CANOGA PERKINS

EdgeAccess

N525
Ethernet Termination
Service Unit
User Manual

NOTICE

Canoga Perkins has prepared this user 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.)

Website: www.canoga.com
Email: fiber@canoga.com

EdgeAccess®
N525 Ethernet Termination Service Unit
User Manual
Model Number N525-UM
Part Number 6913301
Rev. J 10/2010
sw 6.50

For Technical Advisories and Product Release Notes, go to the Canoga Perkins website, www.canoga.com.

CAUTION!

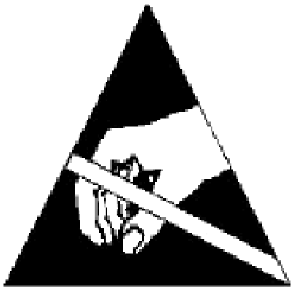
This product may contain a laser diode emitter operating at a wavelength of 1300 nm - 1600 nm. Use of optical instruments (for example: collimating optics) with this product may increase eye hazard. Use of controls or adjustments or performing procedures other than those specified herein may result in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

ATTENTION!

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'avérer 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.



NOTICE!

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 électrostatiques. Il doit absolument être manipulé en respectant les règles de mise à la terre afin de prévenir de telles décharges.

Table of Contents

List of Figures

List of Tables

Chapter 1
Overview

The N525 Series 10/100/1000BASE Ethernet Termination Service Unit terminates Metro Ethernet Services and extends Local Area Networks (LANs) located up to 100 Km apart. Key features are:

- Layer 2 statistics
- VLAN assignment and stacking
- Priority bit (P-Bit) marking
- Alarm information reporting
- Local and remote diagnostic loopback
- Remote software upgrade
- Remote control and monitoring through the SideBand Management Channel (SBMC)

The N525 receives and transmits 10/100/1000BASE Ethernet data on UTP copper cable, single mode fiber optic cable, or multimode fiber optic cable. The N525 supports two hot-swappable, plug-in interface modules. The interface modules include tri-speed (10/100/1000 Mbps) UTP and a variety of 850nm, 1310nm, 1550nm, CWDM Wavelength, and Single Fiber BiDi optical interfaces at 10 Mbps, 100 Mbps and Gigabit. Optical interfaces are listed in Chapter 5.

The N525 front panel, shown in Figure 1, includes:

1. User and Extension ports; supports UTP, ST, SC and LC connectors (depending on Interface Module Type).
2. RS-232 Serial Management Port; support VT100 Terminal emulation and SLIP/PPP
3. Status LEDs:
    - STA shows N525 status
    - CFG shows configuration and setup status
    - 100, 1000, and half/full duplex, depending on the type of module, show status for the User port
    - LNK/RX and TX pairs for the User and Extension ports show that data is received and transmitted

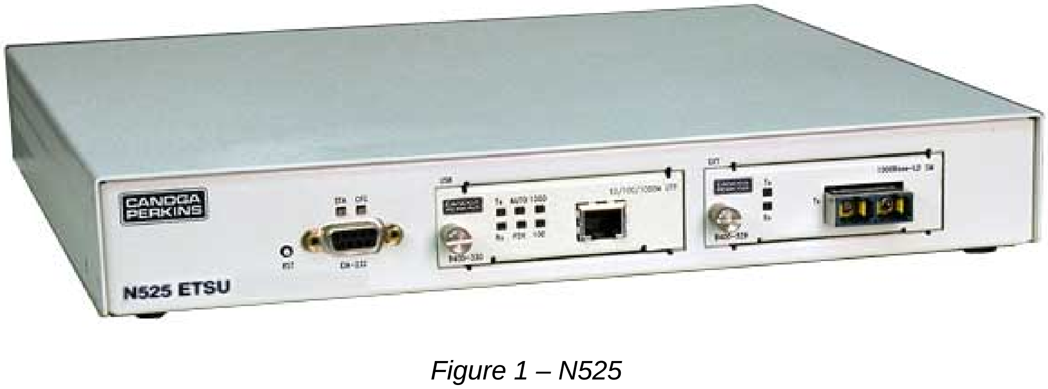


Figure 1 – N525

Management Security

The N525 supports enhanced security for access to Management Functions. Four network security protocols are supported: SNMPv3, Remote Access Dial In User Security (Radius), Secure Shell version 2 (SSH-2) and Secure File Transfer Protocol (SFTP). You can set values and options within the software that will work with the security protocols on your network; for specific information, see the documentation for your implementation. In addition, the N525 supports strong passwords, independent of the security protocol.

1. SNMPv3 provides authentication and encryption across a network.
2. The Radius server maintains user account information. At login, it authenticates the username and password and sends a message to the N525 to allow the login. The Radius server can also be set up to require additional authentication information before accepting the user. If the username or password is not valid, the Radius server sends a message to the N525 to disallow the login and reject the user. Set up the parameters for the N525 on the Radius Client Configuration screen.
3. SSH-2 provides authentication and encryption for a secure remote connection that is similar to a standard Telnet connection, but more secure. Set up the SSH access option individually for each User Account.
4. SFTP adds encryption to protect uploaded files during the file transfer process, such as for a software update.
5. In software, the Security Configuration Menu provides nine options to define password characteristics, as well as parameters that configure lockout and logout for failed access attempts.

Network Performance Assurance

Network Performance Assurance (NPA) is not available in this version of the N525.

Chapter 2
Setup and Installation

This section describes how to set up and install the N525 and its interface modules.

Before setting up the N525, make sure a 9 pin RS-232 cable is available (required to connect the N525's Management Port to a VT100 type terminal or PC for setup and configuration).

Caution: ***Connect the serial cable to the RS-232 management port on the N525 after the PC has booted up. Booting up the PC with the serial cable connected to the N525 might cause the PC to load an incorrect driver, resulting in an erratic cursor on the PC.***

Installing the N525

The N525 is tested and inspected before shipment from the factory. If there is obvious damage to the shipping container, contact the carrier immediately.

Caution: ***Follow electrostatic discharge (ESD) safety precautions when handling Canoga Perkins products, as with all electronic devices with static sensitive components.***

1. Unpack the N525. Keep the shipping container until the unit is installed and fully operational. In the unlikely event that the unit is defective, contact Canoga Perkins Customer Service for a Return Authorization Number (RMA) and instructions for return shipment. Additional Warranty and Product Return information is in Appendix A.

2. The N525 can be rack mounted, wall mounted, or placed on a shelf or any other flat surface.

    a. Rack Mounting: To rack mount the N525, attach Rack Mount Kit 1802-2008 for 19" racks, or Rack Mount Kit 1802-2009 for 23" racks. The Rack Mount Kits includes mounting brackets and screws to attach the brackets to the N525. The brackets attach to the three threaded holes on the side of the N525 toward the front. Be sure to place the Lock Washer between the Screw Head and Bracket as shown figure 5.

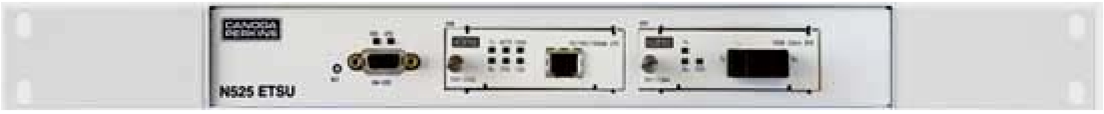


Figure 2 – N525 with 19" Rack Mount Brackets

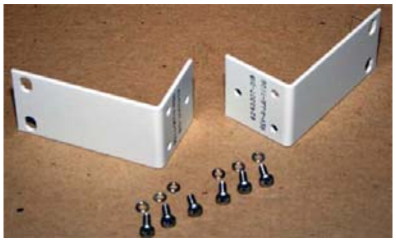


Figure 3 – 19" Rack Mount Kit

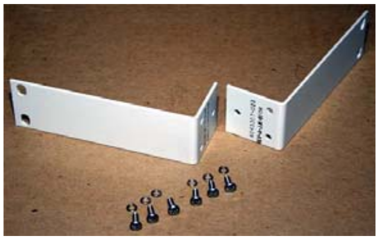


Figure 4 – 23" Rack Mount Kit

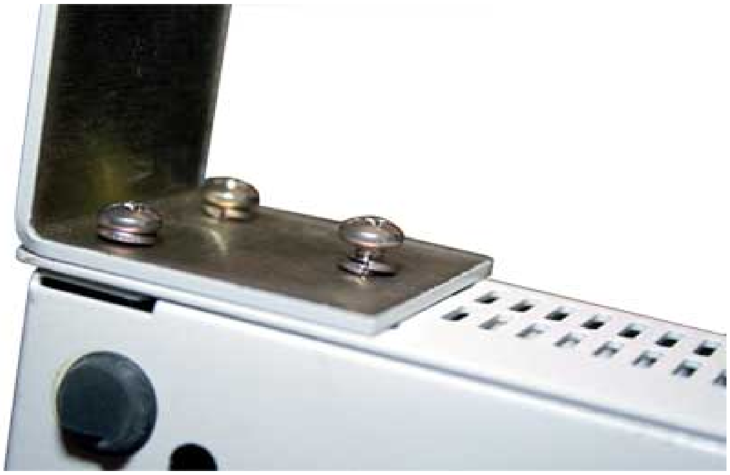


Figure 5 – Bracket Attachment Detail

b. Wall mounting: The N525 has slotted holes on the bottom of the unit for wall mounting. The N525 requires 1" unobstructed space above and below the N525 for ventilation. Canoga Perkins recommends a space of 5" on the right and 3" on the left of N525 bee left unobstructed to facilitate Interface Module Access, Cable Access and Power Entry.

- Install two #10 or #12 screws and anchors in the wall 9 3/8" apart, 1" from the sides and 3/4" from the top of the desired location of the N525. A template is illustrated below. Leave the screws protruding from the wall 3/8" to 3/4".
- Hang the N525 on the screws, matching the keyholes in the N525 to the screws.

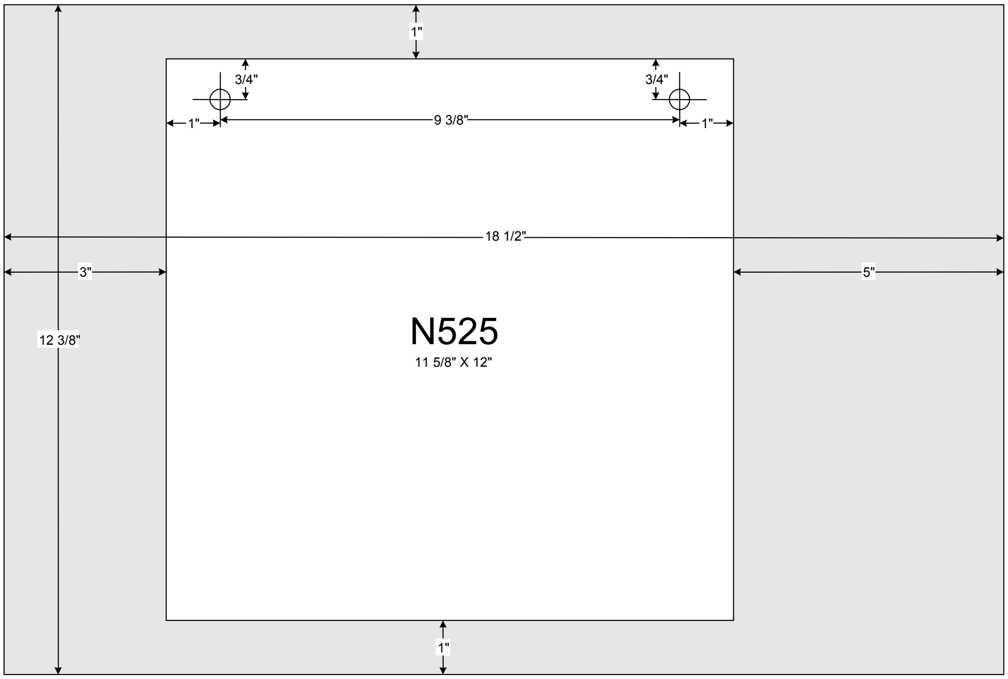


Figure 6 – Wall-Mount Template

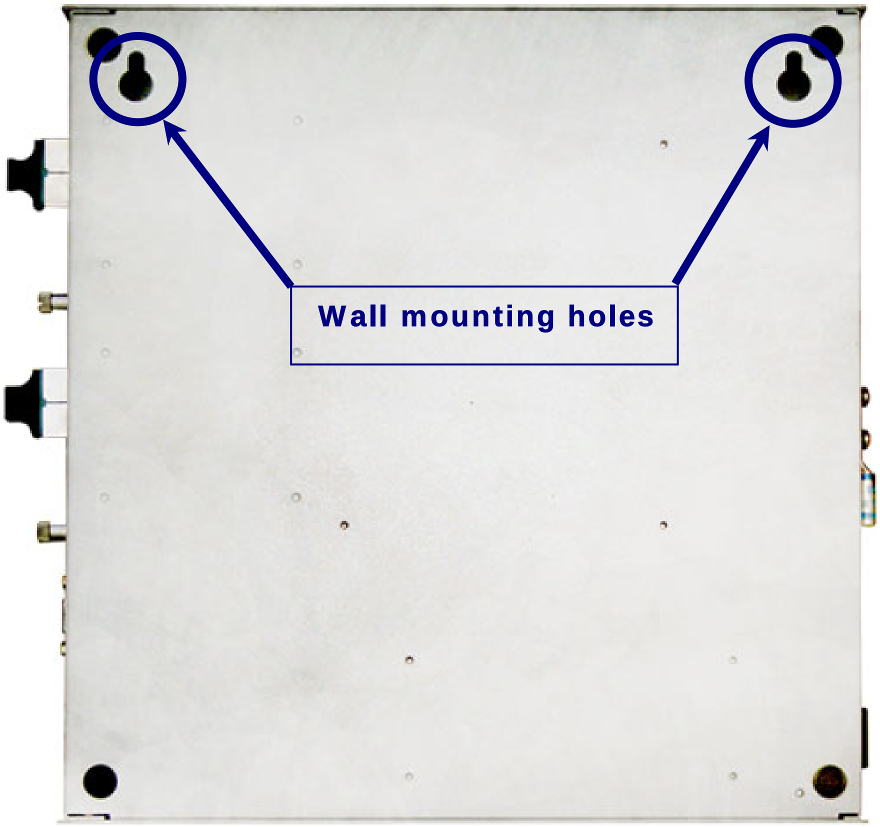


Figure 7 – Bottom of N525 showing wall mounting holes

c. Desktop/Shelf Placement: Place the N525 on a secure, flat surface within reach of the power and fiber optic cables. Leave clearance on the sides (1”), front (5”) and rear (3”) for ventilation and to facilitate Interface Module Access, Cable Access and Power Entry.

3. Insert Interface Modules:

   a. Determine which Interface Modules are for the Extension (EXT) and User (USR) Ports.

   b. Insert a module into the appropriate slot and push firmly on the center of the front panel. If it does not seat properly, pull the module out, inspect for bent connector pins. If there are bent pins or other obstructions, contact Canoga Technical Support for instructions. If all appears normal, reinsert.

   c. When firmly seated, hand-tighten the screw on the Module’s front panel.

4. Connect Chassis Ground: The rear of the N525 has a Grounding Lug for connecting the N525 to Earth Ground. This is required for full electrical safety. Attach a 6 Gauge copper cable between the Ground Lug and Earth Ground.

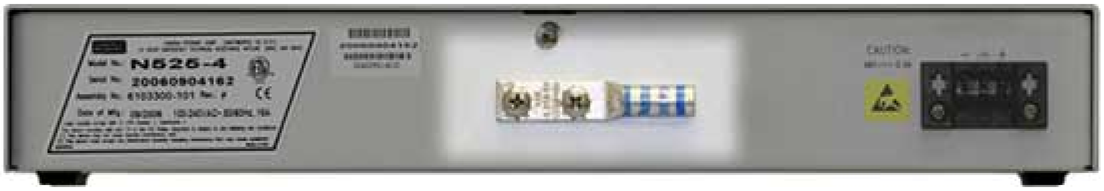


Figure 8 – Ground Lug Location

5. Connecting power. The N525 is available with either AC or DC power.

   a. Connect the AC power as follows:

      - Plug the AC power cord into the socket at the rear of the N525 and the AC outlet.

      - The N525 is shipped with a North American Power Cord. The unit uses a standard IEC AC Power Connector. Country specific power cords are available locally for installations outside North America.

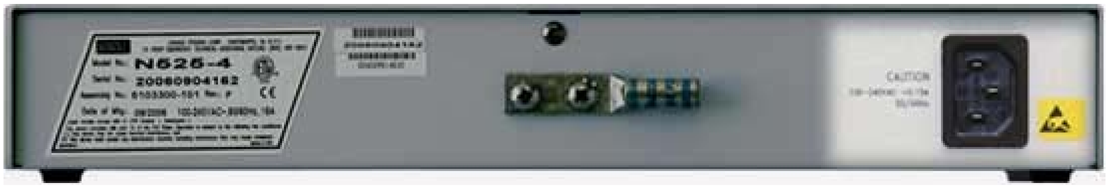


Figure 9 – AC Power Connector Location

Caution: ***Reversing Power and Ground Leads can damage both the DC source and the N525. Damage due to reversing power is not covered under the Warranty.***

b. Connect the DC power as follows:

- The N525 support both Positive and Negative grounded DC Power. Loosen the screws for the GND and +48 or -48 VDC terminals
- Slide the wires under the square washers, and tighten the screws taking care not to cross Power and Ground. The DC Power Terminal Block is removable for ease of installation and replacement. It is recommended the Terminal Block be removed when connecting power to avoid accidentally crossed or shorted power leads from damaging the N525 or your DC Power System.
- Use an ohmmeter to verify that +/- 48 VDC Power lead is not shorted to GND.
- Connect the power cables to the power source.
- Insert the Power Terminal Block into the N525.

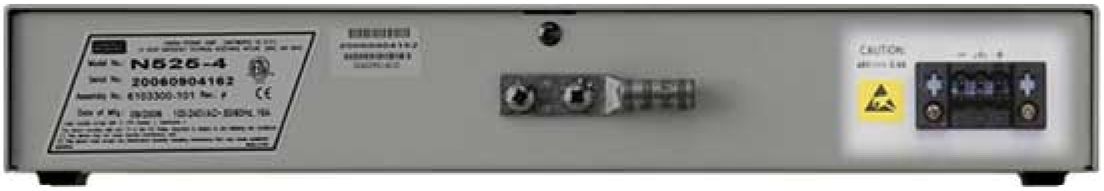


Figure 10 – DC Power Connector Location

6. Dirty optical connectors are a common cause 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.

   a. 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.

   b. Use canned air to blow dust out of the female fiber coupler.

7. Connecting Optical Fiber to Optical Interface Modules:

   a. Plug in the optical cables with Tx (optical output) to Rx (optical input), Rx to Tx orientation.

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

8. Connecting Ethernet Cables to UTP Interface Modules:

   a. Plug the shielded Ethernet Cable into the UTP Connector on the Interface Module.

   b. Be sure the locking tab properly seats.

   c. If the locking tab is broken or missing, replace the cable.

Caution: ***To maintain Lighting and Power Shorting protection, always use Ethernet Cables with a proper Ground Shield cable and connector.***

9. Canoga Perkins recommends you label the cables with the circuit number or other identifier and the signal direction on optical cables (TX or RX).

10. Canoga Perkins recommends that you determine and record optical link attenuation and transmission power before starting normal link traffic. The fiber optic cable optical attenuation and Laser output power determine receive optical power level at the receiving device. Reductions in Laser power or increases in optical loss on the fiber optic cable can cause degraded performance and link outages. For details on link attenuation and Laser output power, see Chapter 4.

Power-Up and Front Panel Functions

The LEDs on the front panel show the system and port status. The *STA* and *CFG* LEDs display management status. Interface Module has two, three or six LEDs; actual number is dependent on Interface Module type.

