	Measure Fiber Link Attenuation and Transmit Power	2-3
Chap	oter 3 User Operation	3-1
3.1	L357 Functions and Power Up	3-1
3.2	Front Panel LEDs	3-1
3.3	Alarms	3-3
3.3.1	Link Loss Forwarding	3-3
3.3.2	Link Loss Echo	3-4
3.3.3	Loopback	3-4
Chap	pter 4 Management - VT-100	4-1
4.1	VT100 Terminal Emulation	4-1
4.2	PC Configuration for Terminal Operation	4-1
4.3	Management User Interface	4-2
4.3.1	General Screen Format	4-2
4.3.2	User Interface Organization	4-3
4.3.3	Login Menu	4-3
4.3.4	DMM Main Menu	4-4
4.4	L357 Main Menu	4-4
4.5	System Configuration Menu	4-5
4.5.1	Hardware Configuration Screen	4-6
4.5.2	Functional Configuration Screen	4-7
4.5.3	Trap Configuration	4-10
4.5.4	Alarm Output Configuration	4-10
4.5.5	IP/SNMP Agent Configuration	4-11
4.5.6	Security Configuration	4-14
4.5.7	User Accounts Screen	4-15
4.5.8	System Information Screen	4-16
4.6	Diagnostics Screen and Loopback	4-17
4.7	Link Status Screen	4-18
4.8	System Alarms	4-19
4.9	Layer 2 Statistics	4-19
4.10	System Log	4-20
4.11	Utilities	4-21
4.11.1	PING Generation	4-22
4.11.2	Static ARP Table	4-23
4.11.3	Dynamic ARP Table	4-23

4.12	Software Upgrade	4
4.13	Change Password	5
4.14	Manage Connected Sessions	5
Chap	ter 5 Maintenance and Troubleshooting5-	1
5.1	General Maintenance	1
5.1.1	Manage Cable Links	1
5.1.2	Check Optical Power Levels	1
5.1.3	Measure Transmitter Output Power	2
5.1.4	Measure Receiver Input Power	2
5.1.5	Measure Fiber Link Attenuation	3
5.2	Troubleshooting	3
5.2.1	LED Indicators	3
5.2.2	New Installation	4
5.2.3	Switch 1 and 2 Settings Ignored	4
5.2.4	Problems With Fiber Optics	4
Chap	ter 6 Specifications6-2	1
6.1	L357 Specifications	1
6.2	L357 Models	1

Appendix A Warranty Information	A-1
Appendix B Acronym and Abbreviation List	B-1

List of Figures

Figure 1. The L357	1-1
Figure 2. Switch 1 Through 8 Locations	2-1
Figure 3. Link Loss Forwarding Propagation	
Figure 4. Link Loss Echo Detection	
Figure 5. Local-Local Loopback Mode	
Figure 6. Local-Remote Loopback Mode	
Figure 7. Remote-Local Loopback Mode	
Figure 8. Remote-Remote Loopback Mode	
Figure 9. General Screen Format	4-2
Figure 10. L357 Main Menu	4-4
Figure 11. System Configuration Menu	4-5
Figure 12. Hardware Configuration Screen	4-6
Figure 13. Remote Hardware Configuration Screen	
Figure 14. Functional Configuration Screen (UTP to Fiber L3	57)4-7
Figure 15. Remote Configuration Menu	
Figure 16. Remote Functional Configuration Screen	
Figure 17. Remote VLAN Configuration Screen	
Figure 18. Remote VLAN Tag Translation Table Screen	4-9
Figure 19. Remote P-Bit Translation Table Screen	
Figure 20. Trap Configuration Screen	
Figure 21. Alarm Output Configuration Screen	4-11
Figure 22. IP/SNMP Agent Configuration Screen	
Figure 23. Host Access Table Screen	4-13
Figure 24. Trap/Notification Destination Table Screen	
Figure 25. Security Configuration Screen	4-14
Figure 26. User Accounts Screen	4-15
Figure 27. System Information Screen	4-17
Figure 28. Diagnostics Screen	4-17
Figure 29. Diagnostics Screen	
Figure 30. Link Status Screen	
Figure 31. System Alarms Screen	4-19
Figure 32. Layer 2 Statistics Screen	
Figure 33. System Log Screen	
Figure 34. Utilities Menu Screen	
Figure 35. PING Generation Screen	
Figure 36. Static ARP Table Screen	
Figure 37. Dynamic ARP Table Screen	
Figure 38. Software Upgrade Screen	
Figure 39. Connected Sessions Screen	

List of Tables

Table 1.	Switch 1 and 2 UTP Speed Settings	
Table 2.	Switch 3 Through 8 Functions	
Table 3. 1	L357 LEDs	
Table 4.	System Configuration Option Definitions	
Table 5. 1	Functional Configuration Option Definitions	
Table 6.	Alarm Output Definitions	4-11
Table 7.	SNMP Configuration Parameters Description	4-12
Table 8.	Security Configuration Option Definitions	4-14
Table 9. 1	Diagnostics Screen Definitions	4-18
Table 10.	Utilities Menu Options	4-21
Table 4.Table 5.Table 6.Table 7.Table 7.Table 8.Table 9.Table 10.	System Configuration Option Definitions Functional Configuration Option Definitions Alarm Output Definitions SNMP Configuration Parameters Description Security Configuration Option Definitions Diagnostics Screen Definitions Utilities Menu Options	4-5 4-8 4-11 4-12 4-14 4-18 4-21

Chapter 1 Overview

The Edge Access L357 Series 10/100/1000 Ethernet Service Unit (ESU) converts and extends Ethernet media between Local Area Networks (LANs) located up to 120 Km apart.

In addition, the L357 offers Quality of Service (QoS) implementation, Ethernet Jumbo Frame support, and Layer 2 statistics, as well as standard Canoga Perkins features, such as local and remote loopback, remote software upgrade, and remote control and monitoring through the Side-Band Management Channel (SBMC).

1.1 L357 Series

The L357 receives and transmits 10/100/1000BASE-T Ethernet data on single mode or multimode fiber optic cable.

The L357 front panel, shown in Figure 1, includes:

- User port options:
 - 10/100/1000BASE-T copper
 - 1000BASE-X fiber
- Extension port: SC connector, simplex or duplex; simplex requires a pair of L357s, one at 1310 nm wavelength and the other at 1550 nm wavelength
- Status LEDs:
 - STA shows L357 status
 - CFG shows configuration and setup status
 - SPD and FDX show status for a UTP User port
 - LNK/RX and TX pairs for the User and Extension ports show that data is received and transmitted



Figure 1. The L357

1.2 L357 Hosts

The L357 can be used in a variety of chassis.

- To use the UCS 1000 Chassis, insert a Model 1230 Bus Access Module (BAM) that holds up to two L357s per BAM.
- To use the UCS 1001 Chassis, insert up to two Model 1230 BAMs with up to two L357s per BAM.
- To use the UCS 1002 Chassis, directly insert the L357s.
- To use a standalone enclosure, directly insert one L357.

The L357 is hot swappable; it can be inserted or removed at any time without disrupting the data transfer of other modules in the chassis.

Chapter 2 Set-up and Installation

This section describes how to set up and install the L357.

2.1 Set Up and Install the L357

Before setting up the L357, make sure the chassis is installed and its Users Manual is available for reference. If the system includes an optional DMM and CIM(s), make sure these are available:

- Serial cable (required to connect the chassis to a VT100 type terminal or PC)
- VT100 type terminal or PC to run the User Interface manager
- The DMM and CIM manuals
- 1. Unpack and inspect all components. Save the shipping carton and packing materials in case you need to return the equipment to the manufacturer. Appendix A provides information for Return Material Authorization (RMA).
- 2. Before inserting the L357, check the front panel to verify that the L357 provides the wavelength that matches its link partner.
- 3. For installation in a UCS 1001 or a Model 1030 enclosure, or if you plan to use the Hardware Option Control (see Section 4.5.2), set Switches 1 through 6 (Switches 7 and 8 are not used); see Figure 2 and Tables 1 and 2. For more information about the hardware switch functions, see Section 3.3.





Figure 2. Switch 1 Through 8 Locations

Switch 1	Switch 2	Speed
Off	Off	1000 Mbps
Off	On	100 Mbps
On	Off	10 Mbps
On	On	Autonegotiate

Table 1. Switch 1 and 2 UTP Speed Settings

Table 2. Switch 3 Through 8 Functions

Switch	Function	On	Off
3	Full Duplex on UTP User Port	Select full duplex	Select half duplex
4	SBMC	Enable SBMC	Disable SBMC
5	LLF, Extension to User	Enable Link Loss Forwarding (LLF) propagating from Extension Port to User Port	Disable LLF propagating from Extension Port to User Port
6	LLF, User to Extension	Enable LLF propagating from User Port to Extension Port	Disable LLF propagating from User Port to Extension Port
7, 8	Not used		

- 4. To install the L357 in a BAM in a UCS 1000 or 1001, follow these steps:
 - a. Insert a BAM into an available slot. Slide the BAM into the rails and push it firmly into the connector, then tighten the captive screws. If you encounter resistance, pull the BAM out and check that no connector pins are bent.
 - b. Insert the L357 into an unused slot in the BAM. Slide the L357 into the rails and push it firmly into the connector, then tighten the captive screw. If you encounter resistance, pull it out and check that no connector pins are bent. If you encounter more difficulty, contact Canoga Perkins at (818) 718-6300 for technical assistance.
- 5. To install the L357 in a UCS Model 1002 or Standalone Enclosure, insert the L357 into an unused slot. Slide the L357 into the rails and push it firmly into the backplane, then tighten the captive screw. If you encounter resistance, pull it out and check that no connector pins are bent. If you encounter more difficulty, contact Canoga Perkins at (818) 718-6300 for technical assistance.
- *Note:* The L357 is hot-swappable and can be inserted or removed without disrupting data transfer in other modules in the chassis.