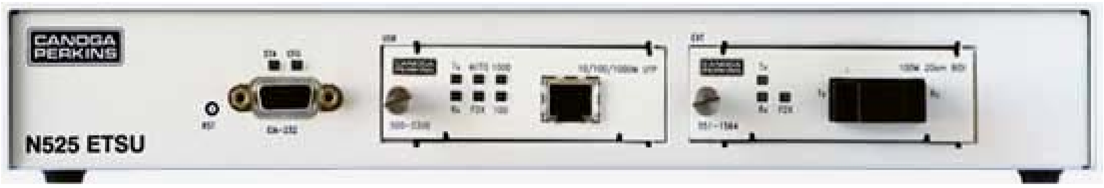
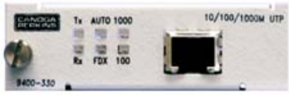


Figure 11 – N525 Front Panel

 *Figure 12 – UTP 10/100/1000 Mbps*	 *Figure 13 – 10Mbps Optical Module*
 Figure 14 – 100Mbps Optical Module	 *Figure 15 – 1000Mbps Optical Module*

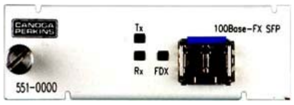


Figure 16 – 100Mbps SFP Module

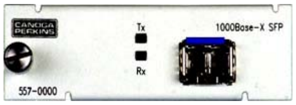


Figure 17 – 1000Mbps SFP Module

During power-up, all LEDs on the N525 and Interface Modules light amber. When start-up has completed, the LEDs on the N525 display status is described in Table 1. Interface Modules display status is described in Table 2.

Table 1 – N525 Front Panel LEDs

LED	Status	Description
STA	Off	No Power
	Green	Normal Operation
	Amber	System Self-Test, Local Loopback
	Amber blinking	Downloading File, Remote Loopback
	Red	Link Down, Major alarm
CFG	Off	SBMC is Disabled
	Green	SBMC is Enabled
	Amber	System Self-Test
	Red	Configuration Error, Remote N525 OS Different Version

Table 2 – Interface Module LEDs

LED	Status	Description
Rx	Modules	All: UTP; 10, 100, 1000 Mbps Optical, SFP
	Off	No activity
	Green	Link Established
	Green blinking	Receiving activity
	Amber blinking	Collisions
	Amber	System self-test
	Red	Remote fault
Tx	Modules	All: UTP; 10, 100, 1000 Mbps Optical, SFP
	Off	No transmission activity
	Green blinking	Transmission activity
	Amber	Port paused
	Red	Port disabled; may be due to LLF
FDX	Modules	UTP; 10, 100 Mbps Optical, 100 Mbps SFP
	Off	Half duplex mode
	Green	Full duplex mode

LED	Status	Description
100	Modules	UTP Module Only
1000	100 Off, 1000 Off	10 Mbps data rate
	100 Green, 1000 Off	100 Mbps data rate
	100 Off, 1000 Green	1000 Mbps data rate

Chapter 3
Management

The N525 has three management interfaces:

- A VT100 terminal interface, available on the RS-232 serial port and through Telnet
- The SideBand Management Channel, available when connected to another N525, to an L351 Media Converter, or to an L357 Ethernet Service Unit
- SNMP

Telnet and SNMP access to the N525 can use either the user data stream (in-band) or the RS-232 serial port when it is configured for PPP or SLIP operation. The SideBand Management Channel is a out-of-band management communication path on the Extension port that communicates with the distant N525, L351 or L357.

Note: If Connectivity Loss Detection (CLD) is enabled and you need to make some other configuration change on the N525, you should disable CLD first. CLD is disabled by default.

Setting Up VT100 Terminal Network Management on the RS-232 Serial Port

When using the RS-232 serial port for VT100 sessions, Canoga Perkins suggests that you use HyperTerminal[1] or other VT100 terminal emulation program when using a PC. The VT100 Telnet terminal interface is only available after the management TCP/IP configuration is complete.

The steps below briefly describe how to set up HyperTerminal on your PC. For details on using MS Windows[2], see your Windows documentation.

1. At your MS Windows desktop, click Start, then highlight Programs, Accessories, the HyperTerminal Folder, and then click HyperTerminal.
2. At the Connection Description dialog, select an icon, enter a name for the connection to the system, and click OK.
3. At the Connect To dialog, pull down the Connect using menu, select the COM port, and click OK.

[1] [2] HyperTerminal and MS Windows are registered trademarks of Microsoft Corporation

4. 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
5. Click OK. HyperTerminal connects to the system and the VT100 terminal emulation starts.
6. Select the Properties button on the Hyperterminal window tool bar, click on the settings tab, and change emulation from Auto Detect to VT100.

Setting Up SNMP Network Management

Typically, the N525 communicates with CanogaView or your network management platform in-band using the transported Ethernet network.

Network Management Platform Setup

Industry standard Management Information Bases (MIBs) are required on your network management platform in order to successfully communication with the N525 using SNMP. Before you start, check that these industry-standard MIBs are loaded:

1. Standard MIB
2. Dot2sd.mib
3. Etherlike.mib
4. If.mib
5. Bridge.mib
6. Pbridge.mib

Additionally, Canoga Perkins Private MIBs are need on the network management platform. The Canoga Perkins Private MIBs are available on Canoga Perkins website, www.canoga.com. The MIBs are located in a password protected area of the website. If you do not yet have a Canoga Perkins username and password, please contact Tech Support.

1. Cp.mib: Supports all Canoga Perkins products
2. Cpsysinf.mib: Supports SNMP access
3. Cphost.mib: Supports Host Table and Host Access functions
4. Cptraptb.mib: Supports the Trap Table

N525 Setup

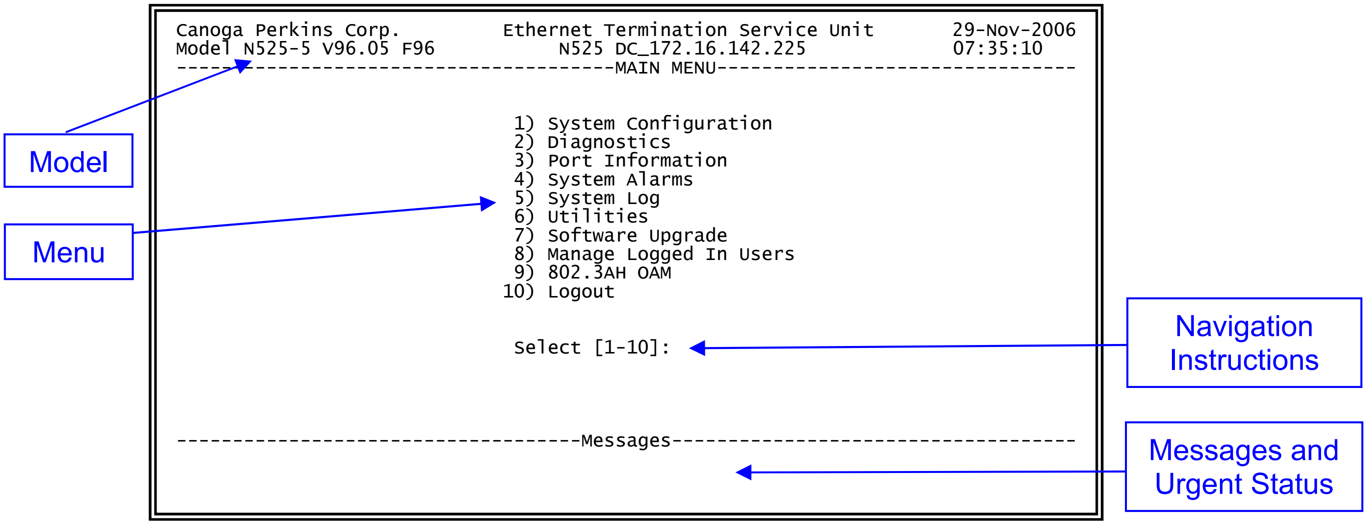
There are several TCP/IP and SNMP parameters that need configuration before accessing the N525 from CanogaView or your network management platform. These parameters include TCP/IP Address, Authorized Host list and privileges. These parameters are initially using VT100 Terminal on the RS-232 serial port. Please see the System Configuration section for details on configuring these parameters.

Management User Interface

The Management User Interface for the N525 provides screens for setup, monitoring, and diagnostics. You can access the screens directly by connecting to the serial port of the N525 or using Telnet.

General Screen Format

A typical screen, shown in Figure 20, 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.



```
Canoga Perkins Corp.         Ethernet Termination Service Unit        29-Nov-2006
Model N525-5 V96.05 F96              N525 DC_172.16.142.225            07:35:10
--------------------------------------MAIN MENU-------------------------------

                              1) System Configuration
                              2) Diagnostics
                              3) Port Information
                              4) System Alarms
                              5) System Log
                              6) Utilities
                              7) Software Upgrade
                              8) Manage Logged In Users
                              9) 802.3AH OAM
                             10) Logout

                              Select [1-10]:



-----------------------------------Messages------------------------------------
```

Figure 20 - 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> once to cancel changes for the selected item or to return to the previous screen; press <Esc> two or more times to return to the Main Menu from two or more menu levels deep.

User Interface Organization

The user interface consists of selectable, nested screens, available in this order; this chapter describes how to use these screens:

Main Menu

System Configuration

- IP/SNMP Agent Configuration
  - Management IP Configuration
  - Auxiliary IP Configuration
  - Host Table
  - Trap Table
- Trap Configuration
- Security Configuration
- Account Configuration
- System Information
- Radius Client Configuration
- SNTP Client Configuration
- SYSLOG Client Configuration
- Hardware Information

Diagnostics

- Loopback Setup
- Latency/Jitter Test
- Ping Generation
- Connectivity Loss Detection
  - CLD Configuration
  - CLD Profile
  - CLD Trap Configuration
  - CLD Statistics

Port Information

- Link Status
- Port Configuration
  - Hardware Information
  - Functional Configuration
  - VLAN Configuration
    - VLAN Rules
    - VLAN ID Translation Table
    - P-Bit Translation Tables
  - Port Filters
- Layer 2 Statistics

  3.1. RMON Group 1 Statistics

System Alarms

System Log

Utilities

- Set Date & Time
- Reset Configuration To Default
- Change Password
- VT100 Baud Rate
- Slip/PPP Baud Rate
- Ping Generation
- Static ARP Table
- Dynamic ARP Table
- License Manager

Software Upgrade

Manage Logged in Users

802.3AH OAM

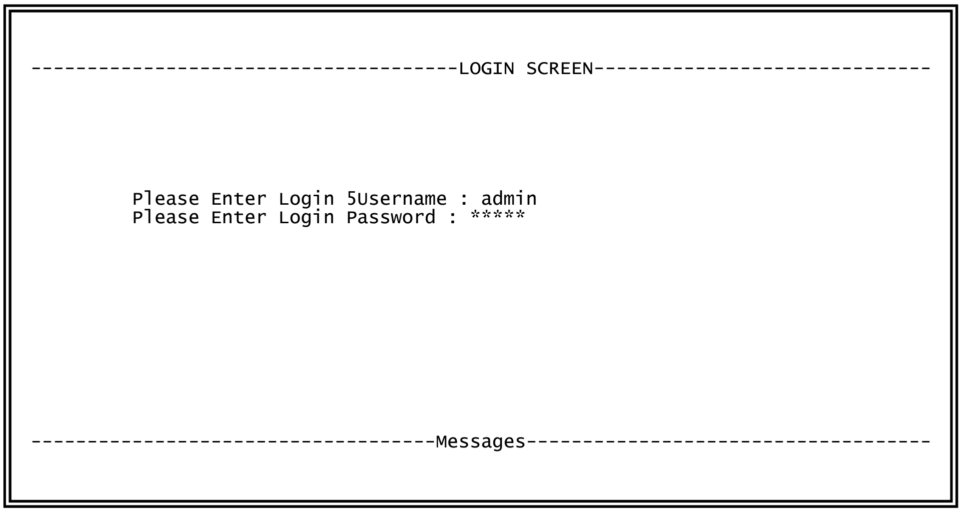
- OAM Control
- OAM Peer Information
- OAM Statistics
- OAM Event Configuration
- OAM Event Log

Logout

Login and Main Menu

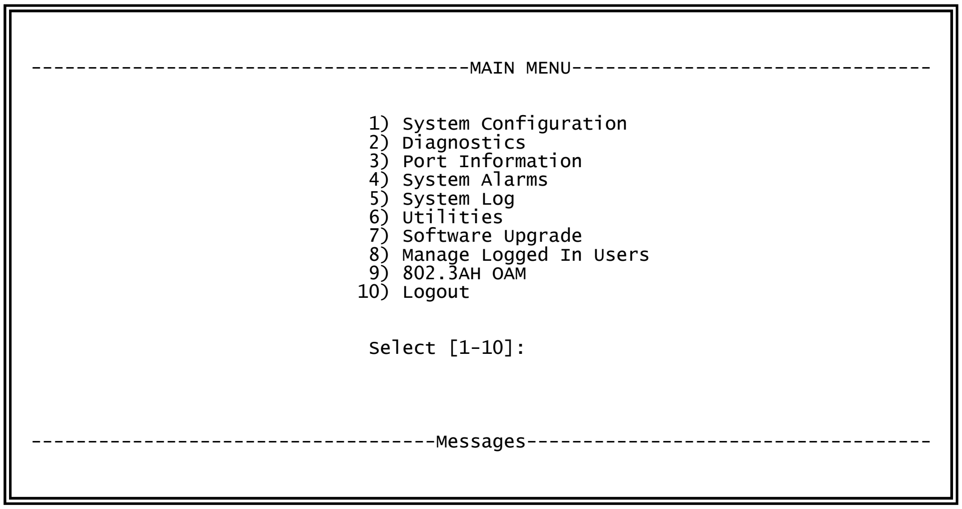
The first screen is the Login Screen. Type your username and press <Enter>. The **Password** prompt will appear. Type your password and press <Enter>. If the username or password was incorrect, you will return to the **Username** Prompt.

The default username and password for the N525 is **admin** and **admin** (lowercase). Canoga Perkins strongly recommends that you change the default username and password during your initial configuration session.



```
--------------------------------------LOGIN SCREEN------------------------------




         Please Enter Login 5Username : admin
         Please Enter Login Password : *****








------------------------------------Messages-------------------------------------
```

The Main Menu appears after you successfully log in. It provides access to all N525 functions including setup, diagnostics, and reports.



```
---------------------------------------MAIN MENU--------------------------------

                              1) System Configuration
                              2) Diagnostics
                              3) Port Information
                              4) System Alarms
                              5) System Log
                              6) Utilities
                              7) Software Upgrade
                              8) Manage Logged In Users
                              9) 802.3AH OAM
                             10) Logout


                              Select [1-10]:




------------------------------------Messages-------------------------------------
```

Figure 21 - Main Menu Selections

System Configuration

View and set values for the system information and communications parameters.

1. **IP/SNMP Agent Configuration**
   The Management IP and Auxiliary IP Address are for managing and conducting performance testing on a TCP/IP network. Enter the Management IP Address in this field.

2. **Trap Configuration**
   This defines the handling of various alarm events. You can log and/or send the event, as well as ignore it. For CLD traps, see Configuring CLD.

3. **Security Configuration**
   This configures user and SNMP security for the N525.

4. **Account Information**
   This managed user access to the N525 including privileges, passwords and access methods.

5. **System Information**
   This allows the addition of administrative information about the N525 and circuit information such as the N525's name, contact, location, customer, circuit, equipment codes and CLIE information.

6. **Radius Client Information**
   This configures the N525 for RADIUS Authentication of user. The N525 implements Radius Passthru for user authentication by a RADIUS Server.

7. **SNTP Client Configuration**
   This configures the N525 to use a primary and secondary SNTP Server for setting date and time.

8. **SYSLOG Client Configuration**
   This configures the N525 to send SYSLOG messages to a SYSLOG Server for collections and dissemination.

9. **Hardware Information**
   This displays information about the N525 including full model numbers of the N525 and its Interface modules, hardware revision levels and serial numbers. When the N525 is connected to a remote N525, L351 or L357 and SideBand Management Channel is enabled, information about the remote device is also displayed.

Diagnostics

Used to set up loopback, latency and jitter, or Ping tests and to configure and run Network Performance Assurance (optional software).

Loopback Setup

This initiates and configures the N525 for loopback diagnostics. Packets are looped back based on the MAC address of the N525. The N525 is configurable to swap origination and destination MAC addresses of the test packet and to recalculate the CRC of the looped packet when the MAC address are swapped.

Latency/Jitter Test

This manually initiated test is used to measure network latency, inter-frame jitter and frame loss from this N525 to a remote N525 in a network. Configuration items are:

1. **To IP Address**
   This is the remote N525's IP Address
2. **From IP Address**
   This selects the originating IP address from the N525 places into the test packets. Choices are Auto Selection, Management IP or Aux IP.
3. **Test VLAN**
   This is the VLAN Tag the test packets will carry. It can be the Management VLAN or any customer VLAN.
4. **Test Packets per sec**
   This lets you control the amount of packets that will be sent for every second the test runs. Settings are: 1, 2, 5, 10, 20, 50 and 100.
5. **DF Bit**
   This applies when you are testing with oversized packets over 1518 bytes in length. It is an identifier in the packet that lets other network devices (i.e. routers, switches, bridges) know if this packet can be fragmented to smaller packets or not.
6. **DSCP Precedence / Drop Probability**
   Short for Differentiated Services Code Point. N525s at the edge of the network classify packets and mark them with either the IP Precedence or DSCP value in a Diffserv network. Other network devices in the core that support Diffserv use the DSCP value in the IP header to select a PHB behavior for the packet and provide the appropriate QoS treatment.
7. **Test Packet Priority**
   This lets you set packet priority: 0 – highest priority / 7 – lowest priority.
8. **Test Duration**
   This is the duration the test will run for in min:sec, 0 – is forever
9. **Min test payload** (40 – 1954)
   This sets the minimum test packet size in bytes. The N525 sends test packets ranging in size from the minimum packet size to the maximum packet size if they are different. This is done by mapping the packets to be sent onto the range of sizes between the minimum and maximum packet sizes. The minimum packet size must be less than or equal to the maximum packet size.

10. **Max test payload** (40 – 1954)
    This sets the maximum test packet size in bytes. The maximum packet size must be greater than or equal to the minimum packet size.

11. **Test Packet Timeout sec**
    The packet timeout for this test in seconds. If a response is not received by the packet timeout value, the packet will be classified as dropped. The value set here is also used to set the maximum values that can be used for both the Latency and Jitter Measurements.

12. **Start/Stop test**
    Starts and Stops the test.

13. **Remote Latency Test**
    When SideBand Management Channel (SBMC) is enabled, you can initiate and view test results of the remote unit from the local unit.

Ping Generation

This is a network trouble shooting tool used to determine if a destination is reachable from the NID. Self-Ping, pinging the Management IP Address tests connectivity between the management processor and the N525's FPGA. This is an additional self-check function.

Remote Connectivity Loss Detection

This enables you to detect loss of connectivity to the remote N525, and to detect undesired link performance. For more information see Connectivity Loss Detection.

Port Information

The Port Information screen shows the current conditions for all ports in the N525 with options to view parameters and statistics for specific ports. Configuration information includes the model number, description, and revision; the serial number; and link, remote fault, and physical status. You must set up each port that you will use before you can set up or assign STP, VLANs or Tagging. Below are the sub menus where these fields reside:

Link Status

Informs you of the current link status of both User and Extension ports of the NID.

Port Configuration

This screen has several submenus. The following describe the submenus:

1. **Hardware Information**
   Displays N525 hardware information, including the installed User and Extension port modules.
2. **Functional Configuration**
   Configures and displays parameters for an individual port
3. **VLAN Configuration**
   The VLAN Configuration screen displays and configures VLAN parameters of the N525.
4. **Port Filters**
   This lets you set filters on the User and Extension ports to control traffic coming out of these specific ports depending on the packet type.

Layer 2 Statistics

Displays current Layer two Statistics

RMON Group 1 Statistics

Short for Remote Monitoring Specification (RMON). This screen displays current RMON statistics.

System Alarms

Displays current conditions for local and remote alarms

System Log

Displays all system events

Utilities

Setup and display basic information. Below are the sub menus:

Set Date & Time

An accurate date and time in the N525 assures accuracy for events listed in the System Log and for traps and alarms sent to the system administrator. You can choose either manual setting of the date and time or configure automatic updating of the clock using SNTP. Method you use depends on the N525's access SNTP Server and your need for accuracy.

Reset Configuration to Default

This allows you to set all parameters within the N525 to be set to factory defaults.

Change Password

This option allows the current account running to change its password.

VT100 Baud Rate

This option changes the baud rate of the RS-232 serial port when configured for VT100 terminal support.