2.2 Install the Cables

The L357 uses both electrical and fiber optic cables. Electrical UTP cables connect to the User Port. Fiber optic cables connect to the Extension port. Dirty optical connectors are a common source of link loss or attenuation problems, especially for single mode fiber (SMF). Clean the connectors before plugging in a cable and whenever there is a significant or unexplained light loss. To prevent contamination, always install protective dust covers on unused fiber optic connectors.

Follow these steps to install the cables:

- 1. Wipe the ferrule and the end-face surface of the male fiber coupler with a lint-free isopropyl alcohol pad from a fiber cleaning kit.
- 2. Use canned air to blow out any dust from the female fiber coupler.

Caution: To avoid damaging the fiber end-surface or connector, use extreme care when installing or removing cables.

- 3. Plug in the optical cables:
 - If you have a single fiber interface, plug the cable into a pair of L357s, one at 1310 nm wavelength and the other at 1550 nm wavelength.
 - If you have a duplex connector, use Tx to Rx, and Rx to Tx orientation.

Caution: To protect the Ethernet port from an intrabuilding lightning surge, use a properly grounded shielded cable.

- 4. If you have copper to the User port, plug the UTP Ethernet cable with RJ-45 connector into the User port on the front of the L357.
- 5. Label each cable and connector with a signal name and direction.

2.3 Measure Fiber Link Attenuation and Transmit Power

Canoga Perkins recommends that you determine and record link attenuation and transmission power before starting normal link traffic. The attenuation factor and transmission power identify potential problems with links near the lower limit of receiver limitations.

For details on link attenuation and transmission power, see Chapter 5.

Chapter 3 User Operation

This chapter describes the hardware features and functions of the L357.

3.1 L357 Functions and Power Up

Each L357 requires a host for power. During the initial power-up sequence, all LEDs light amber. When start-up is complete, the setup and installation are correct, and data is transmitting normally across the link, the STA LED lights green and the LNK/Rx and Tx LEDs for both ports light green or blink green when they transmit or receive data. See Table 3.

3.2 Front Panel LEDs

The LEDs on the front panel show the system and port conditions. The STA LED shows the link condition. The LNK/Rx and Tx LEDs show the conditions on the User and Extension Ports and can be used as an aid when troubleshooting a fault. Table 3 shows the LED states for various conditions.

In the UCS 1000 and 1001, a BAM holds up to two L357s. On the BAM, the STA LED lights green if either L357 is operating normally. If both L357s are in error conditions, the BAM STA LED lights amber.

LED	Status	Description
STA	Off	No power
	Green	Normal operation
	Amber	System self-test
	Amber blinking	Downloading file
	Red	Major alarm
CFG	Off	SBMC is disabled
	Green	SBMC is enabled
	Amber	System self-test
	Red	Configuration error
LNK/Rx (User Port)	Off	No link
	Green	Link Established
	Green blinking	Receiving activity
	Amber	System self-test

Table 3. L357 LEDs

LED	Status	Description
TX (User Port)	Off	No transmission activity
	Green	Transmission activity
	Amber	Port in standby mode or system self-test
	Red	Transmission disabled due to LLF or port disabled
SPD	Off	10 Mbps data rate
	Amber	100 Mbps data rate
	Green	1000 Mbps data rate
FDX	Off	Half duplex mode
	Green	Full duplex mode
LNK/Rx	Off	No link
(Extension Port)	Green	Link Established
	Green blinking	Receiving activity
	Amber	System self-test
Tx (Extension Port)	Off	No transmission activity
	Green blinking	Transmission activity
	Amber	Port in standby mode or system self-test
	Red	Transmission disabled due to LLE, LLF, or user setting

3.3 Alarms

The L357 can generate Major and Minor Alarms.

- In the UCS 1000 and 1002, these alarms are forwarded over the backplane to the CIM and appear on the Major (MAJ) and Minor (MIN) CIM LEDs and then are forwarded to the DMM for monitoring and transfer to the Network Manager as traps.
- In the UCS 1001, the alarm outputs are forwarded to the chassis motherboard.

For details about the Alarm Output Configuration, Alarm Log, and Trap Configuration screens, see Chapter 4.

3.3.1 Link Loss Forwarding

When Link Loss Forwarding (LLF) is enabled, a fault on one side of the L357 propagates to the other side to notify that device and stops signal transmission (brings down the link). See Figure 3. Set the LLF propagation to User to Extension, Extension to User, or both directions. Set this in the User Interface or at Switches 5 and 6; for details on setting the Switches, see Chapter 2.



Figure 3. Link Loss Forwarding Propagation

3.3.2 Link Loss Echo

Caution: To avoid a lockup condition, do not set LLE at both the local and remote ends of the link.

Link Loss Echo (LLE) propagates a link loss to the device connected to an optical Extension or User Port on the L357. See Figure 4. If a link loss is detected on the Extension Port Rx, the Extension Port Tx is disabled, echoing the fault back to the source. LLE configures the L357 to not send data until it receives data. Set this in the User Interface.



Figure 4. Link Loss Echo Detection

Note: LLE on the optical Extension Port is available only when SBMC is disabled; if you enable SBMC, use LLF. A UTP to fiber L357 ignores the LLE User Port setting.

3.3.3 Loopback

The L357 supports four loopback modes that you can set at the local site for both the Local and Remote L357s. These modes loop the data through either the physical layer (PHY) on the User side or the FPGA. For details on setting loopback in software, see Section 4.6.

• Local-Local mode loops the electrical data that the Local L357 receives on the local User Port Rx through the FPGA to the User Port Tx. The data is not sent out the Extension Port Tx and incoming data on the Extension Port Rx is ignored. See Figure 5. To set this mode at the Diagnostics screen, set the Loopback State for the Local module to Local.



Figure 5. Local-Local Loopback Mode

• Local-Remote mode loops the optical data that the Remote L357 receives on the Extension Port Rx through the User PHY to the Extension Port Tx. The data is not sent out the remote User Port Tx and incoming data on the remote User Port Rx is ignored. See Figure 6. To set this mode at the Diagnostics screen, set the Loopback State for the Local module to Remote.



Figure 6. Local-Remote Loopback Mode

• Remote-Local mode loops the electrical data that the Remote L357 receives on the User Port Rx through the FPGA to the User Port Tx. The data is not sent out the remote Extension Port Tx and incoming data on the remote Extension Port Rx is ignored. See Figure 5. To set this mode, at the Diagnostics screen, set the Loopback State for the Remote module to Local.



Figure 7. Remote-Local Loopback Mode

• Remote-Remote mode loops the optical data that the Local L357 receives on the Extension Port Rx through the Local User PHY to the Extension Port Tx. The data is not sent out the local User Port Tx and incoming data on the local User Port Rx is ignored. See Figure 6. To set this mode, at the Diagnostics screen, set the Loopback State for the Remote module to Remote.



Figure 8. Remote-Remote Loopback Mode

For loopback, the L357 uses a unique MAC address that is listed on the Diagnostics screen as Loop Test MAC Address; for details about using the software and accessing the Diagnostics screen, see Chapter 4. In loopback mode, the L357 filters the incoming packets to identify the test packets through the MAC address. You can set two diagnostics options if you want to alter the data during loopback, Swap MAC Address at Loopback Point, which swaps the test MAC address with the source MAC address, and Recalculate CRC at Loopback Point. The test packets are returned to the source according to the selected mode.

Chapter 4 Management - VT-100

If the L357 is installed in a BAM, the system includes a DMM and a CIM, or the L357 is in a Model 1020 enclosure, you can manage the system through VT100 Terminal Emulation, which is accessible by a Telnet session, HyperTerminal or similar terminal emulation software, a standard SNMP network manager, and CanogaView.

4.1 VT100 Terminal Emulation

Connect the VT100 terminal emulation session to the DMM used in the UCS 1000 or 1002 chassis or to the BAM or Model 1020 enclosure. You cannot manage an L357 in a Model 1030 enclosure.

For details on the DMM, see the *Model 1500 Domain Management Module User Manual* (for UCS 1000) or *Model 1502 Domain Management Module User Manual* (for UCS 1002).

Setting up the VT100 session depends on which connection, serial port or Ethernet, you have available for access to the VT100 management program. Canoga Perkins suggests that you use HyperTerminal for your first session. You must set up TCP/IP for the DMM before you can use Telnet; for details, see the manual for the DMM.

4.2 PC Configuration for Terminal Operation

These steps briefly describe how to set up your PC for a terminal connection. For details on using Windows, see your Windows documentation.

- 1. Turn on your PC.
- 2. Accessories, the HyperTerminal Folder, and click HyperTerminal.
- 3. At the Connection Description dialog, select an icon, enter a name for the connection to the system, and click OK.
- 4. At the Connect To dialog, pull down the Connect using menu, select the COM port, and click OK.
- 5. At the COM Properties dialog, on the Port Settings tab, check for these selections:
 - Bits per second: 19200 bps
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
- 6. Click OK. HyperTerminal connects to the system and the VT100 terminal emulation starts.

4.3 Management User Interface

The Management User Interface for the L357 provides screens for setup, monitoring, and diagnostics. You can access the screens directly by connecting to the serial port of the BAM, the Model 1020, the DMM in the chassis, or by establishing a Telnet session with the DMM. For details, see the *Model 1500 Domain Management Module User Manual* (for UCS 1000) or *Model 1502 Domain Management Module User Manual* (for UCS 1002).

These sections discuss the screens for the L357, using a Telnet session for access.

4.3.1 General Screen Format

A typical screen, shown in Figure 9, includes standard descriptions and reference designations. Use this and other screens to configure the system, set operational parameters, and verify the system status. All screens use a common method for navigation.



Figure 9. General Screen Format

Not all screens and menus provide options that you can change. Some menu items reach screens that only report status, such as revision numbers, module type, or alarms. On other screens, you can move through and select options, and enter data.

Use these keys to navigate the screens:

- Space bar When a menu item is highlighted, press <Space> to cycle through all options for that item.
- Tab Press <Tab> to move the highlight to the next column to the right.
- Enter Press <Enter> to select the highlighted option for a menu item.
- Escape Press <Esc> to return to the previous screen.

4.3.2 User Interface Organization

The user interface consists of selectable, nested screens, available in this order:

Main Menu

- 1. System Configuration
 - 1. Hardware Configuration
 - 2. Functional Configuration
 - 3. Trap Configuration
 - 4. Alarm Output Configuration
 - 5. IP/SNMP Agent Configuration
 - 6. Host Access Table (for standalone enclosure, only)
 - 7. Trap/Notification Destination Table (for standalone enclosure, only)
 - 6. Security Configuration
 - 7. User Accounts
 - 1. or 3. Edit User Account
 - 8. System Information
- 2. Diagnostics
 - 1. Loopback Setup
 - 2. Remote Latency/Jitter Test
- 3. Link Status
- 4. System Alarms
- 5. Layer 2 Statistics
- 6. System Log
- 7. Utilities
 - 7. PING Generation (for standalone enclosure, only)
 - 8. Static ARP Table (for standalone enclosure, only)
 - 9. Dynamic ARP Table (for standalone enclosure, only)
- 8. Software Upgrade
- 9. Change Password (for standalone enclosure, only)
- 10. Connected Sessions (for standalone enclosure, only)

Some screen descriptions include detail about SPFs for reference; the information appears on-screen only when the L357 includes one or two SPFs.

This chapter describes each of these screen in detail.

4.3.3 Login Menu

The first screen is the Login Menu. If this is your initial setup and no password has been set, press <Enter> at the prompt for the password. Otherwise, type your password and press <Enter>.

4.3.4 DMM Main Menu

If you are using a DMM, after you log in, the Main Menu for the DMM appears. This is the main management screen for the DMM. For details on all menu options, see the *Model 1500 Domain Management Module Users Manual* (for UCS 1000) or *Model 1502 Domain Management Module Users Manual* (for UCS 1002). From this screen, you can access the L357 by either of two methods.

- To reach the L357 directly, follow these steps:
 - a. Type 4, "Manage or access a specific Module," and press <Enter>.
 - b. Type the slot and chassis numbers with a slash, such as "1/4" for chassis 1, slot 4, and then press <Enter>.
 - c. At the Module Menu, type 4, "Access User Interface," then press <Enter> to reach the Main Menu screen for the L357.
- To reach the chassis, and then select the L357, follow these steps:
 - a. Type 3, "Manage or access a specific Chassis," and press <Enter>, press <Space> to cycle between the chassis in the domain, and then press <Enter> to select the chassis.
 - b. At the Chassis Management screen, press <Space> to cycle to the slot number for the L357, then press <Enter> to reach the Main Menu screen for the L357.
- *Note:* In a UCS 1000 chassis, the slots in the BAM appear as A and B for the slot that the BAM is in.

4.4 L357 Main Menu

The Main Menu appears after you log in and provides access to all functions for the L357: setup, diagnostics, and reports. See Figure 10; options 9, 10, and 11 are available only when the L357 is in a standalone enclosure.

MAIN MENU

System Configuration
 Diagnostics
 Link status
 System Alarms
 Layer 2 Statistics
 System Log
 Utilities
 Software Upgrade
 Change Password
 Manage Logged In Users
 Logout

Figure 10. L357 Main Menu

4.5 System Configuration Menu

The System Configuration menu provides access to most configuration options for the L357. To access the System Configuration menu, see Figure 11 and Table 4 and follow these steps:

- 1. From the Main Menu, type 1, "System Configuration," and press <Enter>. The System Configuration menu appears.
- 2. To return to the Main Menu, press < Esc>.

SYSTEM CONFIGURATION

- 1) Hardware Configuration
- 2) Functional Configuration
- 3) Trap Configuration
- 4) Alarm Output Configuration
- 5) IP/SNMP Agent Configuration
- 6) Security Configuration
- 7) Account Configuration
- 8) System Info Configuration

Figure 11. System Configuration Menu

Configuration Option	Description
1) Hardware	Shows the model, type, revision and serial numbers, Alarm inputs, and Power Supply options; does not offer configurable options
2) Functional	Shows modem functions; you can update the configuration
3) Trap	Shows the trap configuration; you can enable/disable traps to the Network Manager
4) Alarm Output	Shows the alarm configuration; you can set each alarm parameter to Major, Minor or Off
5) IP/SNMP Agent	Shows the SNMP parameters if a Network Manager is in use and the L357 is in a Model 1020; you can set options.
6) Security	Shows parameters for passwords, lockout, and logout; you can set option
7) Account	Shows user account information; you can set options
8) System Info	Shows general information about the L357

Table 4. System Configuration Option Definitions

4.5.1 Hardware Configuration Screen

The Hardware Configuration report shows various configuration settings, including the module type, with model and revision numbers, and the power supply status. In addition, it shows information about the types of User and Extension ports. Use this information when troubleshooting, such as tracking down an error in a data link or the configuration. To view the Hardware Configuration screen, see Figure 12 and follow these steps:

- 1. From the Main Menu, type 1, "System Configuration," and press <Enter>. The System Configuration menu appears.
- 2. From the System Configuration menu type 1, "Hardware Configuration," and press <Enter>. This report shows the data rate, connector type, and wavelength (if fiber) for each port; see Figure 13.
- 3. To return to the System Configuration menu, press < Esc>.

	HARDWARE CONFIGURATION		
	Local	Remote	
Chassis Type	5U UCS 1000	2U UCS 1002	
Chassis/Slot	4/3B	2/5	
CLIM Type	L357-1113	L357-1113	
User Port	10/100/1000M/UTP/RJ45	10/100/1000M//UTP/RJ45	
Extension Port	100 1310 SM SC 10d	100 1310 SM SC 10d	
Serial Number	20030590295	20030590296	
Hardware Rev.	Al	A1	
Power Supply Pri	DC Non Iso	DC	
Power Supply Sec	AC 120/240	DC	
Fan Status	ОК	ОК	
Chassis Temperature	N/A	OK	

Figure 12. Hardware Configuration Screen

	REMOTE	HARDWARE	CONFIGURATION
Model Number	N525		
Hardware Rev.	В2		
Serial Number	20030590295		
User Port Model Number	500-3300		
User Port Description	10/100/1000	UTP	
User Port Hardware Rev.	CA		
User Port Serial Number	20030590296		
Ext Port Model Number	9400-528		
Ext Port Description	1000M LX 131	10/SM/7dB,	/SC
Ext Port Hardware Rev.	A1		
Ext Port Serial Number	20030590297		
Power Supply	AC 120/240		

Figure 13. Remote Hardware Configuration Screen

4.5.2 Functional Configuration Screen

The Functional Configuration report and menu provides information about the hardware, with options to set software control. You can only view the options for the Remote module, but you can set options for the Local L357 to work with the Remote module. For details about how RMTF, LLE, and LLF interact, see "Section 3.3" on page 3-3. Two reported hardware switch functions depend on the type of module:

- An L357 with a UTP User port ignores the LLE User settings.
- An L357 with a fiber User port ignores the User Speed/Duplex settings.

In addition, a system that supports 1000 BASE UTP ports allows only one port set to Master; all others must be set to Slave.