Slip/PPP Baud Rate

This option changes the baud rate the RS-232 serial port when configured for SLIP and PPP support

Ping Generation

This is a network trouble-shooting tool used to determine if a destination is reachable from the N525.

Static ARP Table

The Static ARP table lets you set or change specific IP and MAC addresses

Dynamic ARP Table

The Dynamic ARP table lists currently assigned IP and MAC addresses for various N525 ports.

License Manager

Displays additional features enabled in the N525.

Software Upgrade

Allows you to download and install new firmware, swap active firmware banks, reset active firmware.

Manage Logged in Users

View current users logged in to the NID and allows the Administrator to force off user sessions when needed.

802.3AH OAM

The OAM work of the 802.3ah addresses three key operational issues when deploying Ethernet between locations: Link Monitoring, Fault Signaling and Remote Loopback.

Link Monitoring introduces some basic error definitions for Ethernet so entities can detect failed and degraded connections.

Fault Signaling provides mechanisms for one entity to signal another that it has detected an error.

Remote Loopback, which is often used to troubleshoot networks, allows one station to put the other station into a state whereby all inbound traffic is immediately reflected back onto the link. When a Remote Loopback is initiated or invoked at a Local DTE, the Local DTE generates an event to the system log and a syslog message. Likewise, when a Remote Loopback is exited, this also generates a system log event and a syslog message.

OAM Configuration gives you the ability to enable or disable 802.3ah OAM mode. The Functional Configuration screen allows parameter setting of the OAM mode on a per port basis. This allows you the ability to set the 802.3ah OAM mode for the User port and Extension port independently. You can configure each port to *802.3ah Active Mode*, *802.3ah Passive Mode*, or *Disable* 802.3ah OAM.

When 802.3ah OAM Mode is disabled, the N525 is transparent to 802.3ah OAMPDUs. All incoming OAMPDUs will pass through the N525 transparently and the N525 does not generate any OAMPDUs (effectively, the OAM Sublayer will be bypassed and all frames will be forwarded to the superior sublayer).

When a Remote Loopbacks are initiated or invoked from Local N525, it generates an event to the system log and generates an equivalent Syslog Message. Likewise, when a Remote Loopback is exited, the N525 generates an event to the system log and an equivalent Syslog message.

There are three types of Events: Critical Events, Link Fault Events and Dying Gasp Events. The specific faults that comprise these events are defined as follows:

1. **A Critical Event** occurs when a software reset is invoked. A hard reset does not generate a Critical Event since it resets the processor as soon as it is asserted.

2. **A Link Fault Event** occurs when the local PHY receiver detects a LOC condition.

3. **A Dying Gasp Event** occurs when a power supply failure has occurred.

Logout

Terminates your current session. If this was a Telnet Session, it also drops the Telnet connection.

Managing the N525

You can manage the hardware and the software for the N525, including communication access.

Configuring Methods for the N525

There are two ways to configure the N525: manually using the VT100 User Interface, and using a configuration file download. Though SNMP commands are issued by CanogaView or your network management platform and can be scripted, this is considered a manual configuration since each configurable parameter is individually sent.

Configuration Upload

As more features have been added to the N525, configuring the numerous features and settings on the N525 manually has becoming more time consuming and onerous. Canoga Perkins developed a Backup and Restore mechanism for the N525, able to generate, download, upload and run configuration files. The configuration file naming convention is as follows:

N525xxxx.cfg

The "N525" is a string of four characters which corresponds to the Model Number, "xxxx" may be zero to four characters in length and corresponds to a user defined field and ".cfg" is always used as the file extension.

The configuration file **MUST** begin with a header that contains three variables, each of which is a string of characters of finite length, as described here:

1. CfgFileName is a string that represents the configuration file name and extension (as in the DOS file naming convention). The name must be of maximum 8 characters and the extension is always ".cfg", for a maximum total string length of 12 characters.

2. CfgFileBuiltWithFirmware is a string of 5 characters that represents the firmware level (i.e., application code in the Active Bank) that was running when the configuration file was built.

3. CfgFileUserComments is a string of 50 characters that the user may set to any string desired. This variable contains information relevant to the user.

An example of the header as it would appear on a **N525_001.cfg** file is shown here:

```
### WARNING – DO NOT MODIFY THIS HEADER ###
CfgFileName = N525_001.cfg
CfgFileBuiltWithFirmware = 05.00
CfgFileUserComments =Canoga Perkins, Chatsworth, CA site.
##############################################
```

The configuration file consists of the header followed by a list of keywords. Each keyword represents a user defined variable that is be set in the file.

The configuration file functions is both backward and forward compatible. A configuration file built with a newer firmware version may contain keywords that an older firmware version may not recognize. In this case, the N525 simply skips over the keyword and doesn't act on it.

Similarly, a configuration file built with an older firmware may not have all the keywords that a newer firmware may expect to see. The N525 ignores that expected keywords are missing.

In the case where the N525 encounters a keyword that is not recognized, an error message is generated and placed in the System Log and a Syslog message is sent. This helps the user to spot errors in the configuration files.

Configuration files are uploaded and downloaded in-band using FTP and SFTP, in the same manner that firmware and bootcode is uploaded and downloaded.

Note: TFTP is not supported.

Supported Configuration Parameters

The Configuration Backup and Restore function supports all configurable parameters for the N525.

Avoiding a Loss of Connectivity

Since configuration files contains Manager IP Address, Subnet Mask and Default Gateway parameters, it is conceivable that a user may lose connectivity to a N525 after downloading a configuration file. A configuration file may contain values for the Manager parameters that are different than the current Manager settings. To avoid such situations where management connectivity to the N525 could be lost, three additional “master control keywords” will follow the configuration file header, as shown below:

```
############################################

## The following must be modified to = "Yes" if the specified items
## are to be configured, otherwise the config items will be ignored.

ConfigureIPAddress = No
ConfigureSBMC = No
ConfigureInterface = No

############################################
```

ConfigureIPAddress specifies whether the N525 will adopt or ignore the following configuration file parameters:

- IPAddress
- SubnetMask
- DefaultGateway
- Slip/PPP IPAddress

The default setting for ConfigureIPAddress is “No”, which indicates that the values for each of the above parameters will be ignored.

ConfigureSBMC specifies whether the N525 will adopt or ignore the SBMC Flag parameter. The default is set to “No”, which indicates that the value is ignored.

ConfigureInterface specifies whether the N525 will adopt or ignore the following physical port setup parameters:

- RmtfFlag
- LlfFlag
- FlowControlFlag
- UserPort
- ExtPort
- sbmcFlag
- PvstFilterFlag

The default is set to “No”, which indicates that the value is ignored.

Configuration File Access Privileges

A configuration file is an English-readable file that is not locked or protected; therefore, anyone can edit this file. To ensure that an unauthorized person does not download a configuration file to a N525 in order to change settings that particular user did not have rights to, only those users with supervisor access will be allowed to download configuration files to the N525.

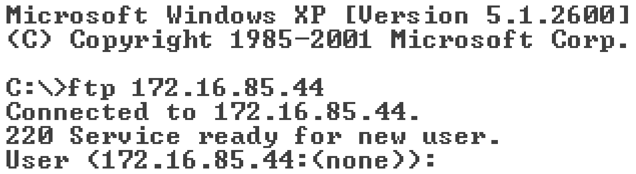
Even though operators are not allowed to download configuration files, they **ARE** allowed to upload configuration files from a N525.

Only observers are **NOT** allowed to upload or download configuration files.

Note: See the Setting Up User Accounts section for more information on User Privilege Levels

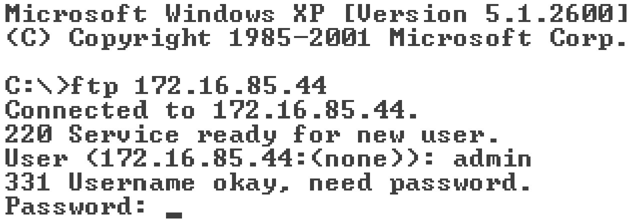
To upload a configuration file from the N525 follow these steps:

1. Open a command prompt on your PC and type [`ftp xxx.xxx.xxx.xxx`] where the x's are is the IP address corresponding to the N525's management IP address and press <Enter>.



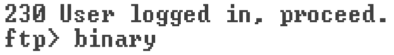
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 172.16.85.44
Connected to 172.16.85.44.
220 Service ready for new user.
User (172.16.85.44:(none)):
```

2. Type the username and password and press <Enter>



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 172.16.85.44
Connected to 172.16.85.44.
220 Service ready for new user.
User (172.16.85.44:(none)): admin
331 Username okay, need password.
Password: _
```

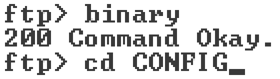
3. Set ftp to "binary" mode by typing [**`binary`**] at the prompt and pressing <Enter>



```
230 User logged in, proceed.
ftp> binary
```

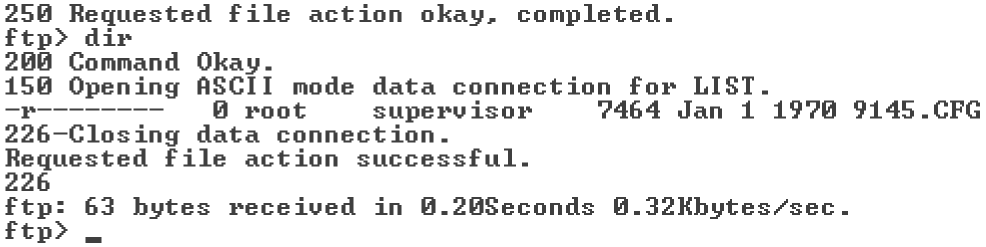
4. Change directory to the CONFIG directory by typing [**`cd CONFIG`**] and pressing <Enter>

Note: The word "CONFIG" has to be capitalized.



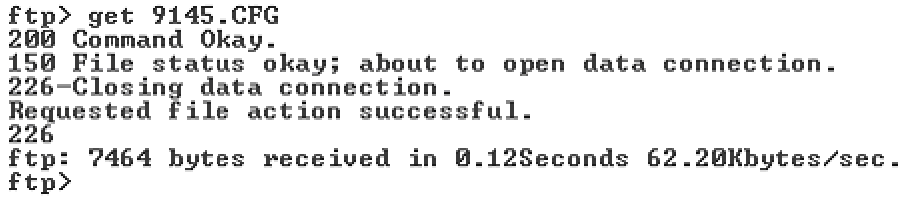
```
ftp> binary
200 Command Okay.
ftp> cd CONFIG_
```

5. Type [**`dir`**] at the prompt to view the contents of the directory and press <Enter>



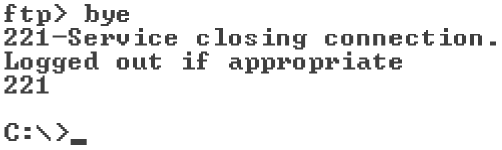
```
250 Requested file action okay, completed.
ftp> dir
200 Command Okay.
150 Opening ASCII mode data connection for LIST.
-r--------   0 root    supervisor    7464 Jan 1 1970 9145.CFG
226-Closing data connection.
Requested file action successful.
226
ftp: 63 bytes received in 0.20Seconds 0.32Kbytes/sec.
ftp> _
```

6. To retrieve the configuration file, type [`get N525.CFG`] and press <Enter>



```
ftp> get 9145.CFG
200 Command Okay.
150 File status okay; about to open data connection.
226-Closing data connection.
Requested file action successful.
226
ftp: 7464 bytes received in 0.12Seconds 62.20Kbytes/sec.
ftp>
```

7. To end the ftp session, type [`bye`] on the prompt and close the window.

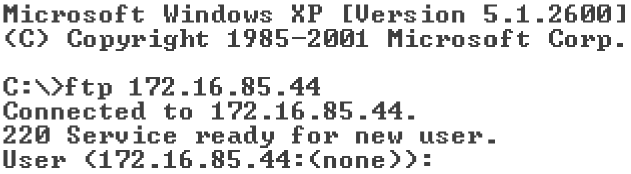


```
ftp> bye
221-Service closing connection.
Logged out if appropriate
221

C:\>_
```

You can use any text editor such as Notepad[1] or WordPad[2] to edit the configuration file. Please see Appendix C for an example format and the different fields of a configuration file.

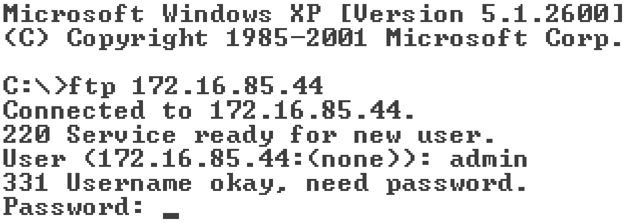
Once you have made your changes to the configuration file and are now ready to download the changes to the N525, follow these steps:

1. Open a command prompt on your PC and type [`ftp xxx.xxx.xxx.xxx`] where the x's are is the IP address corresponding to the N525's management IP address and press <Enter>.



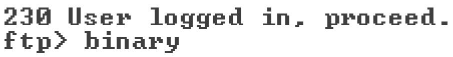
```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 172.16.85.44
Connected to 172.16.85.44.
220 Service ready for new user.
User (172.16.85.44:(none)):
```

2. Type the username and password and press <Enter>



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 172.16.85.44
Connected to 172.16.85.44.
220 Service ready for new user.
User (172.16.85.44:(none)): admin
331 Username okay, need password.
Password: _
```

3. Set ftp to "binary" mode by typing [**`binary`**] at the prompt and press <Enter>

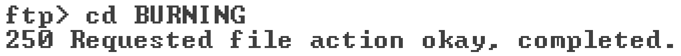


```
230 User logged in, proceed.
ftp> binary
```

[1] [2] Notepad and WordPad are trademarks of Microsoft Corporation

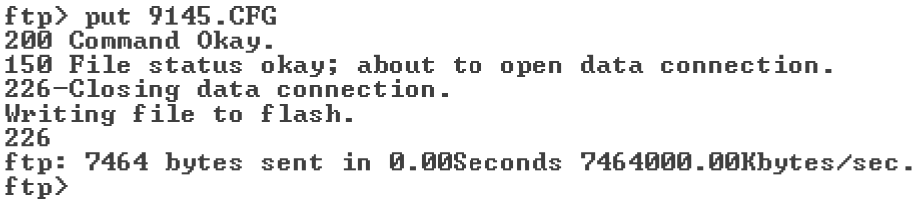
4. Change the directory to BURNING by typing [**cd BURNING**] and press <Enter>

Note: The word “BURNING” has to be capitalized.



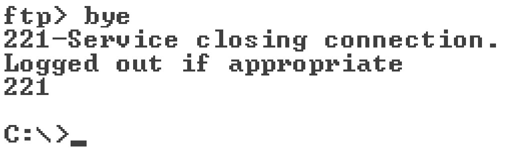
```
ftp> cd BURNING
250 Requested file action okay, completed.
```

5. To download the configuration file, type [put N525.CFG] and press <Enter>



```
ftp> put 9145.CFG
200 Command Okay.
150 File status okay; about to open data connection.
226-Closing data connection.
Writing file to flash.
226
ftp: 7464 bytes sent in 0.00Seconds 7464000.00Kbytes/sec.
ftp>
```

6. To end the ftp session type [bye] on the prompt and close the window.



```
ftp> bye
221-Service closing connection.
Logged out if appropriate
221

C:\>_
```

Manual Configuration – VT100 Session

The System Information screen provides various categories of optional information that system administrators can track. To access the System Information screen, and follow these steps:

1. From the System Configuration Menu, type [5], "System Information," and press <Enter>

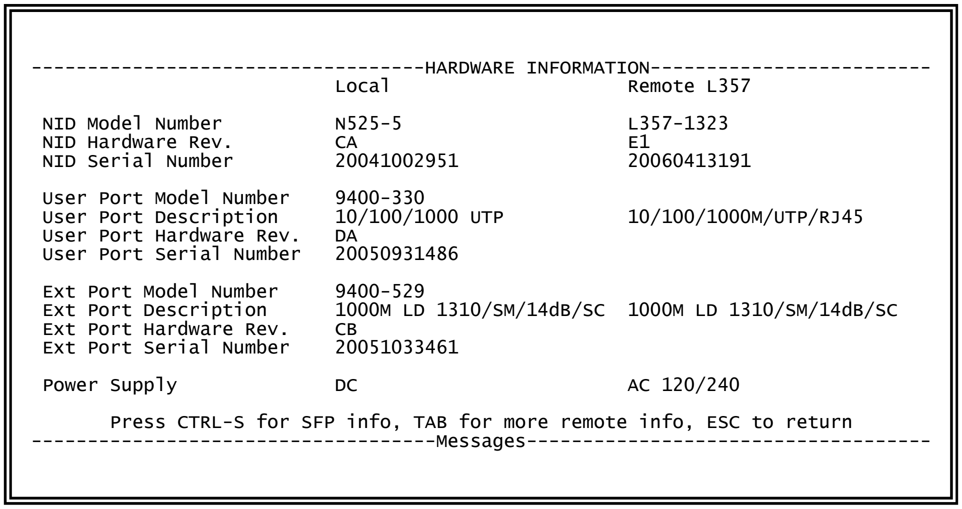
```
-----------------------SYSTEM INFORMATION - LOCAL UNIT--------------------------
 1. System Name         : N525 D
 2. Contact             : Tien Nguyen
 3. Location            : VLAB
 4. Customer            : Canoga Engineering
 5. Information         :
                        :
 6. Circuits            :
                        :
 7. Service Code        :
 8. Date-in-Service     :
 9. Date-Out-of-Service :
10. Equipment Type      :
11. Equipment Code      :
12. Vendor              : FONEX
13. CLEI                :
14. Mfg Date            : 10/01/2004

15. Unit                : Local
                                    Select [1-15]:
-----------------------------------Messages------------------------------------
```

2. At the System Information screen, type the number for an item and press <Enter>, then type the information and press <Enter>.
    a. **System Name** – Displayed in the header of all N525 Management screens, up to 25 characters
    b. **Contact** – up to 25 characters
    c. **Location** – up to 25 characters
    d. **Customer** – up to 25 characters
    e. **Information** – 2 lines, up to 40 characters each
    f. **Circuits** – 2 lines, up to 25 characters each
    g. **Service Code** – up to 10 characters
    h. **Date-in-Service** – [mm/dd/yyyy]
    i. **Date-Out-of-Service** – [mm/dd/yyyy]
    j. **Equipment Type** – up to 10 characters
    k. **Equipment Code –** up to 10 characters
    l. **Vendor –** up to 25 characters
    m. **CLEI** – up to 10 characters
    n. **Mfg Date** – [mm/dd/yyyy]
    o. **Unit** – Displays System Information for a SMBC connected remote N525
3. To change the view between Local and Remote units, type [15], "Unit," press <Enter>. Pressing <Space> cycles between the options. Press <Enter> to select an option.
4. To return to the Main Menu, press <Esc>.

View Device and Module Information

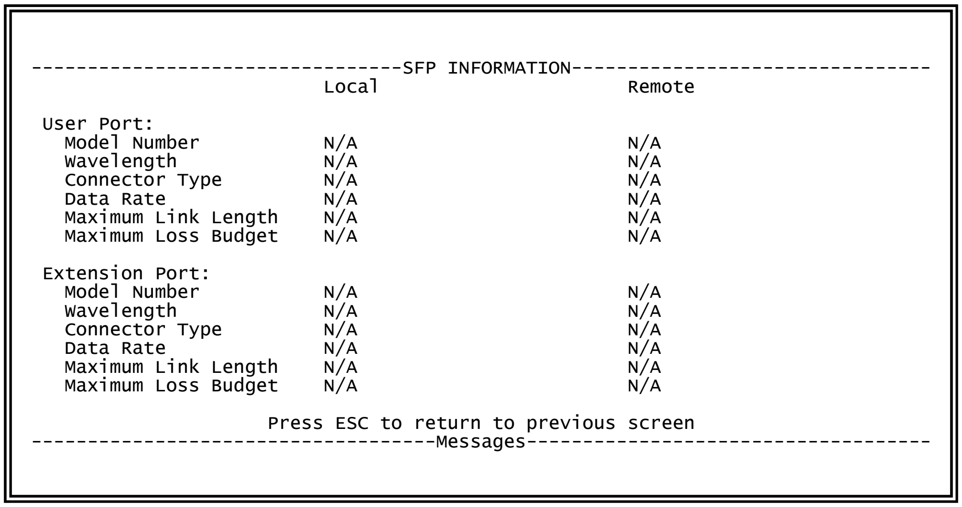
The Hardware Information report shows hardware descriptions, including the type, model, serial, and revision numbers for the N525 and Interface Modules, as well as the power supply status. You can also view similar information for the remote unit. Exact parameters depend on the specific remote unit. Use this information when troubleshooting, such as tracking down an error in a data link or the configuration. To view the Hardware Information screen, follow these steps:

1. From the Main Menu, type [3], "Port Information," and press <Enter>. Then from the Port Information Menu, type [2], "Port Configuration," and press <Enter>. Type [1], "Hardware Information," and press <Enter>.



```
-----------------------------------HARDWARE INFORMATION-------------------------
                           Local                     Remote L357

 NID Model Number          N525-5                    L357-1323
 NID Hardware Rev.         CA                        E1
 NID Serial Number         20041002951               20060413191

 User Port Model Number    9400-330
 User Port Description     10/100/1000 UTP           10/100/1000M/UTP/RJ45
 User Port Hardware Rev.   DA
 User Port Serial Number   20050931486

 Ext Port Model Number     9400-529
 Ext Port Description      1000M LD 1310/SM/14dB/SC  1000M LD 1310/SM/14dB/SC
 Ext Port Hardware Rev.    CB
 Ext Port Serial Number    20051033461

 Power Supply              DC                        AC 120/240

       Press CTRL-S for SFP info, TAB for more remote info, ESC to return
------------------------------------Messages------------------------------------
```

2. To display information about SFP(s) on the User or Extension port interface modules, press <Ctrl-S> to display the SFP Information screen.



```
---------------------------------SFP INFORMATION--------------------------------
                          Local                      Remote

 User Port:
   Model Number           N/A                        N/A
   Wavelength             N/A                        N/A
   Connector Type         N/A                        N/A
   Data Rate              N/A                        N/A
   Maximum Link Length    N/A                        N/A
   Maximum Loss Budget    N/A                        N/A

 Extension Port:
   Model Number           N/A                        N/A
   Wavelength             N/A                        N/A
   Connector Type         N/A                        N/A
   Data Rate              N/A                        N/A
   Maximum Link Length    N/A                        N/A
   Maximum Loss Budget    N/A                        N/A

                     Press ESC to return to previous screen
------------------------------------Messages------------------------------------
```

3. To return to the Main Menu, press <Esc>.

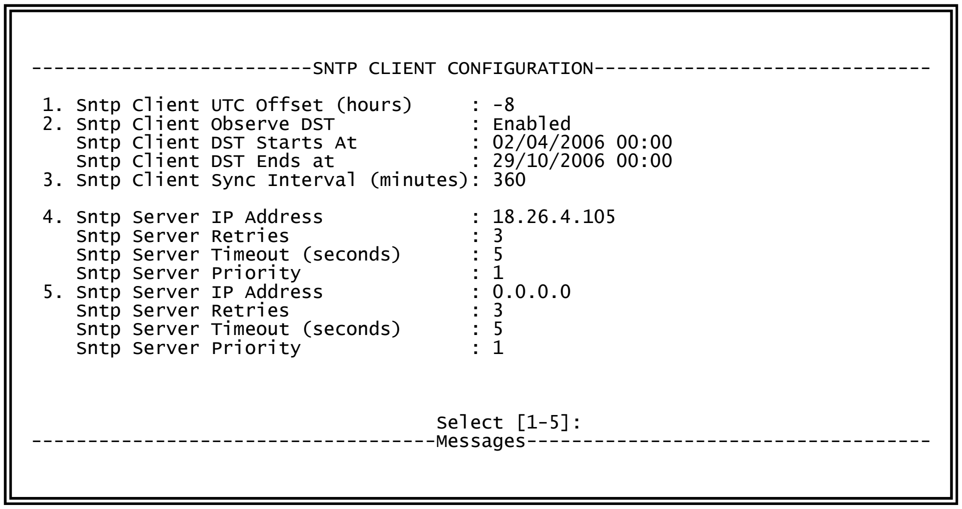
Manage the Date and Time

An accurate date and time in the N525 assures accuracy for events listed in the System Log and for traps and alarms sent to the system administrator. You can choose either of two methods for setting the date and time, depending on your access to an external network and your need for accuracy.

1. For accuracy within a large network, you can set up the N525 to synchronize the system date and time to an SNTP server. When the N525 contacts the SNTP server to synchronize the time, the event appears in the System Log, whether or not the SNTP server responds.
2. If you choose to not use SNTP to maintain the date and time, or do not have access to the Internet or a SNTP server, you can manually set the date and time on the N525.

To set up synchronization with SNTP, follow these steps:

1. At the System Configuration Menu, type [7], "SNTP Client Configuration" and press <Enter>.



```
------------------------SNTP CLIENT CONFIGURATION------------------------------

 1. Sntp Client UTC Offset (hours)     : -8
 2. Sntp Client Observe DST            : Enabled
    Sntp Client DST Starts At          : 02/04/2006 00:00
    Sntp Client DST Ends at            : 29/10/2006 00:00
 3. Sntp Client Sync Interval (minutes): 360

 4. Sntp Server IP Address             : 18.26.4.105
    Sntp Server Retries                : 3
    Sntp Server Timeout (seconds)      : 5
    Sntp Server Priority               : 1
 5. Sntp Server IP Address             : 0.0.0.0
    Sntp Server Retries                : 3
    Sntp Server Timeout (seconds)      : 5
    Sntp Server Priority               : 1



                                    Select [1-5]:
------------------------------------Messages------------------------------------
```

2. At the SNTP Client Configuration screen, type the number for a parameter and press <Enter>, then follow the prompts on the screen.
   a. **sntp Client UTP Offset (hours):**
   Set the difference, in hours, between this N525 and Coordinated Universal Time (UTC), which is similar to Greenwich Mean Time (GMT); Range is -12 to 12
   b. **sntp Client Observe DST:**
   Enables/Disables Daylight Savings Time (Summer Time) and the date and time it starts and ends.

c. **sntp Client Sync Interval (minutes):**
Set how often, in minutes, that the N525 tries to synchronize its time to the SNTP server; Range is 0 (attempt to synchronize at bootup, only) to 1440 (once daily)

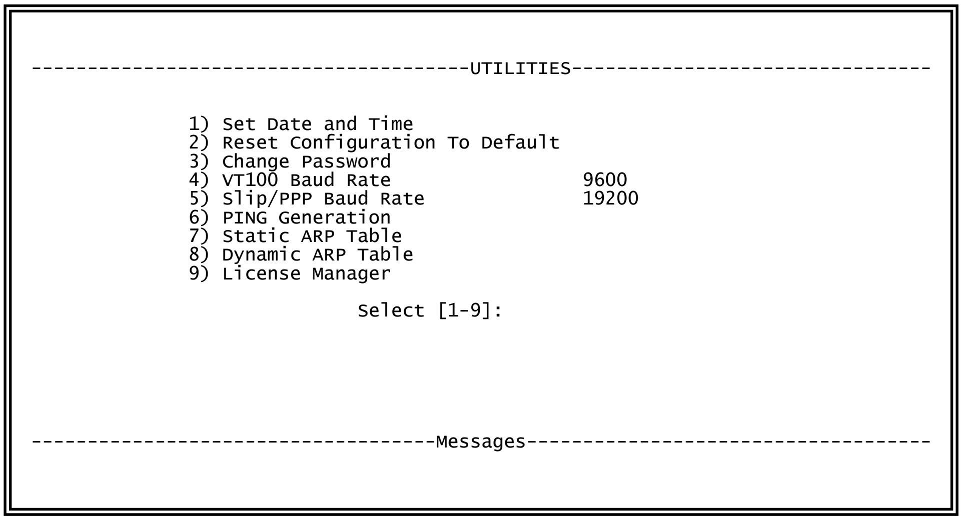
d. **sntp Servers Configuration:**
Sets IP address and operating parameters for 2 servers

- IP Address: Set the address for the SNTP server. 0.0.0.0 indicates no server
- Retries: How many times the N525 tries to synchronize before trying the alternate server or giving up. Range is 0 to 10
- Timeout (seconds): Wait period between unsuccessful attempts. Range is 1 to 30
- Priority: Set which server to contact first. Range is 1 to 255 with 1 the highest priority and 255 the lowest. If the priority is the same for the two servers, the N525 alternates tries between the servers.

3. To return to the Main Menu, press <Esc>.

To manually set the date and time, follow these steps:

1. From the Main Menu, type [6], "Utilities," and press <Enter>.
2. At the Utilities Menu, type [1], "Set Date and Time" and press <Enter>.
3. At the prompt to enter the current date and time, type the current information in DD/MM/YYYY HH:MM format, then press <Enter>.



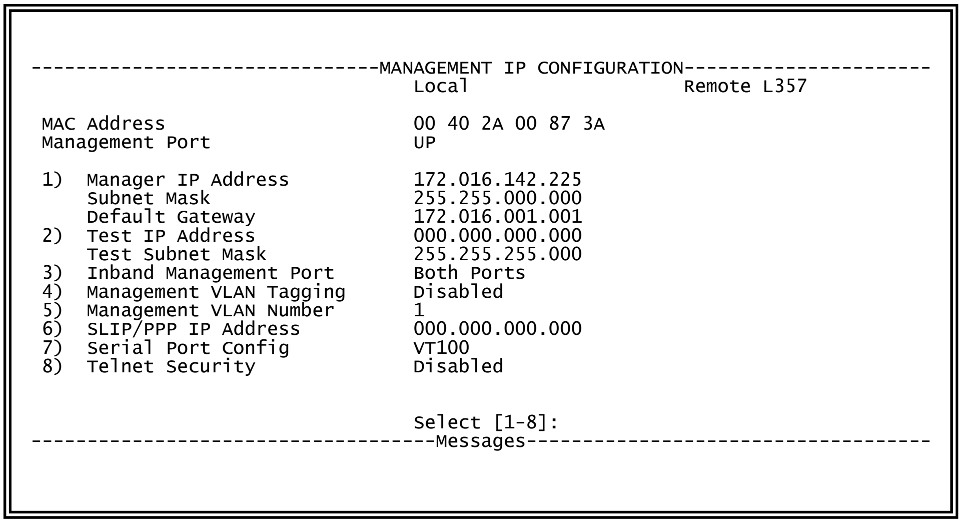
```
---------------------------------------UTILITIES--------------------------------


              1) Set Date and Time
              2) Reset Configuration To Default
              3) Change Password
              4) VT100 Baud Rate                 9600
              5) Slip/PPP Baud Rate              19200
              6) PING Generation
              7) Static ARP Table
              8) Dynamic ARP Table
              9) License Manager
                             Select [1-9]:





------------------------------------Messages------------------------------------
```

4. To return to the Main Menu, press <Esc>.

Configuring SNMP Access

To set values for basic system parameters, including some parameters used by SNMP, go to the IP Configuration screen and follow these steps:

1. From the System Configuration Menu type [1], "IP/SNMP Agent Configuration," and press <Enter>, then type [1], "Management IP Configuration," and press <Enter>.



```
-------------------------------MANAGEMENT IP CONFIGURATION---------------------
                                  Local                  Remote L357

 MAC Address                      00 40 2A 00 87 3A
 Management Port                  UP

 1)  Manager IP Address           172.016.142.225
     Subnet Mask                  255.255.000.000
     Default Gateway              172.016.001.001
 2)  Test IP Address              000.000.000.000
     Test Subnet Mask             255.255.255.000
 3)  Inband Management Port       Both Ports
 4)  Management VLAN Tagging      Disabled
 5)  Management VLAN Number       1
 6)  SLIP/PPP IP Address          000.000.000.000
 7)  Serial Port Config           VT100
 8)  Telnet Security              Disabled


                                  Select [1-8]:
------------------------------------Messages-----------------------------------
```

2. At the Management IP Configuration screen, type the number for an item and press <Enter>. Press <Tab> to highlight the Remote column if needed, then enter data or press <Space> to cycle through the options. Press <Enter> to select an option.

   a. **Manager IP Address**
   Sets the N525 Manager’s IP Address
   Subnet Mask
   Sets the N525 Manager’s IP Subnet MASK
   Default Gateway
   Sets the IP Address of the Default Gateway, a network node that manages connections to other IP subnetworks

   b. **Test IP Address**
   Sets the IP Address for Network Performance Assurance optional feature
   Test Subnet Mask
   Sets the IP Address for Network Performance Assurance optional feature

   c. **Inband Management Port**
   Selects which port(s) allow management communication access. Parameters are Both Ports, Ext Port Only, User Port Only, or No Management

   d. **Management VLAN Tagging**
   Enables/Disable the use of a management VLAN

   e. **Management VLAN Number**
   When management VLAN is Enabled, sets VLAN Tag ID

f. **SLIP/PPP IP Address**
Sets the IP Address for SLIP/PPP access. Address does not need to be configured if SLIP/PPP is not used.

g. **Serial Port Config**
Sets the session type supported by the RS-232 serial port: selections are VT100 or SLIP/PPP.

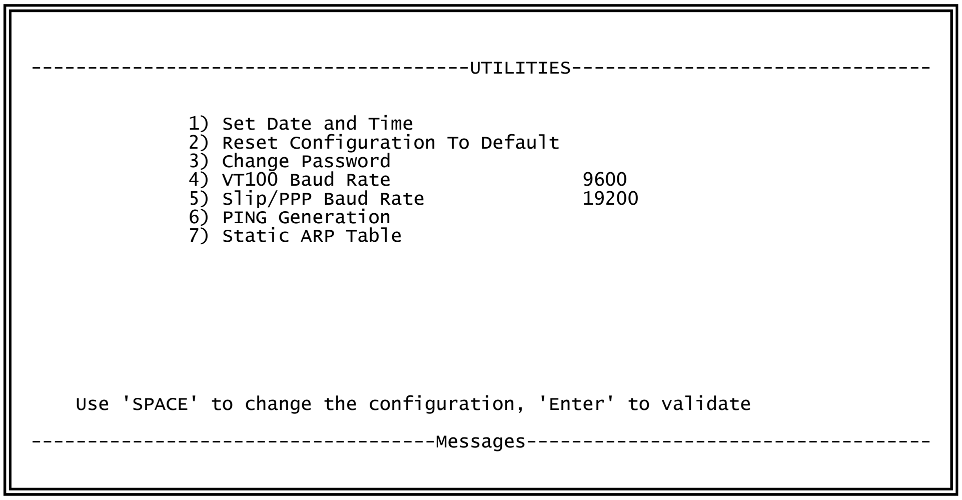
h. **Telnet Security**
Enables or disables checking if Telnet host is listed in the host table. Default is disabled, which allows access to all hosts

3. To return to the Main Menu, press <Esc>.

Set Up the VT100 and SLIP/PPP Baud Rates

Although the default values for the communication parameters meet requirements for most systems, you may need to update them for a particular situation. To update the baud rate, follow these steps:

1. At the Main Menu, type [6], "Utilities," and press <Enter>.
2. To change the baud rate for VT100 sessions, type [4], "VT100 Baud Rate," and press <Enter>. Pressing <Space> cycles through the baud rate options. Options are 9600 or 19200 bps.



```
---------------------------------------UTILITIES--------------------------------


              1) Set Date and Time
              2) Reset Configuration To Default
              3) Change Password
              4) VT100 Baud Rate                  9600
              5) Slip/PPP Baud Rate               19200
              6) PING Generation
              7) Static ARP Table









    Use 'SPACE' to change the configuration, 'Enter' to validate

------------------------------------Messages------------------------------------
```

3. To change the baud rate for SLIP/PPP sessions, type [5], "SLIP/PPP Baud Rate," and press <Enter>. Pressing <Space> cycles through the baud rate options. Options are 9600, 19200, 38400, 57600, or 115200 bps.
4. To return to the Main Menu, press <Esc>.

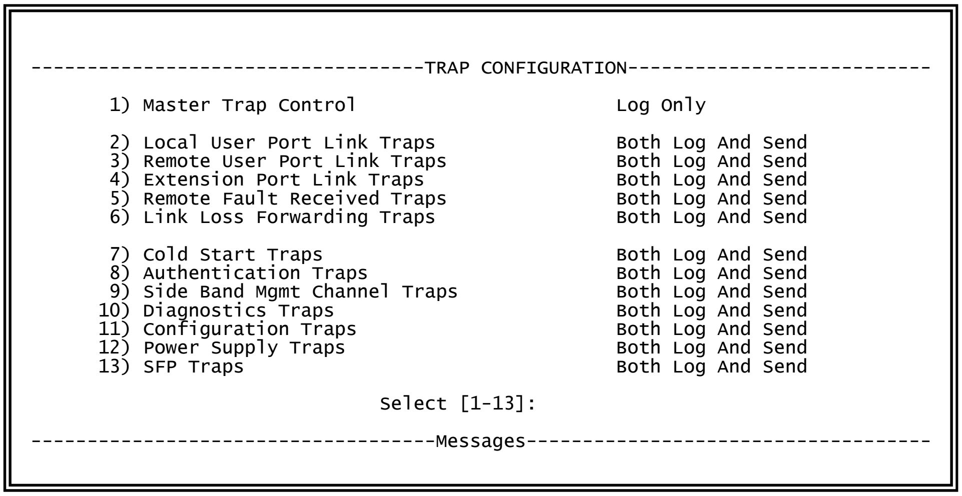
Managing Traps

Traps are SNMP messages that are sent to CanogaView or your network management platform, and to the N525 System Log. Use the Trap Configuration screen to view the current configuration and to enable or disable traps. For a list of events that trigger traps, see Table 3.

Note: To configure CLD traps, see Configuring CLD.

To set up the traps, follow these steps:

1. From the System Configuration Menu, type [2], "Trap Configuration," and press <Enter>.