To access the Functional Configuration screen, see Figure 14 and Table 5 and follow these steps:

- 1. From the Main Menu, type 1, "System Configuration," and press <Enter>. The System Configuration menu appears.
- 2. From the System Configuration menu type 2, "Functional Configuration," and press <Enter>.
- 3. At the Functional Configuration screen, type the number for an item and press <Enter>, then press <Space> to cycle through the options and press <Enter> to select an option for the Local L357.
- 4. To return to the System Configuration menu, press < Esc>.

Chassis/Slot User Port Speed/Duplex Switch Settings:	FUNCTIONAL CONFIGURATION Local 4/3B 1000M/Half	V Remote 2/5 1000M/Half
User Port Speed/Duplex Side Band Mgmt LLF Extension to User LLF User to Extension	1000M/Full Enabled Disabled Disabled	Autonegotiate Enabled Disabled Disabled
 Configuration Option Control User Port Setting Ext Port Setting RMTF/LLE Link Loss Fwd Remote Configuration 	Hardware 1000M/Half Autonegotiate Disabled Disabled	Hardware Autonegotiate Autonegotiate Disabled Disabled

Figure 14. Functional Configuration Screen (UTP to Fiber L357)

Menu Item	Description
1) Configuration Option Control	Software: set the L357 to follow settings in software and ignore hardware switches Hardware: set the L357 to follow hardware switches
 2) User Port Setting AND 3) Ext Port Setting 	Set the User and Ext Ports to specific data rate, 10M, 100M, or 1000M; and duplex, half or full, options; to automatic rate and duplexing; or disable a port
4) RMTF/LLE	Set to User LLE or Disable
5) Link Loss Fwd	Set to User to Extension, Extension to User, Both directions, or Disable LLF
6) Remote Configuration	If the remote device is a 9145 or N525, this option appears; it opens the Remote Configuration menu that allows you to set up selected parameters on the remote device; see Figures 15 through 19

Table 5. Functional Configuration Option Definitions

REMOTE CONFIGURATION

1) Functional Configuration

2) VLAN Configuration

3) VLAN ID Translation Table

4) P-Bit Translation Table

5) Local Configuration

Figure 15. Remote Configuration Menu

REMOTE FUNCTIONAL CONFIGURATION

Use Ext	er Port Speed/Duplex Port Speed/Duplex	100M/Full 1000M/Full
1)	User Port Setting	100M/Full
2)	Ext Port Setting	1000M/Full
3)	1000Base-T Master/Slave	User Master/Ext Slave
4)	RMTF	Disabled
5)	Link Loss Fwd	Both Directions
6)	Flow Control	Disabled
7)	PVST+BPDU Filtering	Disabled
8)	Sideband Management	Enabled

Figure 16. Remote Functional Configuration Screen

		REMOTE VLAN CON	IFIGURATION
		User Port	Ext Port
1)	Drop Untagged Packet?	No	No
2)	Drop Packets with VLAN Tag	ſ	
	not matching VLAN Tag A?	No	No
3)	Remove outermost VLAN Tag?	No No	No
4)	Add VLAN Tag B to Untagged	l	
	Packets only?	No	No
5)	Add VLAN Tag C to Tagged		
	Packets only?	No	No
6)	Add VLAN Tag C to Tagged		
	Packets only using P-Bits		
	of outermost VLAN tag?	No	No
7)	Tag A VLAN ID (0 - 4095)	0	0
8)	Tag B VLAN ID (0 - 4095)	0	0
	Priority (0 - 7)	0	0
9)	Tag C VLAN ID (0 - 4095)	0	0
	Priority (0 - 7)	0	0

Figure 17. Remote VLAN Configuration Screen

REMOTE VLAN TAG TRANSLATION TABLE

	User	Port	Ext P	ort
	In VLAN	Out VLAN	Out VLAN	In VLAN
1)	1	3	54	2
2)	2	2	3	2
3)	0	0	0	0
4)	0	0	0	0
5)	0	0	0	0
6)	0	0	0	0
7)	0	0	0	0
8)	0	0	0	0
9)	Enable VI	LAN		
	Translat	ion? No		No

Figure 18. Remote VLAN Tag Translation Table Screen

```
REMOTE P-BIT TRANSLATION TABLE
```

						User Port	Ext Port
1)	Incoming	P-Bit	0	translated	to	0	0
2)	Incoming	P-Bit	1	translated	to	1	1
3)	Incoming	P-Bit	2	translated	to	2	2
4)	Incoming	P-Bit	3	translated	to	3	3
5)	Incoming	P-Bit	4	translated	to	4	4
6)	Incoming	P-Bit	5	translated	to	5	5
7)	Incoming	P-Bit	6	translated	to	б	б
8)	Incoming	P-Bit	7	translated	to	7	7
9)	P-Bit Tra	anslati	lor	n Enabled?		No	No

Figure 19. Remote P-Bit Translation Table Screen

4.5.3 Trap Configuration

Traps are messages to alert network management about conditions. The DMM logs the traps and the DMM or Model 1020 transmits them by SNMP to the network manager. At the Trap Configuration screen, enable or disable traps individually or use the "Master Trap Control" to enable or disable all traps. See Figure 20. To configure traps, follow these steps:

- 1. From the Main Menu, type 1, "System Configuration," and press <Enter>. The System Configuration menu appears.
- 2. From the System Configuration menu type 3, "Trap Configuration," and press <Enter>.
- 3. At the Trap Configuration menu, type the number for a trap and press <Enter>.

Note: "Master Trap Control" enables or disables all traps. The factory default is Disabled.

- 4. Press <Space> to cycle to Enabled or Disabled, then press <Enter>.
- 5. To return to the System Configuration menu, press < Esc>.

	TRAP	CONFIGURATION
1)	Master Trap Control	Disabled
2)	Extension Port Link Traps	Enabled
3)	Remote Fault Received Traps	Enabled
4)	Link Loss Forwarding Traps	Enabled
5)	Link Loss Echo Traps	Enabled
6)	Remote User Port Link Traps	Enabled
7)	Local User Port Link Traps	Enabled
8)	Configuration Traps	Enabled
9)	Power/Fan/Temperature Traps	Enabled
10)	Cold Start Traps	Enabled
11)	Side Band Mgmt Channel Traps	Enabled
12)	Alarm Input Traps	Enabled
13)	Diagnostics Traps	Enabled
14)	Authentication Traps	Enabled

Figure 20. Trap Configuration Screen

4.5.4 Alarm Output Configuration

Use the Alarm Output Configuration screen to set any or all alarms to Major, Minor, or Off. See Figure 21 and Table 6. To configure alarms, follow these steps:

- 1. From the Main Menu type 3, "Alarm Output Configuration," and press <Enter>. The Alarm Output Configuration screen appears.
- 2. Type the number for the alarm you want to set and press <Enter>.
- 3. Press <Space> to cycle to Major, Minor, or Off, and press <Enter>.

ALARM OUTPUT CONFIGURATION

1)	Factory Defaults	
2)	Link Down Alarm	Off
3) 4)	RMIF Alarm LLF Alarm	Off
5)	Configuration Alarm	Off
6)	Power/Fan/Temperature Alarm	Minor
7)	SBMC Loss Alarm	Off
8)	Power-On Self Test Alarm	Off

Figure 21. Alarm Output Configuration Screen

Alarm	Description
2) Link Down	Loss of Signal (electrical)/Composite Loss of Signal (optical); one or both received signals fail; default is Off
3) RMTF	Not available
4) LLF	Link loss forwarded to module; default if Off
5) Configuration	Setup errors, including mismatches with other modules; default is Off
6) Power/Fan/Temperature	Power is low or fan is off; default is Minor
7) SBMC Loss	Sideband management signal lost; default is Off
8) Power-On Self Test	Module failed when power was turned on; default is Off

Table 6. Alarm Output Definitions

Note: You must enable the Alarm Output item on the System Status & Configuration screen for these settings to take effect.

4.5.5 IP/SNMP Agent Configuration

If the L357 is in a Model 1020, use the SNMP Configuration screen to view and set up the SNMP parameters on the L357. See Figure 22 and Table 7. To view SNMP parameters, follow these steps:

- 1. From the System Configuration menu type 5, "SNMP Configuration," and press <Enter>. The SNMP Configuration screen appears.
- 2. Type the number for the alarm you want to set and press <Enter>.
- 3. Type the information or value, and press <Enter>.
- 4. To return to the System Configuration menu, press < Esc>.

Local	Remote
00 40 2A 00 87 E3	00 40 2A 00 53 E7
UP	UP
172.016.148.030	172.16.143.10
255.255.000.000	255.255.0.0
000.000.000.000	172.16.1.1
000.000.000.000	192.0.0.83
VT100	VT100
Disabled	Disabled
Disabled	Disabled
	Both Ports
	Disabled
	1
	Local 00 40 2A 00 87 E3 UP 172.016.148.030 255.255.000.000 000.000.000.000 000.000.000 VT100 Disabled Disabled

Figure 22. IP/SNMP Agent Configuration Screen

Table 7.	SNMP	Configuration	Parameters	Description
----------	------	---------------	------------	-------------

Item	Description
1) Ethernet IP Address Subnet Mask Default Gateway	Enter the IP address for access through the Ethernet network, the mask that sets the network ID part of the IP address, and the address of the network node that connects to another network
2) SLIP/PPP IP Address	Enter the IP address for access through SLIP or PPP
3) Serial Port Config	Set the type of serial port connection: VT100, SLIP, or PPP
4) BOOTP	Enable this if the module needs to obtain its IP address from a BOOTP server; when the unit has an IP address, disable BOOTP
5) Host Table	Access the Host Table screen (for standalone enclosure, only)
6) Trap Table	Access the Trap Table screen (for standalone enclosure, only)
8) Inband Management Port	Set the port that will receive management packets; can be Ext. only, User only, Both ports, or No Management
9) Management VLAN	Enable or disable the Management VLAN
10) Management VLAN Number	Set the number for the VLAN; range is 0-4095

The SNMP agent allows access to up to 24 Host IP addresses listed in the Host Table. Set up the Host information for the L357 on the Host Table screen. See Figure 23. To access the Host Table, follow these steps:

- 1. From the SNMP Configuration menu, type 13, Host Table, and press <Enter>. The Host Table screen appears.
- 2. To add a Host, type 1 and press <Enter>, or to edit a Host, type 3 and press <Enter>, then follow the prompts to enter values to set the access and protocol parameters.
- 3. To delete a host, type 2 and press <Enter>, then at the prompt, select the Host.
- 4. To return to the SNMP Configuration menu, press <Esc>.

		HC	OST ACCI	ESS TABLE			
Managing Host	Telnet	FTP	SNMP	SNMP	V1/V2c Rd	V1/V2c Wr	V1/V2c
IP/Mask Bits	Access	Access	Access	Protocol	Community	Community	Access
172.016.002.232/32	Yes	FTP	Write	V1/V2c/V3	public	netman	Superv
172.002.002.232/32	Yes	FTP	None	V1/V2c/V3	public	netman	Observ
172.016.142.001/32	Yes	Both	Write	V1/V2c/V3	public	netman	Observ

Figure 23. Host Access Table Screen

The Trap/Notification Destination Table screen lists information about and options to set up hosts to receive notification of traps and alarms. To access the Trap/Notification Destination Table screen, see Figure 24 and follow these steps:

- 1. From the SNMP Configuration menu type 7, "Trap Table," and press <Enter>.
- 2. At the Trap/Notification Destination Table screen, type 1 to edit a host or 2 to add a host at the Edit Notification Destination Entry screen, or type 3 to remove a host.

Note: To add or edit a host entry, follow the prompts on the notification destination entry screen.

3. To return to the SNMP Configuration menu, press < Esc>.

		TRAP/NOTIF:	ICATION DESTINATION '	TABLE
Managing		Trap	Username/	Security
Host	Port	Туре	Community	Level
172.16.14.200	163	V1-Trap	public	N/A
172.16.100.20	162	V2c-Trap	public	N/A
172.16.142.1	163	V3-Trap	public	Auth/No Priv

|--|

4.5.6 Security Configuration

The Security Configuration menu provides options to set values for general parameters for passwords, lockout, and logout. To access the Security Configuration screen, see Figure 25 and Table 8 and follow these steps:

- 1. From the System Configuration menu type 6, "Security Configuration," and press <Enter>.
- 2. At the Security Configuration screen, type the number for an item and press <Enter>, then press <Space> to cycle through the options and press <Enter> to select an option.
- 3. To return to the System Configuration menu, press <Esc>.

	SECURITY CO	NFI(GURATION
]	PASSWORD CONFIGURATION		
1.	Minimum Length	:	0
2.	Minimum Alpha Characters	:	0
3.	Minimum Numeric Characters	:	0
4.	Minimum Punctuation Characters	:	0
5.	Maximum Consecutive Character Types	:	0
б.	Maximum Same Character	:	0
7.	Allow username in password	:	Disabled
8.	Password Expiration Time	:	0
9.	Password Reuse Count	:	0
]	LOCKOUT/LOGOUT CONFIGURATION		
10.	Lockout After Failed Attempts	:	0
11.	Lockout Type	:	Hard
	Lockout time	:	0
12.	Display Lockout Message	:	Disabled
13.	Lockout Message	:	Account has been locked out
14.	Lockout Craft Port	:	Disabled
15.	Inactivity Logout time (mins)	:	0

Figure 25. Security Configuration Screen

Menu Item	Description
1. Minimum Length	Define characteristics of passwords; the range for all
2. Minimum Alpha Characters	fields is from 0 through 15
3. Minimum Numeric Characters	
4. Minimum Punctuation Characters	
5. Maximum Consecutive Character	
Types	
6. Maximum Same Character	
7. Allow username in password	Enable or disable the username appearing as or within the password
8. Password Expiration Time	Set how often in days, 1 through 365, that the passwords must be reset; $0 = disabled$

Table 8. Security Configuration Option Definitions

Menu Item	Description
9. Password Reuse Count	Set whether the password must be changed or can be used again immediately; values are 0 (new password can be the same) or 1 (new password must be different)
10. Lockout After Failed Attempts	Set how many times, from 1 to 10, that a user can try to log in before a lockout; $0 = disabled$
11. Lockout Type Lockout time	Set the type of lockout: Hard requires another user with admin access to unlock the account on the User Accounts screen; Timed requires that the user wait for Lockout time before trying again; Lockout time is from 0 (none) to 30 minutes
12. Display Lockout Message13. Lockout Message	Enable or disable and set the message, up to 30 characters, that appears at lockout
14. Lockout Craft Port	Disable access to the serial port to prevent any unauthorized access; to re-enable the craft port, run a Telnet session
15. Inactivity Logout time (mins)	Set the time, between 1 and 30 minutes, before automatic log-out with no activity; $0 = disabled$

4.5.7 User Accounts Screen

The User Accounts screen provides options to set values for parameters for specific users. To access the User Accounts screen, see Figure 26 and follow these steps:

1. From the System Configuration menu type 7, "Account Configuration," and press <Enter>.

		US	ER ACCOUNTS		
	Account	Access	Access		Locked
Username	State	From	Level	Description	Out
admin	Enabled	UI/SNMPv3	Supervisor	Upgrade Account	No

Figure 26. User Accounts Screen

- 2. To add a user, type 1, or to edit an existing user, type 3, and press <Enter>, then type the Username and follow the prompts on the Edit User Account screen to enter values or press <Space> to cycle through options for these parameters:
- Account State: enabled or disabled
- Access From: UI, SNMPv3, or UI/SNMPv3
 - UI indicates access through Telnet, Console, SSH, FTP, or SFTP, and requires additional parameter setup
 - SNMPv3 enhances security and requires additional parameter setup
- Access level: Supervisor, Operator, or Observer
- Description: optional; up to 17 characters

- UI Password: password that allows access through Telnet, Console, SSH, FTP, or SFTP; 8 to 15 characters
- UI Password Expires: Yes or No
- UI Password Expires in (days): 0 (never) to 365
- Allow UI Lockout of User: Yes or No; can disable access for this user after excessive failed attempts to log in
- Allow UI Logout of User: Yes or No; can automatically log user out after excessive inactivity
- UI Logout Locked State: shows current state as Locked, Unlocked, Logged out, or Logged in
- SNMPv3 Authentication Protocol: MD5, SHA, or None; sets how to authenticate the user
- SNMPv3 Authentication Password: password that generates the authentication key for the user if the authentication protocol is MD5 or SHA; 8 to 15 characters.
- SNMPv3 Authentication Key: Shows the key that authenticates the user for MD5 or SHA Authentication Protocol; this is generated automatically for the Authentication Password, but can be changed if the user's host uses a different Authentication Key generation algorithm; 16 Hex characters for MD5 protocol or 20 Hex characters for SHA protocol.
- SNMPv3 Privacy Protocol: DES or None; sets the protocol for encryption
- SNMPv3 Privacy Password: password that generates the encryption key for the user if the privacy protocol is DES; 8 to 15 characters
- SNMPv3 Privacy Key: Shows the key that encrypts messages for DES Privacy Protocol; this is generated automatically for the Privacy Password, but can be changed if the user's host uses a different Privacy Key generation algorithm; 16 Hex characters
- 3. To delete a user, type 2, then follow the prompts to select the user name and confirm the choice; the User Accounts screen reappears.
- 4. To return to the System Configuration menu, press < Esc>.

4.5.8 System Information Screen

The System Information menu provides options to enter general information about this module in the system. To access the System Information screen, see Figure 27 and follow these steps:

- 1. From the System Configuration menu type 8, "System Info Configuration," and press <Enter>.
- 2. At the System Information screen, type the number for an item and press <Enter>, then follow the prompts to type in your information.
- 3. To return to the System Configuration menu, press < Esc>.

		System	Information	_	Local	Unit
1.	System Name	:				
2.	Contact	:				
3.	Location	:				
4.	Customer	:				
5.	Information	:				
		:				
б.	Circuits	:				
		:				
7.	Service Code	:				
8.	Date-in-Service	:				
9.	Date-Out-of-Service	:				
10.	Equipment Type	:				
11.	Equipment Code	:				
12.	Vendor	:				
13.	CLEI	:				
14.	Mfg Date	:				
15.	Unit	:				

Figure 27. System Information Screen

4.6 Diagnostics Screen and Loopback

Use the Diagnostics menu for troubleshooting the L357; you can view current loopback conditions and set up loopback. See Figure 28.