```
----------------------------------TRAP CONFIGURATION--------------------------

      1) Master Trap Control                        Log Only

      2) Local User Port Link Traps                 Both Log And Send
      3) Remote User Port Link Traps                Both Log And Send
      4) Extension Port Link Traps                  Both Log And Send
      5) Remote Fault Received Traps                Both Log And Send
      6) Link Loss Forwarding Traps                 Both Log And Send

      7) Cold Start Traps                           Both Log And Send
      8) Authentication Traps                       Both Log And Send
      9) Side Band Mgmt Channel Traps               Both Log And Send
     10) Diagnostics Traps                          Both Log And Send
     11) Configuration Traps                        Both Log And Send
     12) Power Supply Traps                         Both Log And Send
     13) SFP Traps                                  Both Log And Send

                                 Select [1-13]:

-----------------------------------Messages-----------------------------------
```

2. At the Trap Configuration Menu, type the number for a trap and press <Enter>. Pressing <Space> cycles between *Log Only*, Send Only, *Both Log and Send* and *Disabled*. Press <Enter> to select your choice. Defaults are 1) Master Trap Control: Log Only, all others (2-13): Both Log and Send.

3. To return to the Main Menu, press <Esc>.

These selections do not affect how the Major and Minor events are reported. Table 3 describes Trap functions.

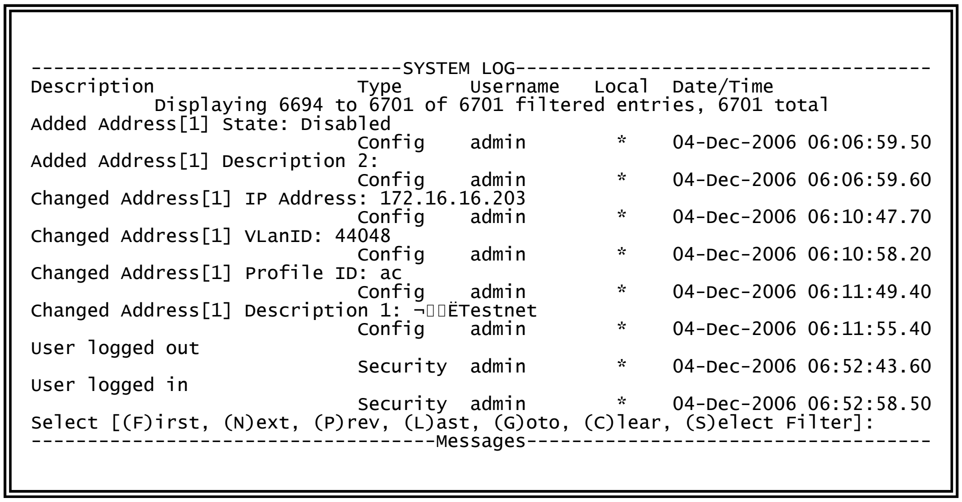
Table 3 – Trap Configuration Options

Trap	When enabled, sends a Trap if. . .
Local/User Port Link, Remote User Port Link, or Extension Port Link	The link went down and came back up
Remote Fault Received	A port receives an RMTF
Link Loss Forwarding	A port loses a received link and transmits notification to the next port
Cold Start	The N525 is reset by a power failure or forced reset
Authentication	An unauthorized host attempts SNMP access
Side Band Mgmt Channel	SBMC is lost or back online
Diagnostics	Loopback is enabled or disabled
Configuration	When the N525's remote unit has an incompatible

Trap	When enabled, sends a Trap if. . .
	firmware
Power Supply	When the power supply is failing
SFP	An SFP change occurs

View System Events and Traps

The System Log lists all events that occurred since the last power-up or when the log was last cleared. The log lists items in reverse chronological order. 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. To access the user friendly System Logs, follow these steps:



```
---------------------------------SYSTEM LOG-------------------------------------
Description                  Type      Username   Local  Date/Time
           Displaying 6694 to 6701 of 6701 filtered entries, 6701 total
Added Address[1] State: Disabled
                             Config    admin        *    04-Dec-2006 06:06:59.50
Added Address[1] Description 2:
                             Config    admin        *    04-Dec-2006 06:06:59.60
Changed Address[1] IP Address: 172.16.16.203
                             Config    admin        *    04-Dec-2006 06:10:47.70
Changed Address[1] VLanID: 44048
                             Config    admin        *    04-Dec-2006 06:10:58.20
Changed Address[1] Profile ID: ac
                             Config    admin        *    04-Dec-2006 06:11:49.40
Changed Address[1] Description 1: ¬□□ËTestnet
                             Config    admin        *    04-Dec-2006 06:11:55.40
User logged out
                             Security  admin        *    04-Dec-2006 06:52:43.60
User logged in
                             Security  admin        *    04-Dec-2006 06:52:58.50
Select [(F)irst, (N)ext, (P)rev, (L)ast, (G)oto, (C)lear, (S)elect Filter]:
------------------------------------Messages------------------------------------
```

1. From the Main Menu, type [5], "System Log," and press <Enter>. The System Log appears.

2. To view additional events or clear the log, follow the prompts on the screen.

2. To return to the Main Menu, press <Esc>.

Update Software

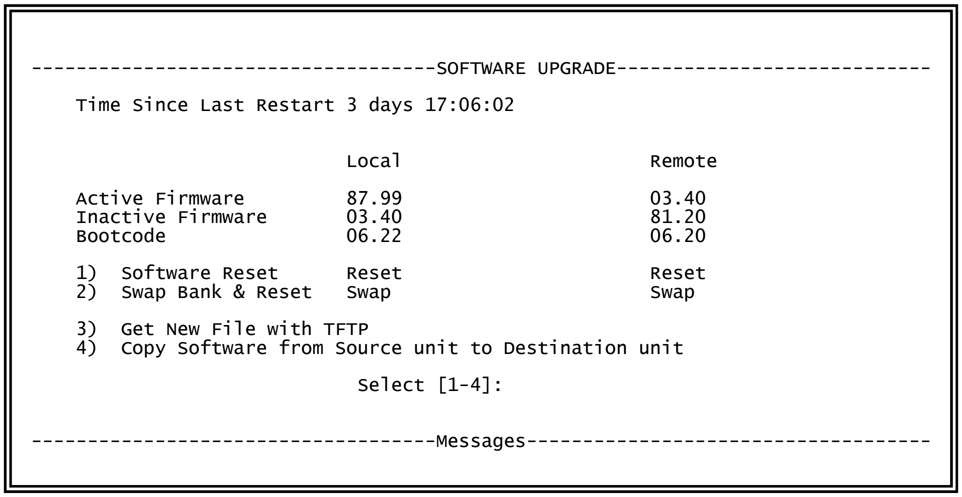
Each N525 has two flash memory banks that store software:

1. The Active Flash Memory holds the software currently in use
2. The Inactive Flash Memory holds the new software from a download or the older version of software

Software is downloaded to the inactive memory to avoid disrupting service. Resetting the N525 and swapping banks does not affect operation and is transparent to user traffic.

Use the Software Upgrade report and menu screen to check the current version of the firmware and upgrade it and the remote N525, if necessary. To access the Software Upgrade Menu and check the software version, follow these steps:

1. From the Main Menu, type [7], "Software Upgrade," and press <Enter>. The Software Upgrade screen appears.
   Note: Line 4 is only present when the remote unit is SBMC Connected N525.



```
------------------------------------SOFTWARE UPGRADE----------------------------

    Time Since Last Restart 3 days 17:06:02


                            Local                      Remote

    Active Firmware         87.99                      03.40
    Inactive Firmware       03.40                      81.20
    Bootcode                06.22                      06.20

    1)  Software Reset      Reset                      Reset
    2)  Swap Bank & Reset   Swap                       Swap

    3)  Get New File with TFTP
    4)  Copy Software from Source unit to Destination unit
                             Select [1-4]:


------------------------------------Messages------------------------------------
```

2. Record the numbers for the Active and Inactive Firmware for both the local and remote N525s.

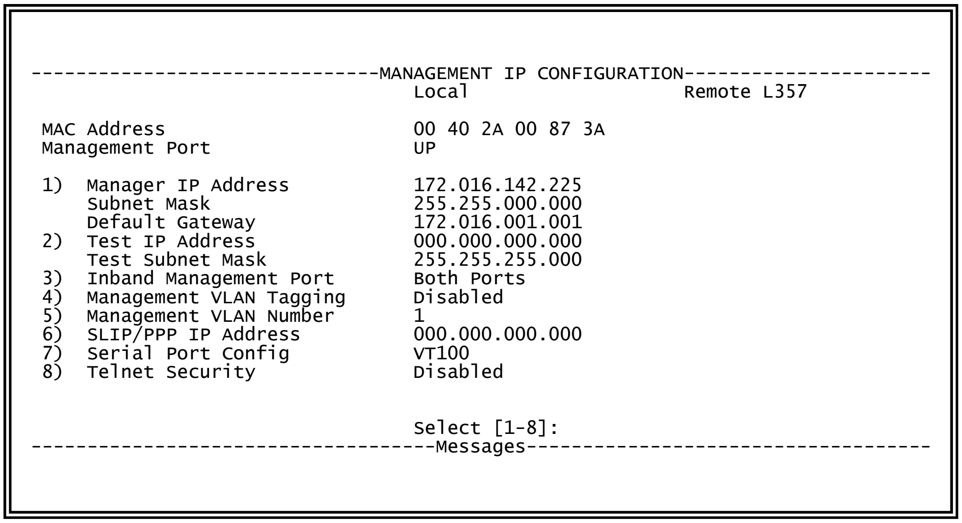
3. Access the Canoga Perkins website, click Downloads, scroll to the N525 filename and compare version numbers listed there with the version numbers you recorded. The N525 firmware filename is similar to *N5250106.zip*, where N525 indicates the module and 0106 indicates the version number.

4. Download the software from the website to your local TFTP, FTP, or SFTP server.

Caution: To ensure compatibility when two N525s are connected using the EXT ports, you must upgrade all connected units with the same firmware. Failure to do so will cause CFG alarms and could result in user traffic disruption.

To upgrade N525 software, follow these steps:

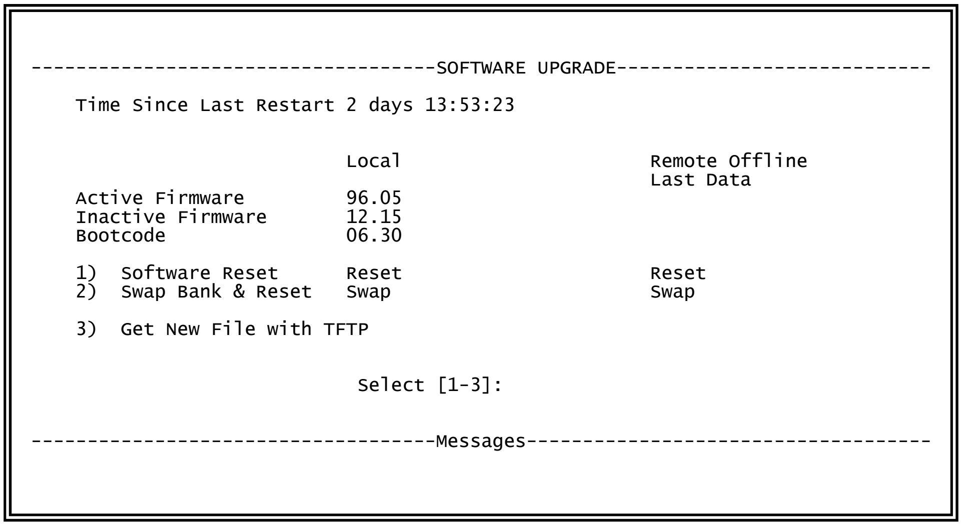
1. Access the SNMP Configuration Menu before starting the software upgrade: enter the IP Address, Subnet Mask, and Default Gateway for the N525.



```
-------------------------------MANAGEMENT IP CONFIGURATION----------------------
                                  Local                  Remote L357

 MAC Address                      00 40 2A 00 87 3A
 Management Port                  UP

 1)  Manager IP Address           172.016.142.225
     Subnet Mask                  255.255.000.000
     Default Gateway              172.016.001.001
 2)  Test IP Address              000.000.000.000
     Test Subnet Mask             255.255.255.000
 3)  Inband Management Port       Both Ports
 4)  Management VLAN Tagging      Disabled
 5)  Management VLAN Number       1
 6)  SLIP/PPP IP Address          000.000.000.000
 7)  Serial Port Config           VT100
 8)  Telnet Security              Disabled


                                  Select [1-8]:
------------------------------------Messages------------------------------------
```

2. From the Main Menu, type [7], "Software Upgrade," and press <Enter>.

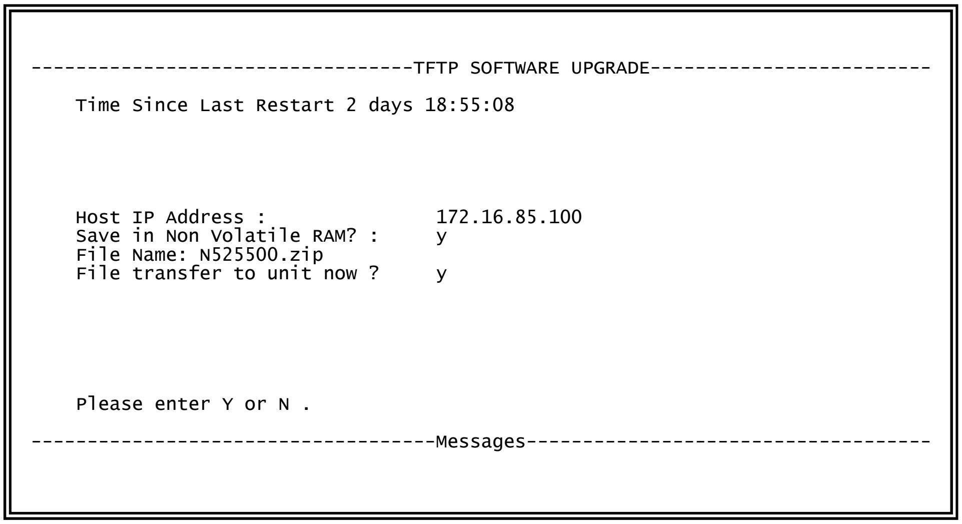
3. At the Software Upgrade Menu, type [3], Get New File with TFTP, and press <Enter>.



```
------------------------------------SOFTWARE UPGRADE----------------------------

    Time Since Last Restart 2 days 13:53:23


                        Local                      Remote Offline
                                                   Last Data
    Active Firmware     96.05
    Inactive Firmware   12.15
    Bootcode            06.30

    1)  Software Reset      Reset                  Reset
    2)  Swap Bank & Reset   Swap                   Swap

    3)  Get New File with TFTP

                         Select [1-3]:

------------------------------------Messages------------------------------------
```

4. At the prompts, type the IP address for the TFTP, FTP, or SFTP server and the Filename.

5. When ready, type [Y] to initiate the file transfer.

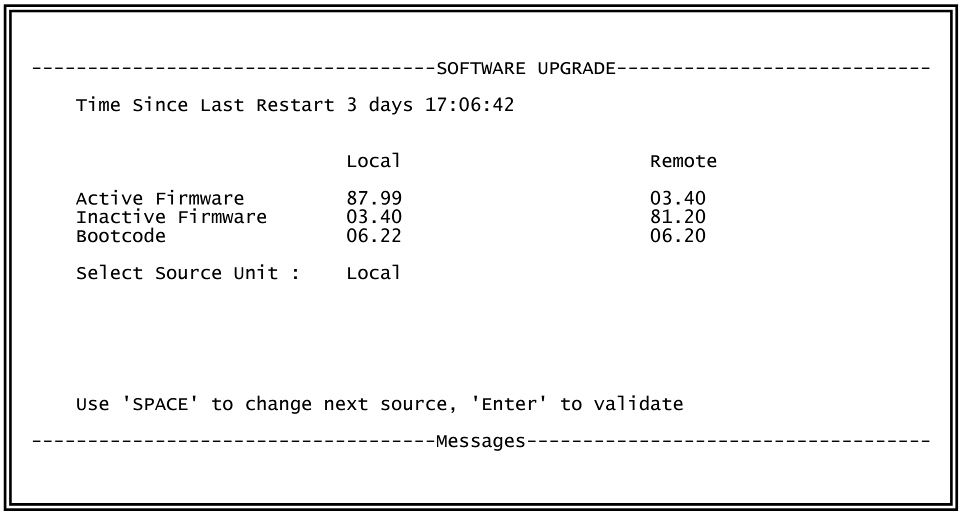


```
----------------------------------TFTP SOFTWARE UPGRADE-------------------------
    Time Since Last Restart 2 days 18:55:08




    Host IP Address :                172.16.85.100
    Save in Non Volatile RAM? :      y
    File Name: N525500.zip
    File transfer to unit now ?      y






    Please enter Y or N .
------------------------------------Messages------------------------------------
```

To upgrade a remote N525, or upgrade the local N525 from software stored on a Domain Management Module of the UCS1000 or UCS1002 chassis through an L51 or L357 follow these steps.

Note: The SideBand Management Channel must be enabled with the remote N525, L351 or L357.

1. Verify that SBMC is enabled on both the local and remote N525s; details on page 3-43.



```
------------------------------------SOFTWARE UPGRADE----------------------------
    Time Since Last Restart 3 days 17:06:42

                            Local                      Remote

    Active Firmware         87.99                      03.40
    Inactive Firmware       03.40                      81.20
    Bootcode                06.22                      06.20

    Select Source Unit :    Local






    Use 'SPACE' to change next source, 'Enter' to validate
------------------------------------Messages------------------------------------
```

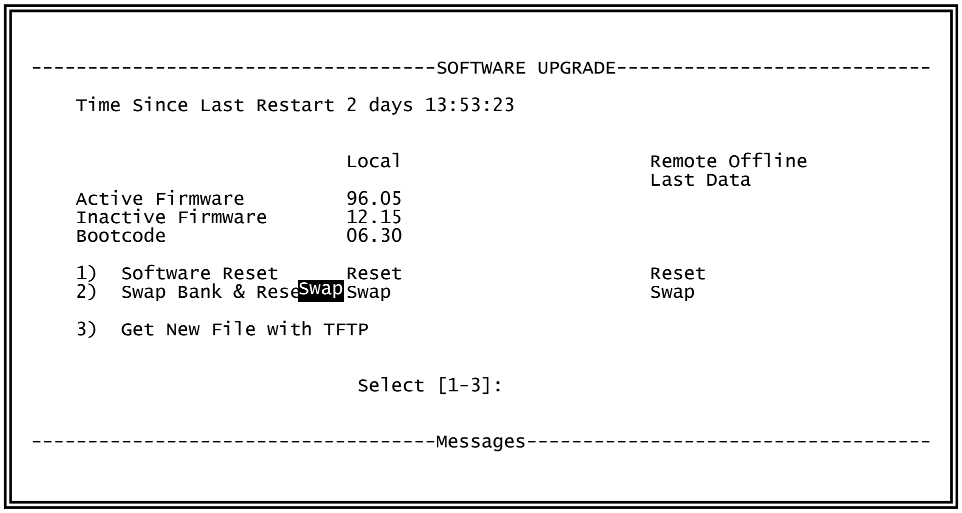
2. From the Main Menu, type [7], "Software Upgrade," and press <Enter>.

3. At the Software Upgrade Menu, type [4], "Copy Software from Source unit to Destination unit," and press <Enter>.

4. 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 [7], "Software Upgrade," and press <Enter>.
2. At the Software Upgrade Menu, type [2], "Swap Bank & Reset," press <Tab> to highlight the Remote column, and press <Enter>.



```
------------------------------------SOFTWARE UPGRADE----------------------------

    Time Since Last Restart 2 days 13:53:23


                            Local                       Remote Offline
                                                        Last Data
    Active Firmware         96.05
    Inactive Firmware       12.15
    Bootcode                06.30

    1)  Software Reset      Reset                       Reset
    2)  Swap Bank & ReseSwap Swap                       Swap

    3)  Get New File with TFTP


                             Select [1-3]:


------------------------------------Messages------------------------------------
```

3. Type [2], "Swap Bank & Reset," check that the Local column is highlighted, and press <Enter>. Both modules reset and start using the new firmware.

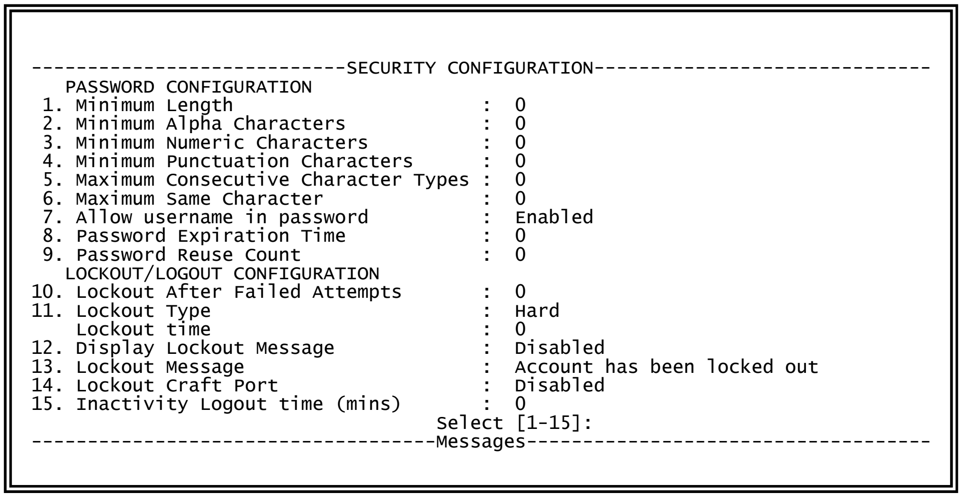
Configuring Access Security

The N525 has comprehensive management access security features, including SNMPv3 authorization, RADIUS, configurable password formatting and user access controls. Typically, you must have supervisor access to configure and manage security for the N525.

Setting General Security Parameters

General security parameters include passwords characteristics, unsuccessful log-in attempt lockout, and inactivity timer. To set general security parameters, access the Security Configuration Menu and follow these steps:

1. At the Main Menu, type [1], "System Configuration," and press <Enter>.
2. From the System Configuration Menu, type [3], "Security Configuration," and press <Enter>.



```
----------------------------SECURITY CONFIGURATION------------------------------
   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
 6. Maximum Same Character            :  0
 7. Allow username in password        :  Enabled
 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
                                    Select [1-15]:
------------------------------------Messages------------------------------------
```

3. At the Security Configuration Menu, type the number for the item you wish to configure and press <Enter>. Type the applicable information or press <Space> to cycle through the options for that item. Press <Enter> to select the option or to enter the information you typed.

   Password Configuration

   a. **Minimum Length**
   Minimum length in characters of a valid password. 0 – 15 Characters

   b. **Minimum Alpha Characters**
   Minimum number of alpha (a-z) characters required in a valid password. 0 – 15 Characters, 0 disables restriction.

   c. **Minimum Numeric Characters**
   Minimum number of numeric (0-9) characters required in a valid password. 0 – 15 Characters, 0 disables restriction.

d. **Minimum Punctuation Characters**
Minimum number of Punctuation characters required in a valid password. 0 – 15 Characters, 0 disables restriction.

e. **Maximum Consecutive Character Types**
Maximum number consecutive characters of the same character type (Alpha, Numeric, Punctuation) allowed in a valid password. 0 – 15 Characters, 0 disables restriction.

f. **Maximum Same Character**
Maximum number of times a character can be used in a valid password. 0 – 15 Characters, 0 disables restriction.

g. **Allow Username in Password**
Enable or disable using the username as or within the password

h. **Password Expiration Time**
Sets in days, 1 through 365, that the passwords must be reset. , 0 disables Password Expiration.

i. **Password Reuse Count**
Set if the current password can be reused or must be changed to something different. A setting of 0 allows reuse, 1 requires a different password.

Lockout/Logout Configuration

a. **Lockout After Failed Attempts**
Sets the number of failed attempts log-in before the user is locked out. 0 – 10 attempts, 0 disables the Lockout function.

b. **Lockout Type**
Hard requires another user with supervisor access to unlock the account in the User Accounts Menu. Timed requires the User wait (Lockout time) before attempting another log-in attempt.
Lockout Time
Lockout time period, 0 to 30 minutes.

c. **Display Lockout Message**
Enables or disables user screen display of a Lockout Message

d. **Lockout Message**
Sets the Lockout Message to be displayed when the user is Locked Out, up to 30 characters in length

e. **Lockout Craft Port**
Enables or disable management access from the RS-232 serial port to prevent unauthorized access. The craft port can be re-enabled from a Telnet session or a SNMP command

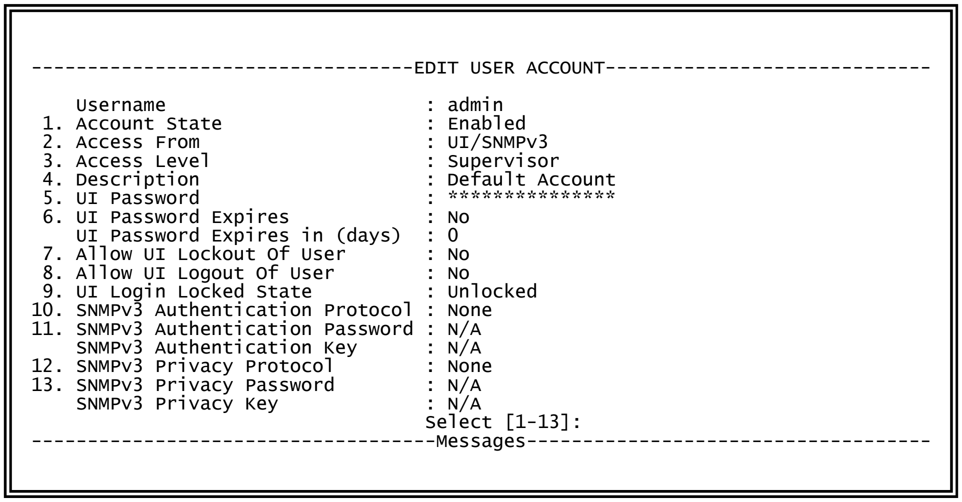
f. **Inactivity Logout Time**
Sets the time, 0 to 30 minutes, when a user session is automatically logged out and disconnected due to inactivity. 0 disables the function.

4. To return to the Main Menu, press <Esc>.

Setting Up User Accounts

You can set up an account for a user, whether another supervisor, operator, or observer, to access the N525. You can also update or delete usernames or permissions. Setting certain values for some parameters, such as SNMPv3 Authentication and Privacy Protocols, determine or limit which values you can set for other parameters. To manage a user account, follow these steps:

1. At the Main Menu, type [1], "System Configuration," and press <Enter>.
2. At the System Configuration Menu, type [4], "Account Configuration," and press <Enter>. The User Accounts Menu appears.



```
---------------------------------EDIT USER ACCOUNT----------------------------

    Username                       : admin
 1. Account State                  : Enabled
 2. Access From                    : UI/SNMPv3
 3. Access Level                   : Supervisor
 4. Description                    : Default Account
 5. UI Password                    : ***************
 6. UI Password Expires            : No
    UI Password Expires in (days)  : 0
 7. Allow UI Lockout Of User       : No
 8. Allow UI Logout Of User        : No
 9. UI Login Locked State          : Unlocked
10. SNMPv3 Authentication Protocol : None
11. SNMPv3 Authentication Password : N/A
    SNMPv3 Authentication Key      : N/A
12. SNMPv3 Privacy Protocol        : None
13. SNMPv3 Privacy Password        : N/A
    SNMPv3 Privacy Key             : N/A
                                   Select [1-13]:
-----------------------------------Messages-----------------------------------
```

3. To add a user, type [a], or to edit an existing user, type [e], and press <Enter>. Type the username. Follow the prompts on the Edit User Account Menu to enter values or select options by pressing <Space> to cycle through available parameters.

   a. **Account State**
   Enables or Disables user access to the N525's management functions. Options are Enabled and Disabled.

   b. **Access From**
   Configures authorized access methods via the User Interface (UI) using Telnet, VT100 on the RS-232 serial port, SSH, FTP, and SFTP or by SNMPv3. Options are UI, SNMPv3, or UI/SNMPv3 (both UI and SNMPv3)

   c. **Access Level**
   Assign user privilege level. Levels are supervisor, operator, or observer

   d. **Description**
   Account description. This is optional and is 0 to 17 characters long.

   e. **UI Password**
   Password that allows access through Telnet, Console, SSH, FTP, or SFTP. Passwords are 8 to 15 characters in length.

   f. **UI Password Expires**
   Configures if Passwords expire and require replacement, Yes or No.
   UI Password Expires in (days)

If UI Password Expire is set to ***Yes***; this configures how long the Password is valid. Duration setting from 0 (never) to 365 days. A setting of 0 is equal to UI Password Expire is set to ***No***

g. **Allow UI Lockout of User – Yes/No**
Sets if the User can be blocked from the system after excessive failed attempts to log in.

h. **Allow UI Logout of User**
Sets if user gets automatically logged off upon excessive inactivity

i. **UI Logout Locked State**
Displays current user state: Locked, Unlocked, Logged Out, or Logged In

j. **SNMPv3 Authentication Protocol**
Sets SNMPv3 authentication protocol: MD5, SHA, or None

k. **SNMPv3 Authentication Password**
Password that generates the MD5 or SHA authentication key: 8 to 15 characters
SNMPv3 Authentication Key
Displays the MD5 or SHA Authentication Protocol Key that authenticates the user. the Key is generated automatically by the Authentication Password, but can be changed if the user's host uses a different Authentication Key generation algorithm. the Key is 16 Hex characters for MD5 protocol or 20 Hex characters for SHA protocol.

l. **SNMPv3 Privacy Protocol**
Selects encryption protocol: DES or None

m. **SNMPv3 Privacy Password**
Password that generates the DES Privacy Protocol Encryption Key: 8 to 15 characters
SNMPv3 Privacy Key
Displays the DES Privacy Protocol Key and is generated automatically from the Privacy Password. It can be changed if the user's host uses a different Privacy Key generation algorithm: 16 Hex characters

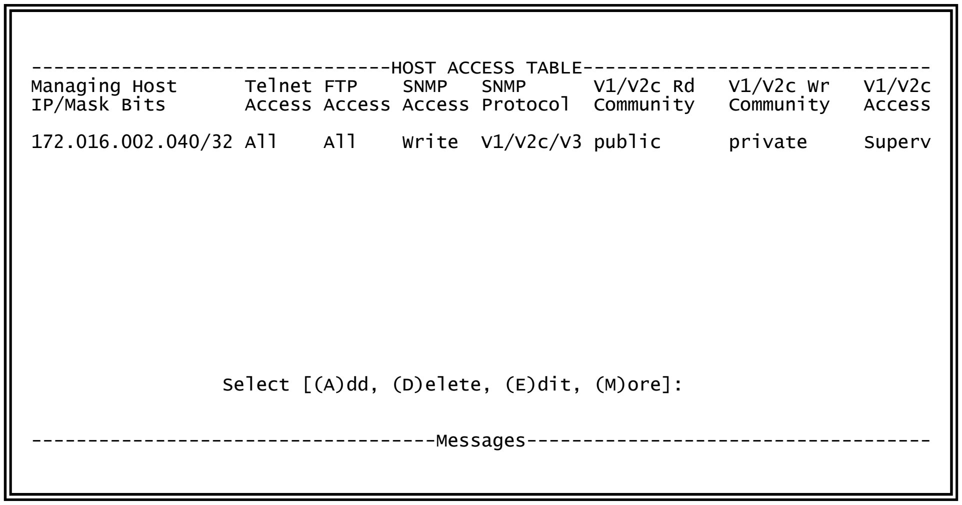
4. To delete a user, type [d], then follow the prompts to select the username and confirm the choice. When completed, the User Accounts Menu reappears.

5. To return to the Main Menu, press <Esc>.

Configuring Host Access

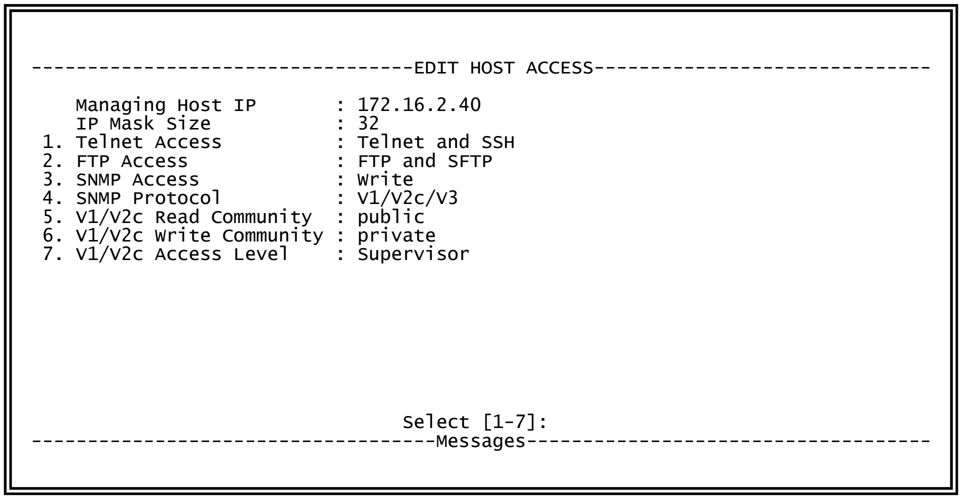
The N525's SNMP Agent allows access by up to 24 Host IP addresses. Configuration and editing the Host information Table is by the Host Access Table Menu. To access the Host Access Table, follow these steps:

1. From the System Configuration Menu, type [1], "IP/SNMP Agent Configuration," and press <Enter> Then type [3], "Host Table," and press <Enter>.



```
-------------------------------HOST ACCESS 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

172.016.002.040/32 All    All    Write  V1/V2c/V3 public      private     Superv









                 Select [(A)dd, (D)elete, (E)dit, (M)ore]:

-----------------------------------Messages-----------------------------------
```

2. At the Host Access Table Menu, type [a] to add a host. At the prompt, enter the Host IP Address and Subnet Mask, or type [e] to edit an existing Host.



```
---------------------------------EDIT HOST ACCESS-----------------------------

    Managing Host IP       : 172.16.2.40
    IP Mask Size           : 32
 1. Telnet Access          : Telnet and SSH
 2. FTP Access             : FTP and SFTP
 3. SNMP Access            : Write
 4. SNMP Protocol          : V1/V2c/V3
 5. V1/V2c Read Community  : public
 6. V1/V2c Write Community : private
 7. V1/V2c Access Level    : Supervisor








                                 Select [1-7]:
-----------------------------------Messages-----------------------------------
```

3. The Edit Host Access Menu sets the following parameters.

   a. **Telnet Access**
   Telnet and SSH, Telnet Only, SSH Only, or None

b. **FTP Access**
Select FTP and SFTP, FTP Only, SFTP Only, or None

c. **SNMP Access**
Select Write (also allows Read access), Read, or None

d. **SNMP Protocol**
Select V1/V2c/V3, V1/V2c, or V3

e. **V1/V2c Read Community**
Enter name of community, up to 11 characters

f. **V1/V2c Write Community**
Enter name of community, up to 11 characters

g. **V1/V2c Access Level**
Select Supervisor, Operator, or Observer

4. To remove a host, type [d], then follow the prompts.
5. To return to the Main Menu, press <Esc>.

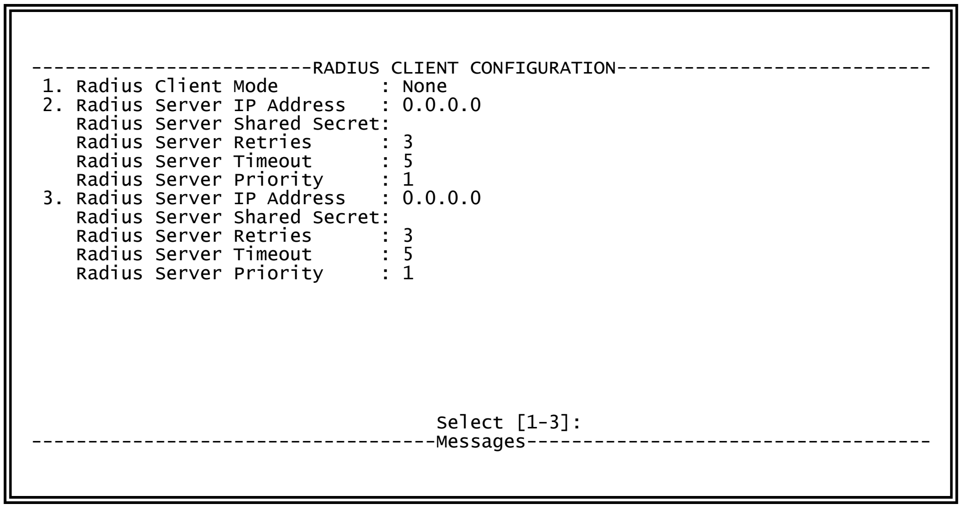
Configuring a Radius Client

Before setting the N525 as a Radius Passthru Client, you must set related attributes on the Radius Server to predefined values in order to properly authenticate and configure the user. The N525 uses four vendor-specific attributes, type 25 in the Radius RFC. Canoga Perkins vendor' identifier is 919.

1. **Attribute 1 - Access From**
   Values: 1, UI (default); 2, SNMP; and 3, UI and SNMP
2. **Attribute 2 - Access Level**
   Values: 2, Observer (default); 3, Operator; and 4, Supervisor
3. **Attribute 3 - Description**
   A string, optional and not predefined. The default is "Radius Account."
4. **Attribute 4 - Logout User**
   Values: 0, No, and 1, Yes (default).

Use the Radius Client Configuration Menu to set up communications with the Radius Server to enable Radius Authentication of users at login. To access the Radius Client Configuration Menu, follow these steps:

1. From the System Configuration Menu, type [6], "Radius Client Configuration," and press <Enter>. The Radius Client Configuration Menu appears.



```
-------------------------RADIUS CLIENT CONFIGURATION----------------------------
 1. Radius Client Mode         : None
 2. Radius Server IP Address   : 0.0.0.0
    Radius Server Shared Secret:
    Radius Server Retries      : 3
    Radius Server Timeout      : 5
    Radius Server Priority     : 1
 3. Radius Server IP Address   : 0.0.0.0
    Radius Server Shared Secret:
    Radius Server Retries      : 3
    Radius Server Timeout      : 5
    Radius Server Priority     : 1







                                    Select [1-3]:
------------------------------------Messages------------------------------------
```

2. At the prompt, type [1] to set the authentication mode. Type [2] or [3] to configure access to a primary and alternate Radius servers, and then follow the prompts on the screen.

   a. **Radius Client Mode**
   Configures the primary and secondary authentication servers. The secondary server is accessed if the primary server does not respond or rejects the user. "Radius" is the Radius Server, "Local" is the N525's User Account database. "None" uses only the N525 account database. Choices are Radius then Local, Local then Radius, or None

   b. **Radius Server**
   Enter values for these parameters for a primary or alternate Radius server:

   c. **IP Address**
   Sets the address for the Radius Server. An Address 0.0.0.0 indicates no server

   d. **Shared Secret**
   Must match the Shared Secret set on the Radius Server

   e. **Retries**
   How many times the N525 tries to authenticate the user before trying the Secondary Server or giving up. Range is 0 to 10

   f. **Timeout**
   How long, in seconds, between unsuccessful attempts. Range is 1 to 30

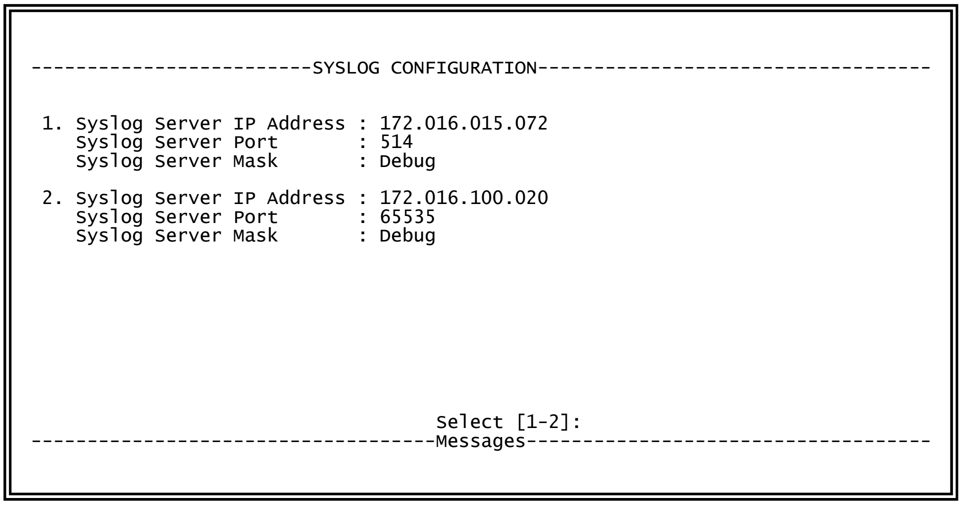
   g. **Priority**
   Sets which server to contact first; Range is 1 (highest priority) to 255 lowest priority) Should priority get set the same for two servers, the N525 will alternate tries between the servers

3. To return to the Main Menu, press <Esc>.

Syslog Client Configuration

You can configure and display two server destinations for Syslog messages. In addition to setting the host address and port, you can set the server mask for the notification. To access and update the Syslog Client Configuration, follow these steps:

1. From the System Configuration Menu type [9], "Syslog Client Configuration," and press <Enter>, then type [3], "Trap Table," and press <Enter>. The Trap/Notification Destination Table screen appears.