DIAGNOSTICS

1) Loopback Setup

Figure 28. Diagnostics Screen

Use the Loopback Setup screen to view current loopback conditions and set up loopback conditions for troubleshooting the L357. See Figure 29 and Table 9. For details about using loopback, see Chapter 3. To run a loopback test, follow these steps:

- 1. From the Main Menu, type 2, "Diagnostics," and press <Enter>. The Diagnostics menu appears.
- 2. From the Diagnostics menu, type 1, "Loopback Setup," and press <Enter>. The Loopback Setup screen appears.
- 3. Type the number for the loopback option you want to set, press <Tab> to highlight the Remote column if needed, press <Space> to cycle through the options, and press <Enter>.
- 4. When you finish running Loopback, press <Esc> to return to the Diagnostics menu, then press <Esc> to return to the Main Menu

Note: The Model 1030 enclosure does not support loopback options.

	DIAGNOSTICS	
Chassis/Slot	Local 4/3B	Remote 2/5
Loopback Switch Setting:	N/A	N/A
Loop Test MAC Address:	00 40 2A 80 58 32	00 40 2A 80 58 33
 Loopback Option Control Loopback State Swap MAC Address 	Software Disabled	Software Disabled
at Loopback Point?	Yes	Yes
at Loopback Point?	Yes	Yes

Figure 29. Diagnostics Screen

Selection	Description
Loopback Switch Setting	Shows hardware setting only when in a Model 1020; Local, Remote, or Normal
Loop Test MAC Address	Shows unique MAC address for destination of loopback packets
1) Loopback Option Control	Set to Hardware (option for Model 1020 only) or Software
2) Loopback State	Set to Local, Remote, or Clear All Loopbacks
3) Swap MAC Address at Loopback Point?	Set to Yes or No; use to run loopback packets through a switch
4) Recalculate CRC at Loopback Point?	Set to Yes or No; use to run loopback packets through a switch

4.7 Link Status Screen

Use the Link Status screen to view the current link conditions on the L357. See Figure 31. To view link status, follow these steps:

- 1. From the Main Menu, type 3, "Link Status," and press <Enter>. The Link Status screen appears.
- 2. When you finish checking the Link Status, press <Esc> to return to the Main Menu.

LINK STATUS

Chassis Slot	Local 4 3B	Remote 2 5
User Port	Link Up	Link Up
Extension Port	Link Up	Link Up

Figure 30. Link Status Screen

4.8 System Alarms

Use the System Alarms screen to view alarms and faults on the L357. See Figure 31. To view alarm status:

- 1. From the Main Menu, type 4, "System Alarms," and press <Enter>. The System Alarms screen appears.
- 2. When you finish checking the Alarm status, press <Esc> to return to the Main Menu.

SYSTEM ALARMS

	Local	Remote
Configuration Errors	No	No
User Port	Up	Up
Extension Port	Up	Up
Remote Fault User/Ext	N/A	N/A
Ext Port Remote Fault	No	No
Link Loss Echo User/Ext	No	No
Link Loss Fwd Ext->User	No	No
Link Loss Fwd User->Ext	No	No
Side Band Mgmt Channel	OK	OK
Chassis Management	OK	OK
Alarm Relay Inputs	N/A	N/A
Power Supply Primary	OK	OK
Power Supply Secondary	OK	OK
Fan	OK	OK
Chassis Temperature	N/A	OK

Figure 31. System Alarms Screen

4.9 Layer 2 Statistics

Use the Layer 2 Statistics screen to view data transfer protocol statistics on the L357. See Figure 31. To view layer 2 statistics, follow these steps:

- 1. From the Main Menu, type 5, "System Alarms," and press <Enter>. The Layer 2 Statistics screen appears.
- 2. To reset the counters, press <Ctrl-R>.
- 3. When you finish checking the statistics, press <Esc> to return to the Main Menu.

		LAYER 2 STATISTICS				
	Local	Local	Remote	Remote		
	User Port	Ext Port	Ext Port	User Port		
Link State	UP	UP	UP	UP		
Speed/Duplex	1000M/FULL	1000M/FULL	1000M/FULL	1000M/FULL		
Frames Sent	28207788	28319769	28200427	28200710		
Frames Rcvd	28319769	28207788	28200711	28200426		
Bytes Sent	837493720	926021313	831705864	831880780		
Bytes Rcvd	926020552	837494685	831881457	831705499		
Undersize (< 64)	0	0	0	0		
Frames > 1518	0	0	0	0		
Oversize (>10000)	0	0	0	0		
CRC Errors	0	0	0	0		
Fragments	0	0	0	0		
Collisions	0	0	0	0		
Late Collisions	0	0	0	0		
Dropped	0	0	0	0		
Frames Sent Rate	7802/s	7796/s	7815/s	7802/s		
Frames Rcvd Rate	7796/s	7802/s	7802/s	7815/s		

Figure 32. Layer 2 Statistics Screen

4.10 System Log

Use the System Log screen to view a list of user actions with date and time. See Figure 33.

As events fill the System Log, older events drop off to make room for new events. Event Types include System, which involves system-level resources; Trap, also reported to the Network Manager; and Security, which shows security information and violations. A * Local event indicates that the user has an account defined on the local User Account screen; other users can log in through a DMM.

To access the System Log screen, follow these steps:

- 1. From the Main Menu, type 6, "System Log," and press <Enter>.
- 2. At the System Log screen, type F to view the first entry, N to view the next entry, P to view the previous entry, L to view the last entry, or C to clear the log.
- 3. To return to the Main Menu, press < Esc>.

	SYSTEM	I LOG			
Description	Туре	Username	Local	Date/Time	
Local User Port Link Up					
	Trap	SYSTEM	*	02-Oct-2003	13:17:36.68
Side Band Management Onl	line				
	Trap	SYSTEM	*	02-Oct-2003	15:28:15.80
Log initialized					
	Trap	SYSTEM	*	02-Oct-2003	16:30:14.00
user attempted to login	with inval	id passwor	ď		
	Security	SYSTEM	*	02-Oct-2003	16:37:11.60
Cold Start					
	System	SYSTEM	*	02-Oct-2003	16:37:14.80
user logged in					
	Trap	admin	*	02-Oct-2003	16:59:26.60
Select [(F)irst, (N))ext, {P)re	ev, (L)ast,	(C)lea	ar]	

Figure 33. System Log Screen

4.11 Utilities

Use the Utilities screen to set the time and date, reset a configuration, or enable or disable the remote console port. See Figure 34 and Table 10. To access the Utilities screen, follow this step:

- 1. From the Main Menu, type 6, "Utilities," and press <Enter>. The Utilities menu appears.
- 2. To return to the Main Menu, press <Esc>.

UTILITIES

```
    Set Date and Time
    Reset Configuration To Default
    Reset Remote Configuration To Default
    Remote Craft Port: Enabled
    Modem/Slip/PPP Baud Rate 19200
    Modem Initialization String AT
    PING generation
    Static ARP Table
    Dynamic ARP Table
```

Figure 34. Utilities Menu Screen

Table 10.	Utilities N	Menu Options
-----------	-------------	--------------

Item	Definition
1) Set Date and Time	Change the time and date information for the modem if needed; if in a chassis with a DMM, the DMM date and time overrides the L357
2) Reset Configuration To Default3) Reset Remote Configuration To Default	Restores all configurable settings to the defaults except for: date and time; password; BOOTP; Telnet timeout
4) Remote Craft Port	Enable or disable the console port on the remote module

Item	Definition
5) Modem/Slip/PPP Baud Rate	Select the baud rate, 9600, 19200, 38400, 57600, or 115200 bps for the modem/SLIP/PPP serial port (standalone enclosure, only)
6) Modem Initialization String	The default string is "AT" (standalone enclosure, only)
7) PING Generation	Access the PING diagnostics screen (standalone enclosure, only)
8) Static ARP Table	Set or change specific IP and MAC addresses (standalone enclosure, only)
9) Dynamic ARP Table	View current IP and MAC addresses (standalone enclosure, only)

4.11.1 PING Generation

Use the PING Generation screen to test the connection to a specific IP address. See Figure 35.

PING Generation

```
IP Address to PING: 0.0.0.0
PING count (1 to 255, 0 = forever): 0
```

Figure 35. PING Generation Screen

To use PING to check a connection, follow these steps:

- 1. From the Main Menu, type 7, "Utilities," and press <Enter>.
- 1. From the Utilities menu, type 7, "PING Generation," and press <Enter>.
- 2. At the PING menu prompt, set the PING parameters, and press <Enter>. "PING response received..." indicates a good connection; "TIMEOUT: Unable to reach [IP address]..." indicates a faulty connection.
- 3. To stop the PING, press < Esc>.

4.11.2 Static ARP Table

Use the Static ARP Table to set specific IP and MAC addresses for up to 10 ports. See Figure 36.