```
-------------------------SYSLOG CONFIGURATION-----------------------------------

 1. Syslog Server IP Address : 172.016.015.072
    Syslog Server Port       : 514
    Syslog Server Mask       : Debug

 2. Syslog Server IP Address : 172.016.100.020
    Syslog Server Port       : 65535
    Syslog Server Mask       : Debug







                                     Select [1-2]:
------------------------------------Messages------------------------------------
```

2. To enter a new Syslog Server to edit and existing entry, select Syslog Server [1] or [2] and press <Enter>. Enter the values for the Server.

   a. **Syslog Server IP Address**
   Enter the IP address for the Syslog Server

   b. **Syslog Server Port**
   Enter the UDP Port number used by the Syslog Server, 1-65535

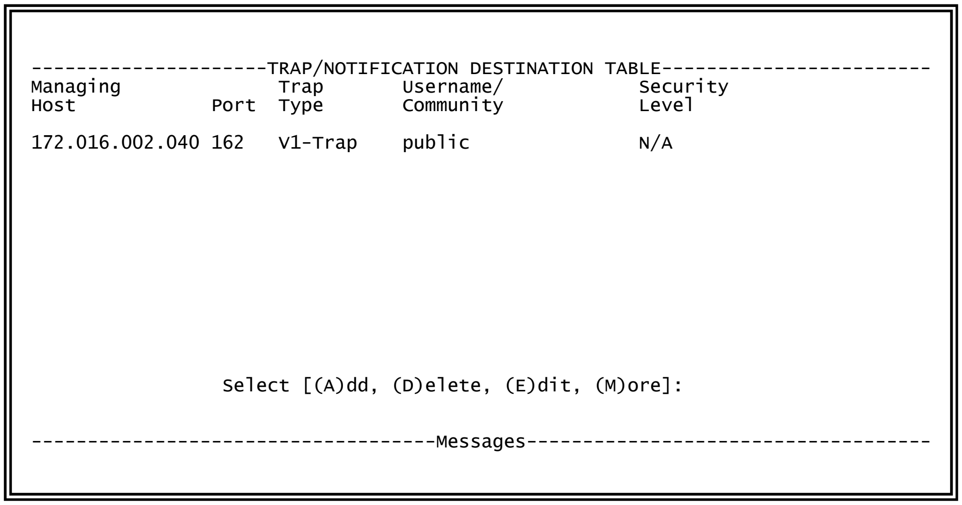
   c. **Syslog Server Mask**
   This sets the Syslog Message Mask. Pressing <Space> cycles through the options. Options are Debug, Emergency, Alert, Critical, Error, Warning, Notice and Informational.

3. To return to the Main Menu, press <Esc>.

Trap Destination Configuration

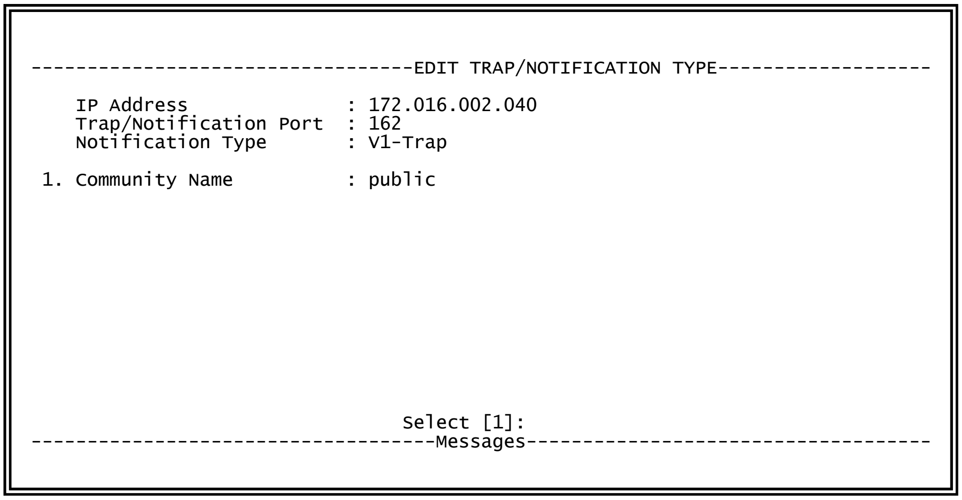
You can configure and display the destinations for Trap messages. In addition to setting the host address and port, you can set the security level for the notification, and then set values for various security related parameters. To access and update the Trap Notification/Destination Table, follow these steps:

1. From the System Configuration Menu type [1], "IP/SNMP Agent Configuration," and press <Enter>, then type [3], "Trap Table," and press <Enter>. The Trap/Notification Destination Table screen appears.



```
---------------------TRAP/NOTIFICATION DESTINATION TABLE------------------------
Managing              Trap       Username/           Security
Host             Port  Type       Community           Level

172.016.002.040 162   V1-Trap    public              N/A









                 Select [(A)dd, (D)elete, (E)dit, (M)ore]:

------------------------------------Messages------------------------------------
```

2. To add a destination, type [a] and press <Enter>. To edit an existing destination, type [e] and press <Enter>, then follow the prompts to set values for these parameters:



```
---------------------------------EDIT TRAP/NOTIFICATION TYPE-------------------

    IP Address             : 172.016.002.040
    Trap/Notification Port  : 162
    Notification Type       : V1-Trap

 1. Community Name          : public









                                 Select [1]:
-----------------------------------Messages------------------------------------
```

a. **IP Address**
IP address of the destination

b. **Trap/Notification Port**
UDP Port number for the destination. Range is 1 to 65535, typically set to 162

c. **Notification Type**
Sets the SNMP version and configuration

V1-Trap:	Unacknowledged message with SNMPv1 protocol
V2c-Trap:	Unacknowledged message with SNMPv2c protocol
V2c-Inform:	Acknowledged message with SNMPv2c protocol
V3-Trap:	Unacknowledged message with SNMPv3 authentication and optional message encryption
V3-Inform:	Acknowledged message with SNMPv3 authentication and optional message encryption

d. **Community Name**
Enter the V1-Trap, V2-Trap, or V2c-Inform notification Community Name. Up to 10 characters.

e. **SNMPv3- Trap Notification**
Pressing <Space> cycles through security options when SNMPv3 Trap Notification is selected.

- Security Name: The name of the N525 user account.
- Security Level: No Auth/No Priv - No user authentication or message encryption
  Auth/No Priv - Authentication by user name, no message encryption
  Auth/Priv - Authentication by user name and message encryption

f. **SNMPv3- Inform Notification**
To configure SNMPv3-Inform notification, either type [a] value and press <Enter> or

press <Space> to cycle through the options for these parameters:

- Security Name: Enter the name of the user account at the destination. Up to 10 characters
- Engine ID: Enter the SNMP Engine ID at the destination. 64 Hex characters.
- Authentication Protocol: Notification authentication. Option are MD5, SHA, or None.
- Authentication Password: The password that generates the authentication key for the message when the authentication protocol is MD5 or SHA. 8 to 15 characters.
- Authentication Key: The authentication key for MD5 or SHA Authentication Protocol. The key generates automatically from the Authentication Password, but can be changed if the destination uses a different Authentication Key generation algorithm. 16 Hex characters for MD5 protocol or 20 Hex characters for SHA protocol.
- Privacy Protocol: Set the protocol for encrypting the notification when MD5 or SHA is used. Options are DES or None.
- Privacy Password: If the Privacy Protocol is DES, enter the password that generates the encryption key for the message. 8 to 15 characters.
- Privacy Key: Shows the that encrypts the message for DES Privacy Protocol key. This key automatically generates from the Privacy Password, but can be changed if the destination uses a different Privacy Key generation algorithm. 16 Hex characters.
- Security Level: No Auth/No Priv - No user authentication or message encryption
  Auth/No Priv - Authenticates by user name, no message encryption
  Auth/Priv - Authenticates by user name and message encryption
- Retries: Number of times to resend the message if not acknowledged. Range is 0 to 10
- Timeout in Seconds: Time to wait, in seconds, for an acknowledgement before resending. Range is 1 to 30 seconds

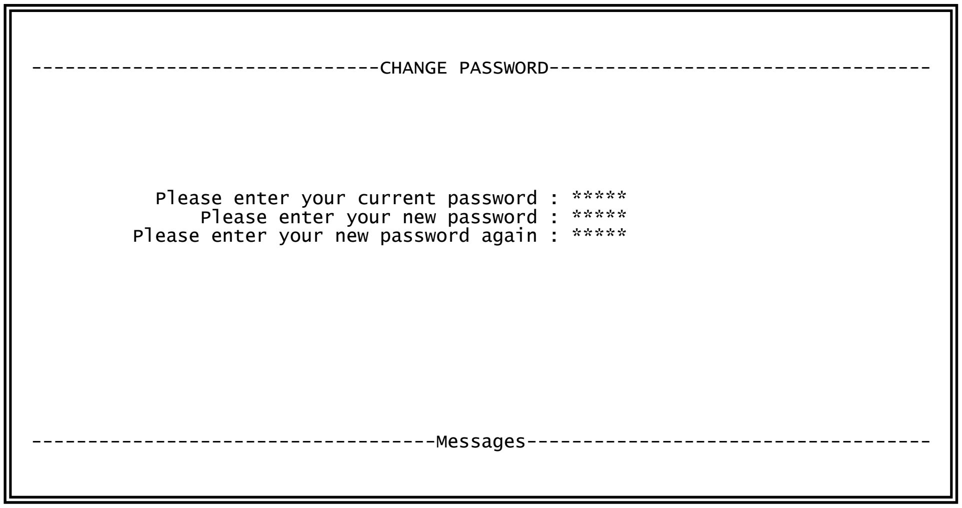
3. To delete a destination, type [d] and press <Enter>. At the prompt, highlight the IP Address for that Host you want to delete and press <Enter>. The host table appears again with your changes.

4. To return to the Main Menu, press <Esc>.

Changing Your Password

Whether you have supervisor, operator, or observer access, you can update your password in order to maintain system security. You cannot change the password for any other users. To update your password, follow these steps:

1. At the Main Menu, type [6], "Utilities," and press <Enter>.
2. At the Utilities screen, type [3], "Change Password," and press <Enter>, then follow the prompts on the screen to enter your current password, then change it and confirm your new password.



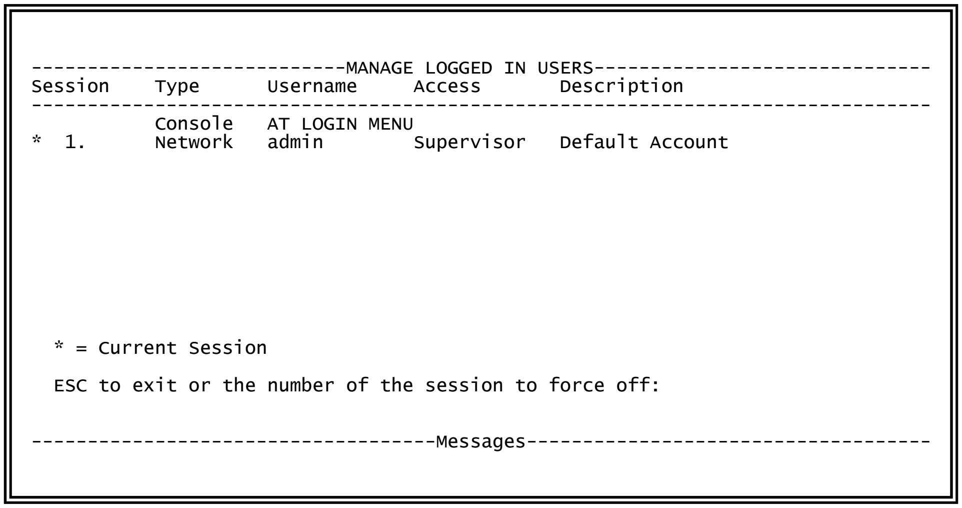
```
-------------------------------CHANGE PASSWORD----------------------------------




           Please enter your current password : *****
               Please enter your new password : *****
         Please enter your new password again : *****








-----------------------------------Messages-------------------------------------
```

3. To return to the Main Menu, press <Esc>.

Managing Logged In Users

At times, you may need to monitor which users are currently logged in to the N525 and, if needed, force off specific sessions (requires supervisor access). The Manage Logged In Users screen shows current users by session number. An asterisk (*) next to the session number indicates your session. To access the Manage Logged In Users screen, follow these steps:

1. From the Main Menu, type [8], "Manage Logged In Users," and press <Enter>.
2. To force a session off, type the number for that session and press <Enter>.



```
----------------------------MANAGE LOGGED IN USERS------------------------------
Session    Type      Username     Access       Description
--------------------------------------------------------------------------------
           Console   AT LOGIN MENU
*  1.      Network   admin        Supervisor   Default Account








  * = Current Session

  ESC to exit or the number of the session to force off:

------------------------------------Messages------------------------------------
```

Note: Although a user with any level of access can view this screen, you must have supervisor access to force off a session.

3. To return to the Main Menu, press <Esc>.

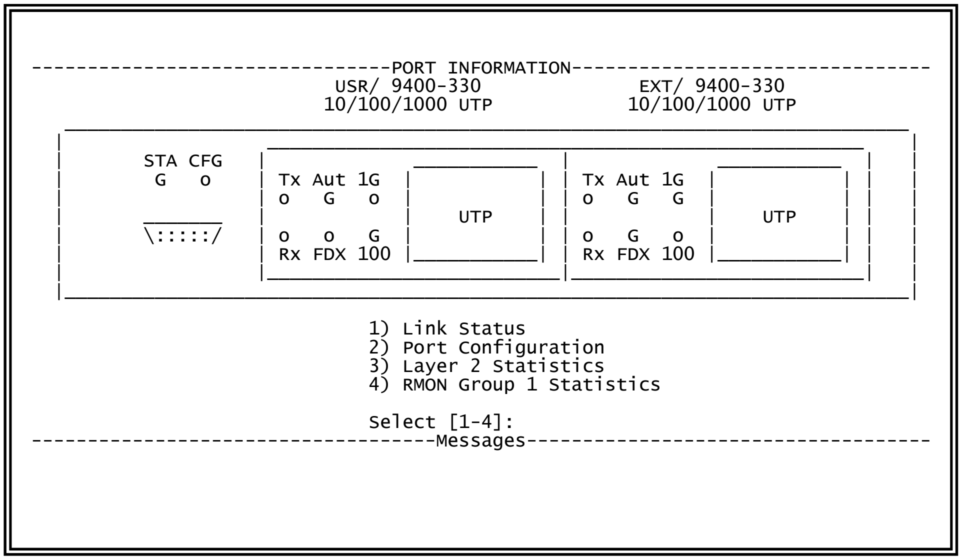
Managing the Network Interface

When configuring ports, it is best to configure options in this order:

1. Set up the physical layer, such as port speeds.
2. Set up the VLAN rules, translation, and priority bits.
3. When all aspects of the link are ready, connect cables and start the network services.

Configuring Ports

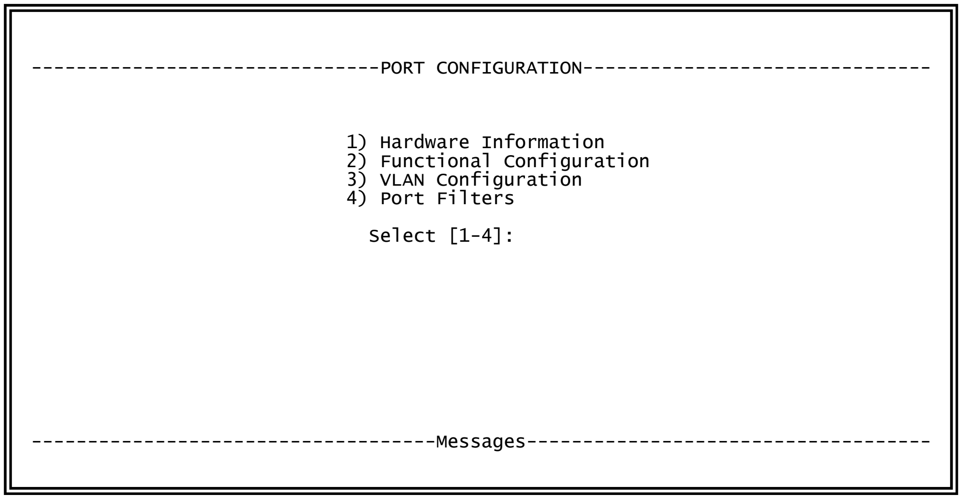
Port functions are configured on the Functional Configuration Menu. This screen also displays data speed and duplex settings for the local N525 and the remote N525, L351 or L357. If the remote device is an L351 or L357, you can configure that device. For details, see the user manual for the L351 or L357. The Port Information screen displays general Port status and menu for access Port Configuration and port Status/Performance functions.



```
--------------------------------PORT INFORMATION--------------------------------
                           USR/ 9400-330              EXT/ 9400-330
                          10/100/1000 UTP            10/100/1000 UTP
   ____________________________________________________________________________
  |                  _____________________________________________________     |
  |       STA CFG   |             ___________  |             ___________  |    |
  |        G   o    | Tx Aut 1G  |           | | Tx Aut 1G  |           | |    |
  |                 | o   G   o  |           | | o   G   G  |           | |    |
  |       _______   |            |    UTP    | |            |    UTP    | |    |
  |       \:::::/   | o   o   G  |           | | o   G   o  |           | |    |
  |                 | Rx FDX 100 |___________| | Rx FDX 100 |___________| |    |
  |                 |__________________________|__________________________|    |
  |____________________________________________________________________________|

                              1) Link Status
                              2) Port Configuration
                              3) Layer 2 Statistics
                              4) RMON Group 1 Statistics

                              Select [1-4]:
------------------------------------Messages------------------------------------
```

To configure N525 ports, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [2], "Port Configuration," and press <Enter>.



```
-------------------------------PORT CONFIGURATION-------------------------------


                            1) Hardware Information
                            2) Functional Configuration
                            3) VLAN Configuration
                            4) Port Filters

                              Select [1-4]:







------------------------------------Messages------------------------------------
```

2. At the Port Configuration Menu, type [2], "Functional Configuration," and press <Enter>.

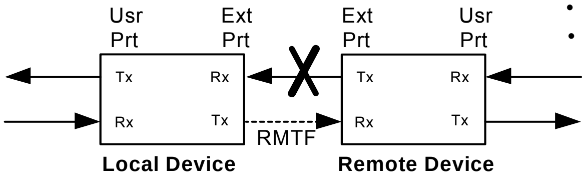
3. At the Functional Configuration Menu, type the number for an item and press <Enter>. Pressing <Space> cycles through the options. Press <Tab> to highlight the select Local or Remote columns. Press <Enter> to select an option.

   a. **User Port Setting**
      Sets data rate and duplex option on the User port. After typing [1] <Enter>, pressing <Space> cycles through the Data Speed and Duplex options. Options are Interface Module dependant.

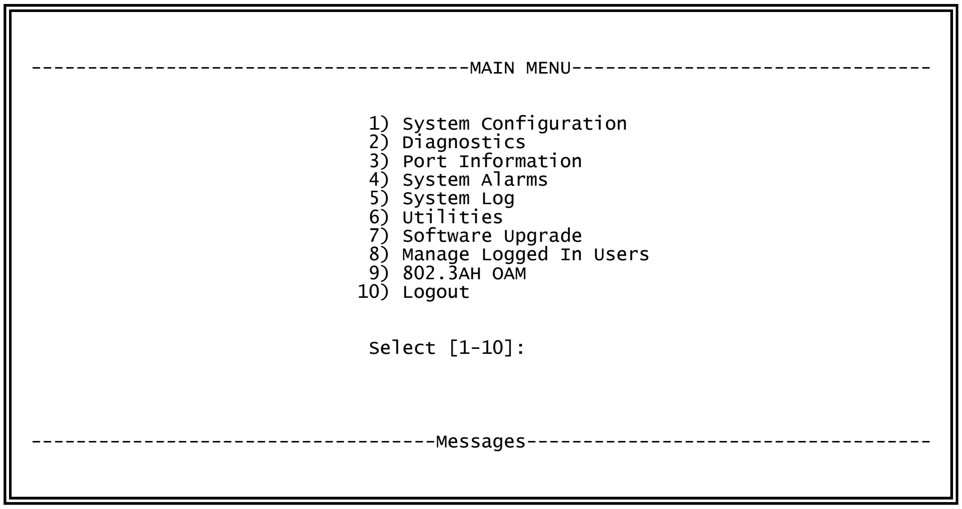
   b. **Ext Port Setting**
      Sets data rate and duplex option on the User port. After typing [1] <Enter>, pressing <Space> cycles through the Data Speed and Duplex options. Options are Interface Module dependant.

   c. **RMTF**
      Enables or Disables Remote Fault Forwarding (RMTF) when SBMC is enabled. Enables or Disables Remote Fault Forwarding and Link Loss Echo (RMTF/LLE) when SBMC disabled. Pressing <Space> cycles through the options. Options are Disabled, Ext Port Enabled.

      If an optical port loses the receive optical signal, it sends a Remote Fault (RMTF) signal on its Transmit to the distant end on the optical link. The Rx LED is off, and an alarm flags the link loss on the optical port. When a optical port receives a Remote Fault signal, the Rx LED lights red and an alarm flags the remote side optical link failure. Both local and remote link partners must be configured to the same RMTF enable/disable setting. RMTF complies with the IEEE802.3u Remote Fault standard. See Figure 18.



- Local device Rx detects link loss
- Tx transmits RMTF to remote device
- Local device Rx turns OFF
- Remote device Rx lights red

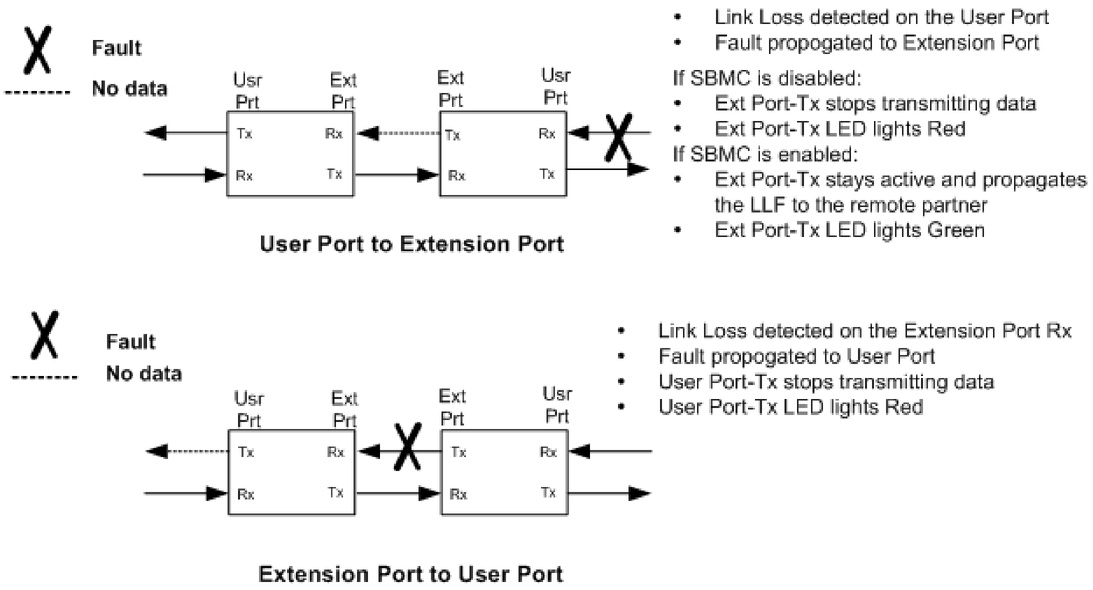