	S	STATIC ARP TABLE	
	IP Address	MAC ADDRESS	Port
1.	172.16.2.7	00-90-37-56-6C-34	
2.	172.16.3.23	00-7C-25-33-57-9C	

Figure 36. Static ARP Table Screen

To use view, set, or remove an address, follow these steps:

- 1. From the Main Menu, type 7, "Utilities," and press <Enter>.
- 2. From the Utilities menu, type 8, "Static ARP Table," and press <Enter>.
- 3. At the prompt, type 1 to add an entry or 2 to remove an entry, and follow the prompts.
- 4. To return to the Utilities menu, press <Esc>.

4.11.3 Dynamic ARP Table

Use the Dynamic ARP Table to view the currently assigned IP and MAC addresses for various ports. See Figure 37.

		DYNA	MIC ARP TABLE		
IP Address	MAC ADDRESS	Port	IP Address	MAC ADDRESS	Port
170 16 0 00	00 00 00 00 00 01	2			
1/2.10.2.82	00-98-2C-BE-27-01	3			
172.16.153.6	00-50-54-C3-33-41	4			
172.16.142.1	00 90 27 4F D1 8D	3			

Figure 37. Dynamic ARP Table Screen

To use view an address, follow these steps:

- 1. From the Main Menu, type 7, "Utilities," and press <Enter>.
- 2. From the Utilities menu, type 9, "Dynamic ARP Table," and press <Enter>.
- 3. To return to the Utilities menu, press <Esc>.

4.12 Software Upgrade

Use the Software Upgrade report and menu screen to check the current version of the firmware and upgrade it and the remote L357, if necessary. To access the Software Upgrade screen and check the software version, see Figure 38 and follow these steps:

- 1. From the Main Menu, type 8, "Software Upgrade," and press <Enter>. The Software Upgrade screen appears.
- 2. Record the numbers for the Active and Inactive Firmware for both the local and remote modules.
- 3. Access the Canoga Perkins Web site, click Downloads, scroll to the L357 file name and compare the version numbers listed there with the version numbers you recorded. The L357 firmware file name is similar to L3570106.zip, where L357 indicates the module and 0106 indicates the version number.
- 4. Download the software from the Web site to your local TFTP server.

		SOF"	TWARE U	JPGRADE	
		Local			Remote
Acti	lve Firmware	01.19			01.19
Inac	ctive Firmware	01.17			01.17
Boot	code	05.04			05.04
1)	Software Reset	Reset			Reset
2)	Swap Bank	Swap			Swap
3)	Copy Software f	From Source	unit t	o Destination	unit

⁴⁾ Get New File with TFTP

Figure 38. Software Upgrade Screen

Caution: To ensure compatibility when two or more units are connected, you must upgrade all connected units with the same software.

If the firmware on the L357 is outdated, you need to upgrade it. If the L357 is in a chassis or 1030 enclosure within a domain with a DMM, go to the User Manual for the DMM and use that procedure to install the new software. If the L357 is in a Model 1020, follow these steps:

- 1. If needed, access the SNMP Configuration menu before starting the software upgrade: enter the IP address, subnet Mask, and default gateway for the SNMP agent.
- 2. From the Main Menu, type 8, "Software Upgrade," and press <Enter>.
- 3. At the Software Upgrade menu, type 4, Get New File with TFTP, and press <Enter>.
- 4. At the prompts, type the IP address for the TFTP server and the File Name.
- 5. At the prompt, type Y to transfer the file and start the upgrade.

To upgrade a remote unit to the same version of software, follow these steps:

1. From the Main Menu, type 8, "Software Upgrade," and press <Enter>.

- 2. At the Software Upgrade menu, type 3, "Copy Software from Source unit to Destination unit," and press <Enter>.
- 3. At the prompt, select the Source, which is the inactive bank for the local module, then select the Destination, which is the inactive bank for the remote module, and press <Enter>; the upgrade runs automatically.

To run the new software, swap banks, and reset the module, follow these steps:

- 1. From the Main Menu, type 8, "Software Upgrade," and press <Enter>.
- 2. At the Software Upgrade menu, type 2, "Swap Bank," press <Tab> to highlight the Remote column, and press <Enter>.
- 3. Type 2, "Swap Bank," check that the Local column is highlighted, and press <Enter>. Both modules reset and start using the new firmware.

4.13 Change Password

If the L357 is in a standalone enclosure, you can update your password in order to maintain system security. You cannot change the password for any other users, especially those who are not logged in. To access the Change Password screen, follow these steps:

- 1. From the Main Menu, type 9, "Change Password," and press <Enter>.
- 2. To change the password, follow the prompts on the screen.
- 3. To return to the Main Menu, press < Esc>.

4.14 Manage Connected Sessions

If the L357 is in a standalone enclosure, you can use the Connected Sessions screen to view all currently logged in users and force a user off, if necessary. See Figure 39. To access the Software Upgrade screen and check the software version, follow these steps:

- 1. From the Main Menu, type 10, "Manage Logged In Users," and press <Enter>. The Connected Sessions screen appears.
- 2. To force a user off, type the number for that session, and press <Enter>.
- 3. To return to the Main Menu, press < Esc>.

CONNECTED SESSIONS Session Type Username Access Description Console AT LOGIN MENU * 1. Telnet admin Supervisor 2. Telnet admin Supervisor * = Current session

Figure 39. Connected Sessions Screen

Chapter 5 Maintenance and Troubleshooting

5.1 General Maintenance

Well-maintained components and clearly identified cables help assure optimum system operation. Damaged fiber cables and dirty connectors are a common source of signal loss or attenuation. Single mode and multimode fiber optics are especially sensitive to contamination. Inspect, clean, and test all components to maintain optimum performance.

Note: To avoid damage and signal loss, do not over-tighten or force-fit optical connectors.

- To clean the ferrules and end-face surfaces of male fiber couplings, use a lint-free pad saturated with isopropyl alcohol.
- To clean the female fiber connectors, use canned air.
- To prevent damage and contamination, place protective dust caps on all unused optical connectors.

5.1.1 Manage Cable Links

Plan to manage the cables to ensure trouble-free operation and maintenance tasks.

• Position and secure the fiber optic cables to prevent excessive bends and damage. Follow the guidelines for the bend radius for specific fiber cables.

Note: If no minimum bend radius is specified, the typical long-term, low-stress radius is not less than 15 times the cable diameter (based on Federal Standard FS-1037C).

- Always connect the fiber optic cables in the standard Tx to Rx and Rx to Tx scheme.
- Label each cable near each end with the signal direction, source, and destination to minimize connection errors.

5.1.2 Check Optical Power Levels

To ensure the proper performance levels, measure the fiber link loss, or link attenuation, for all fiber links. Each L357 is shipped with a document that lists the output power for each laser transmitter. To determine link attenuation, use either the L357 Tx source or a hand-held 1310/1550 nm laser source, a fiber optic test jumper cable (with known loss), and an optical power meter.

Note: For accurate results, warm up each unit for at least 30 minutes before checking power levels.

The transmission laser in the L357 turns on automatically when the chassis receives power.

5.1.3 Measure Transmitter Output Power

To measure the output power, follow these steps:

- 1. Clean the connectors on the fiber optic test cable, then plug it in to the Tx connector on the L357.
- 2. Warm up each component for at least 30 minutes.
- 3. Set the optical power meter to the proper wavelength.
- 4. Wait two or three minutes for the power reading to stabilize, and then read the output power.
- 5. Subtract out the test cable loss, then record the power level and compare it to the value on the performance sheet for that particular L357. Measurement tolerance is +/- 0.5 dBm.
- *Note:* When referencing optical power levels with numerical values less than zero, the reading closer to zero is the greater value; for example, -17 dBm is greater than -20 dBm.
- 6. If the reading is incorrect, repeat the measurement with a different test cable. If the power level is still not within range, call Technical Support.
- 7. After calculating the link attenuation, subtract that value from the L357 Tx output value to determine the power expected at the remote cable end, which is the input power at the remote receiver.

5.1.4 Measure Receiver Input Power

If you know the link attenuation, skip this section. Otherwise, follow these steps to use the L357 to measure the link attenuation.

- 1. At the local site, connect the fiber link cable to Tx on the L357.
- 2. At the remote site, set the optical power meter to the proper wavelength and connect it to the fiber link cable.
- 3. Record the optical power level and compare it with the sensitivity level listed on the data sheet for the link fiber type.
- 4. Subtract the remote power level from the value for the transmitter output power at the local site. The result provides the link loss, in dB. This power level must not exceed the limit for Rx sensitivity listed on the data sheet for the remote unit.
- *Note:* If you cannot determine the Rx sensitivity, contact Canoga Perkins Technical Support Department for assistance.

5.1.5 Measure Fiber Link Attenuation

Determine and record link attenuation before starting normal link traffic. The attenuation factor identifies potential problems with links that are on the threshold of receiver limitations.

Measure optical fiber links at the shortest wavelength of operation to determine the limiting factor in the loss budget. Each device that transmits to an L357 has a loss budget that is specified by the manufacturer and recorded on a data sheet provided with the equipment. That loss budget must be greater than the total of the measured loss of the fiber link and the attenuation of the L357s.

Use a power meter calibrated for the laser source, then factor in approximately 1 dB for the connector loss from the patch cables between the L357 and the local device. (Each fiber connection can generate 0.5 dB of additional loss.)

Note: Consider this measurement when extending the link at WWDM wavelengths because the shorter wavelengths have a greater loss.

To measure attenuation:

- 1. Attach the transmit fiber to the local and remote ends of the link.
- *Note:* To avoid damage, do not over-tighten or force-fit the optical connectors.
- 2. With a properly calibrated optical power meter, measure the optical power on the fiber that will be connected to the Rx connector at one site. Record this reading.

Note: Use either a hand-held power meter or other similar measuring device.

3. Repeat this process at the other site.

5.2 Troubleshooting

This section describes fault conditions and corrective action. The multifunction LEDs and the alarms display all failures.

As a rule, whenever there is a significant signal loss, check the fiber path and the minimum bend radius for potential problems. Remove and inspect the cable connectors, being careful not to damage the fiber end-face surface or the connector housing. Clean all optical connectors before reinstalling them.

5.2.1 LED Indicators

For details on the LED status during a normal start-up, see Chapter 3.

The front panel LEDs show both normal and fault conditions. Additional information about fault conditions appears in the System Alarms and System Status & Configuration screens. To aid troubleshooting, Table 3 lists the functions of the front panel LEDs.

5.2.2 New Installation

On new installations, make sure that all steps in Chapter 2 are complete:

- 1. Check that the STA LED is green.
- 2. Check that the fiber type (multimode or single mode) matches the L357 optical mode.
- 3. Make these checks:
 - All fiber cabling is of the same type; do not mix multimode and single mode cables.
 - The fiber optic cable is within the specifications and loss budget of the optic interface module.
 - The line length between the L357 and the remote link does not exceed the allowable loss budget or overdrive limit.
 - All host modules in the link are turned on.
 - All fiber cables are connected Tx to Rx and Rx to Tx.

5.2.3 Switch 1 and 2 Settings Ignored

If the L357 was installed in a UCS 1000 or 1002 and set in the User Interface to software control, it ignores the hardware switch settings. To restore it to hardware control, access the Utilities screen and reset the configuration to default. For details on setting the L357 hardware switches, see Chapter 2.

5.2.4 Problems With Fiber Optics

If the System Alarms screen shows that an Extension Port link is down, inspect and clean the cables and connectors, then replace any damaged fiber. Retest modules after cleaning.

Chapter 6 Specifications

See also the specifications for the chassis or standalone enclosure.

6.1 L357 Specifications

Physical Specifications

Dimensions:	3.0"H x 1.0"W x 9.0"D (7.6 cm x 2.5 cm x 22.8 cm)
Weight:	0.3 lb. (0.136 Kg)
Operating Temperature:	0° to 50° C
Operating Humidity:	Up to 90% (non-condensing)
Power Consumption:	5 VDC 800 mA, Maximum
Optical Connectors:	SC

Regulatory Compliance

- ETL, ETLc (UL 60950/CSA C22.2 No. 60950)
- EN 60950
- EN 60825-1
- FCC Part 15B, Class A
- EN 55022
- EN 55024
- EN 61000-3-2
- EN 61000-3-3
- R&TTE Directive (EN 300-386)
- C-Tick (AS/NZS 3548)
- NEBS Level 3 Tested and Certified
- CE Mark

6.2 L357 Models

Model	Fiber Optic Options, Extension Port
1000Base-T to User Port: 10/	1000Base-X 100/1000M UTP RJ45
L357-1110	1000BASE SX 850 nm MM 6 dB SC
L357-1113	1000BASE LX 1310 nm SM 7 dB SC
L357-1323	1000BASE LD 1310 nm SM 14 dB SC
L357-1333	1000BASE XD 1310 nm SM 21 dB SC
L357-1533	1000BASE ZX 1550 nm SM 21 dB SC
L357-1543	1000BASE EX 155 0 nm SM 23 dB SC

1000Base-T to User Port: 10/	1000 Mbps BIDI Interfaces 100/1000M UTP RJ45
L357-1354	Single Fiber 1000 Mbps 1310 nm 20 Km
L357-1564	Single Fiber 1000 Mbps 1550 nm 20 Km
1000Base-T to User Port: 10/	1000 Mbps CWDM Optical Interfaces 100/1000M UTP RJ45
L357-1070	1000 Mbps CWDM 1470 nm SM 22 dB SC
L357-1071	1000 Mbps CWDM 1490 nm SM 22 dB SC
L357-1072	1000 Mbps CWDM 1510 nm SM 22 dB SC
L357-1073	1000 Mbps CWDM 1530 nm SM 22 dB SC
L357-1074	1000 Mbps CWDM 1550 nm SM 22 dB SC
L357-1075	1000 Mbps CWDM 1570 nm SM 22 dB SC
L357-1076	1000 Mbps CWDM 1590 nm SM 22 dB SC
L357-1077	1000 Mbps CWDM 1610 nm SM 22 dB SC
1000Base-SX t User Port: 100	to 1000Base-X 00M SX 850 nm MM 6 dB SC
L357-2110	1000BASE SX 850 nm MM 6 dB SC
L357-2113	1000BASE LX 1310 nm SM 7 dB SC
L357-2323	1000BASE LD 1310 nm SM 14 dB SC
L357-2333	1000BASE XD 1310 nm SM 21 dB SC
L357-2533	1000BASE ZX 1550 nm SM 21 dB SC
L357-2543	1000BASE EX 1550 nm SM 23 dB SC
1000Base-SX t User Port: 100	to BIDI 00M SX 850 nm MM 6 dB SC
L357-2354	Single Fiber 1000 Mbps 1310 nm SM 20 Km
L357-2564	Single Fiber 1000 Mbps 1550 nm SM 20 Km
1000Base-LX t User Port: 100	to 1000Base-X 00M LX 1310 nm SM 7 dB SC
L357-3110	1000BASE SX 850 nm MM 6 dB SC
L357-3113	1000BASE LX 1310 nm SM 7 dB SC
L357-3323	1000BASE LD 1310 nm SM 14 dB SC
L357-3333	1000BASE XD 1310 nm SM 21 dB SC
L357-3533	1000BASE ZX 1550 nm SM 21 dB SC
L357-3543	1000BASE EX 1550 nm SM 23 dB SC

1000Base-LX to BIDI User Port: 1000M LX 1310 nm SM 7 dB SC		
L357-3354	Single Fiber 1000 Mbps 1310 nm SM 20 Km	
L357-3564	Single Fiber 1000 Mbps 1550 nm SM 20 Km	
1000Base-SX to 1000 Mbps CWDM Optical Interfaces User Port: 1000M SX 850 nm MM 6 dB SC		
L357-2070	1000 Mbps CWDM 1470 nm SM 22 dB SC	
L357-2071	1000 Mbps CWDM 1490 nm SM 22 dB SC	
L357-2072	1000 Mbps CWDM 1510 nm SM 22 dB SC	
L357-2073	1000 Mbps CWDM 1530 nm SM 22 dB SC	
L357-2074	1000 Mbps CWDM 1550 nm SM 22 dB SC	
L357-2075	1000 Mbps CWDM 1570 nm SM 22 dB SC	
L357-2076	1000 Mbps CWDM 1590 nm SM 22 dB SC	
L357-2077	1000 Mbps CWDM 1610 nm SM 22 dB SC	
1000Base-LX to 1000 Mbps CWDM Optical Interfaces User Port: 1000M LX 1310 nm SM 7 dB SC		
L357-3070	1000 Mbps CWDM 1470 nm SM 22 dB SC	
L357-3071	1000 Mbps CWDM 1490 nm SM 22 dB SC	
L357-3072	1000 Mbps CWDM 1510 nm SM 22 dB SC	
L357-3073	1000 Mbps CWDM 1530 nm SM 22 dB SC	
L357-3074	1000 Mbps CWDM 1550 nm SM 22 dB SC	
L357-3075	1000 Mbps CWDM 1570 nm SM 22 dB SC	
L357-3076	1000 Mbps CWDM 1590 nm SM 22 dB SC	
L357-3077	1000 Mbps CWDM 1610 nm SM 22 dB SC	

Appendix A Warranty Information

Current Warranty information is available on-line in the Client Login Area of the Canoga Perkins web site (www.canoga.com) or by contacting Technical Support at 800-360-6642 (voice) or fiber@canoga.com (email).

Appendix B Acronym and Abbreviation List

BAM	Bus Access Module
CIM	Chassis Interconnect Module
DMM	Domain Management Module
FPGA	Field Programmable Gate Array
LLE	Link Loss Echo
LLF	Link Loss Forwarding
LNK	Link
Mbps	Megabits per second
MDM	Modem
MMF	Multimode Fiber
PHY	Physical Layer
RMTF	Remote Fault
Rx	Receive signal
SBMC	Side-Band Management Channel
SM	Single Mode
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
TRM	Terminal
Tx	Transmit signal

CANOGA PERKINS CORPORATION



20600 Prairie Street Chatsworth, California 91311-6008 USA Phone: (818) 718-6300 FAX: (818) 718-6312 Web Site: www.canoga.com Email: fiber@canoga.com