```
---------------------------------------MAIN MENU---------------------------------


                              1) System Configuration
                              2) Diagnostics
                              3) Port Information
                              4) System Alarms
                              5) System Log
                              6) Utilities
                              7) Software Upgrade
                              8) Manage Logged In Users
                              9) 802.3AH OAM
                             10) Logout

                              Select [1-10]:



------------------------------------Messages-------------------------------------
```

Figure 22 - Remote Fault Signal

d. **Link Loss Fwd**
Enables or Disables Link Loss Forwarding (LLF). Pressing <Space> cycles through the options. Options are Disabled, User – Ext, Ext – User, and Both Directions.

When Link Loss Forwarding (LLF) is enabled, a fault on one side of the N525 propagates to the other side to notify that device and stops signal transmission (brings down the link). See Figure 19. Set the LLF propagation to User to Extension, Extension to User, or both directions. Set this in the User Interface at the Functional Configuration screen (see Managing the Network Interface).



- Link Loss detected on the User Port
- Fault propogated to Extension Port

If SBMC is disabled:
- Ext Port-Tx stops transmitting data
- Ext Port-Tx LED lights Red

If SBMC is enabled:
- Ext Port-Tx stays active and propagates the LLF to the remote partner
- Ext Port-Tx LED lights Green

User Port to Extension Port

- Link Loss detected on the Extension Port Rx
- Fault propogated to User Port
- User Port-Tx stops transmitting data
- User Port-Tx LED lights Red

Extension Port to User Port

Figure 23 - Link Loss Forwarding Propagation

e. **Flow Control**
Enables or Disables flow control on the Remote port. Pressing <Space> cycles through the options. Options are Disabled, Ext Port Enabled.

f. **Maximum Frame Size:** Sets maximum allowable Ethernet Frame size the N525 will forward. Size range is 1518-10000.

g. **Sideband Management**
Enables or disables SideBand Management Channel (SBMC) communications with a remote N525, L351 or L357. When enabled, pressing <Ctrl-L> verifications SMBC connectivity with the remote unit.

h. **Remote Configuration**
Displays Functional Configuration of SBMC connected remote N525, L351 or L357.

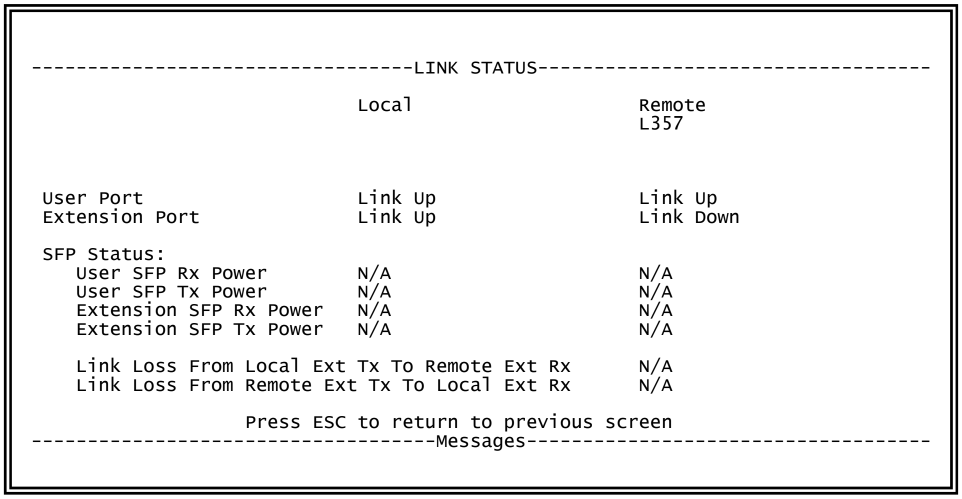
4. To return to the Main Menu, press <Esc>.

Check Port and Link Status

The Port Information screen shows the current conditions for the N525 ports. The Link Status screen shows current conditions for the link, including SFP power. To access port and link status, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. The Port Information screen appears.

2. To view status for the link, at the Port Information screen, type [1], "Link Status," and press <Enter>. The Link Status screen appears.



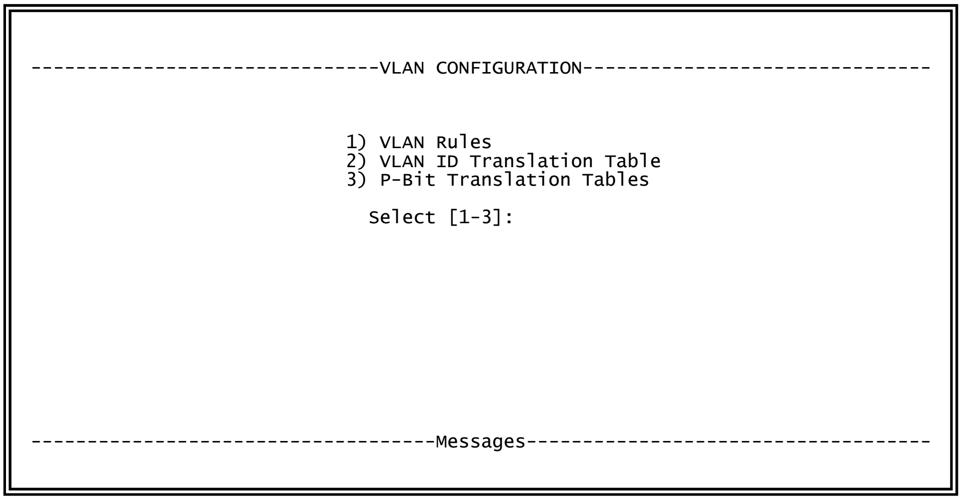
```
----------------------------------LINK STATUS-----------------------------------
                            Local                    Remote
                                                     L357



 User Port                  Link Up                  Link Up
 Extension Port             Link Up                  Link Down

 SFP Status:
    User SFP Rx Power       N/A                      N/A
    User SFP Tx Power       N/A                      N/A
    Extension SFP Rx Power  N/A                      N/A
    Extension SFP Tx Power  N/A                      N/A

    Link Loss From Local Ext Tx To Remote Ext Rx     N/A
    Link Loss From Remote Ext Tx To Local Ext Rx     N/A

                  Press ESC to return to previous screen
------------------------------------Messages------------------------------------
```

3. To return to the Main Menu, press <Esc>.

Configuring VLAN Rules, Priority, and Translation

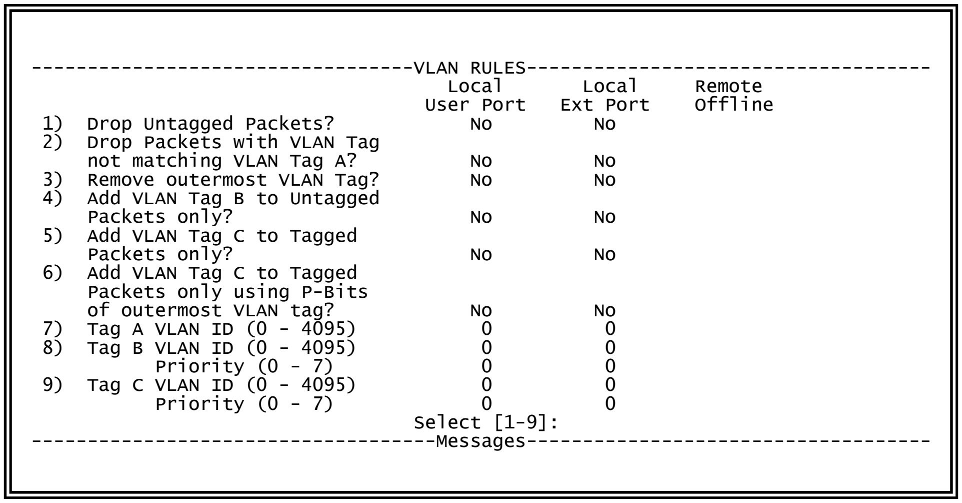
The VLAN Configuration Menu provide options to configure user traffic VLAN tagging parameters on User and Extension ports. To configure VLAN tags, translation, and priority, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [2], "Port Configuration," and press <Enter>. At the Port Configuration Menu, type [3], "VLAN Configuration and press <Enter>.



```
-------------------------------VLAN CONFIGURATION-------------------------------


                            1) VLAN Rules
                            2) VLAN ID Translation Table
                            3) P-Bit Translation Tables

                              Select [1-3]:









------------------------------------Messages------------------------------------
```

2. To configure VLAN Tagging rules, type [1], "VLAN Rules," and press <Enter>."



```
----------------------------------VLAN RULES------------------------------------
                                     Local       Local     Remote
                                   User Port   Ext Port    Offline
 1)  Drop Untagged Packets?            No          No
 2)  Drop Packets with VLAN Tag
     not matching VLAN Tag A?          No          No
 3)  Remove outermost VLAN Tag?        No          No
 4)  Add VLAN Tag B to Untagged
     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
                                  Select [1-9]:
-----------------------------------Messages-------------------------------------
```

3. At the VLAN Rules Menu, type the number for an item and press <Enter>. Pressing <Space> cycles through the options for that item, pressing <Enter> selects the option. Pressing <Tab> moves between User Port and Ext Port columns. When connected to a remote N525 and SBMC is enabled, you can configure options on the remote N525.

   a. **Drop Untagged Packets?**
   The N525 will discard all user traffic that does not have a VLAN Tag. Yes discards packets, No does not.

   b. **Drop Packets with VLAN Tag not matching VLAN Tag A?**
   The N525 discards all user traffic that does not have a VLAN Tag matching to VLAN Tag A (menu item 7). Yes discards packets, No does not.

   c. Remove outermost VLAN Tag?
   Removes the outer-most VLAN Tag. Takes no action on untagged packets. Yes removes outermost tag, No does not.

   d. Add VLAN Tag B to Untagged Packets only?
   Adds VLAN Tag B (item 8 below) to all untagged packets. Yes add tags, No does not.

   e. Add VLAN tag C to tagged packets only?
   Adds VLAN Tag C (item 9 below) to all untagged packets. Yes add tags, No does not.

   f. Add VLAN Tag C to Tagged Packets only using P-Bits of outermost VLAN tag?
   Adds VLAN Tag B (item 8 below) to all untagged packets, using the Priority Bit setting of the user's packet (if tagged), overriding the VLAN Tag C's Priority Bit setting. Yes add tags with user P-Bit setting, No does not.

   g. **Tag A VLAN ID (0-4095)**
   Sets VLAN ID for Tag A. ID setting of 0 – 4095 are valid.

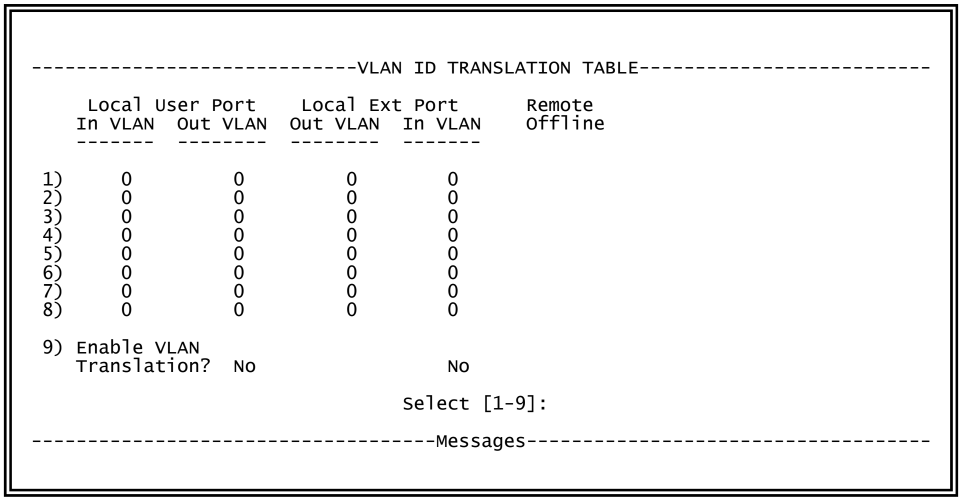
   h. **Tag B VLAN ID (0-4095)**
   Sets VLAN ID for Tag B. ID setting of 0 – 4095 are valid.
   Priority (0 - 7)
   Sets P-Bit of VLAN Tag B. Values of 0-7 are Valid.

   i. **Tag C VLAN ID (0-4095)**
   Sets VLAN ID for Tag C. ID setting of 0 – 4095 are valid.
   Priority (0 - 7)
   Sets P-Bit of VLAN Tag C. Values of 0-7 are Valid.

4. To return to the Main Menu, press <Esc>.

The N525 can change VLAN Tag IDs on user packets. This is useful to avoid VLAN ID conflicts in the network. The N525 can translate up to 8 VLAN IDs. To Configure VLAN Translations so outgoing packets receive a new tag based on the previous tag, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [2], "Port Configuration," and press <Enter>. At the Port Configuration Menu, type [3], "VLAN Configuration and press <Enter>.
2. At the VLAN Configuration Menu, type [2], "VLAN ID Translation Table," and press <Enter>."



```
-----------------------------VLAN ID TRANSLATION TABLE--------------------------

     Local User Port    Local Ext Port      Remote
    In VLAN  Out VLAN  Out VLAN  In VLAN    Offline
    -------  --------  --------  -------

 1)     0         0         0        0
 2)     0         0         0        0
 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 VLAN
    Translation?  No                 No
                                  Select [1-9]:

------------------------------------Messages------------------------------------
```

3. To add an entry to the Table or change an existing entry, type the entry number (1 to 8). As you enter VLAN IDs, the cursor will automatically move from one column to the next. If the N525 will corrected to a remote N525 and SBMC is enabled, the remote N525 will also be configured.

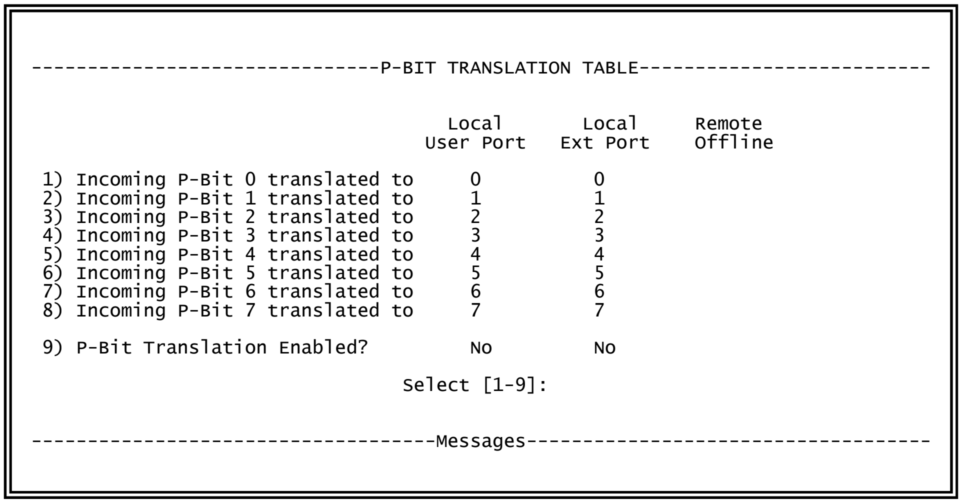
   Type the VLAN ID the N525 will receive from the **Local User Port - In VLAN** and press <Enter>.
   Type the VLAN ID the N525 will change the In VLAN ID into and send on the Extension port (**Local User Port - Out VLAN)** press <Enter>.
   Type the VLAN ID the N525 will receive from the **Local Ext Port - In VLAN** and press <Enter>.
   Type the VLAN ID the N525 will change the In VLAN ID into and send on the Extension port (**Local User Port - Out VLAN)** press <Enter>.
   The above steps will be repeated for the remote N525 when SBMC is enabled.

4. To enable or disable use of the VLAN Translation Table on the User or Extension ports, type [9] and press <Enter>; press <Tab> to cycle through the ports.
5. To return to the Main Menu, press <Esc>.

To configure VLAN Priority Bit (P-Bit) follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [2], "Port Configuration," and press <Enter>. At the Port Configuration Menu, type [3], "VLAN Configuration and press <Enter>.

2. At the VLAN Configuration Menu, type [3], "P-Bit Translation Tables," and press <Enter>.



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

                                   Local       Local      Remote
                                 User Port   Ext Port    Offline

 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     6          6
 8) Incoming P-Bit 7 translated to     7          7

 9) P-Bit Translation Enabled?         No         No
                                 Select [1-9]:


-----------------------------------Messages------------------------------------
```

3. At the P-Bit Translation Tables, type the number for an incoming P-Bit and press <Enter>, then type values for P-bits for outgoing packets, and then press <Enter> to confirm.

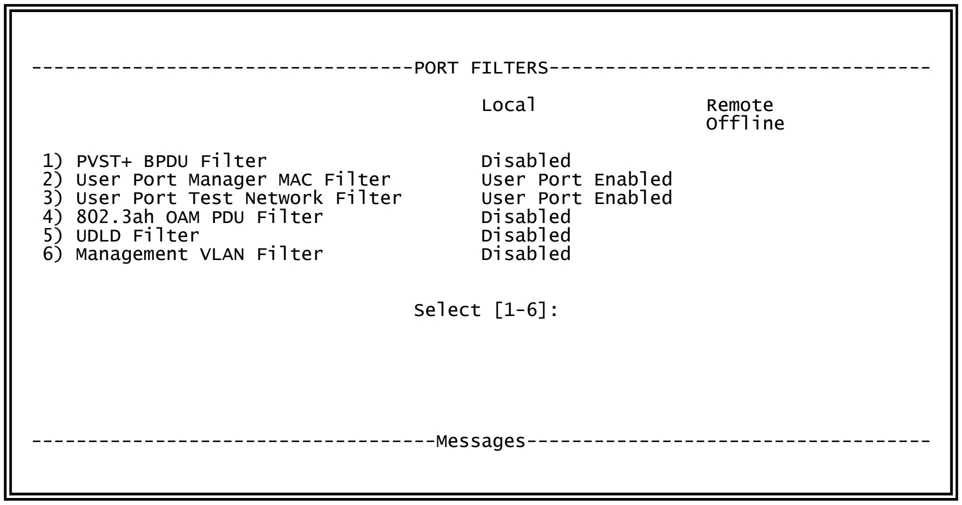
4. To enable or disable the P-Bit Translation Table, type [9] and press <Enter>. Pressing <Tab> cycles between Local User and Extension ports and the remote N525's ports (when SBMC is enabled).

5. To return to the Main Menu, press <Esc>.

Configuring Port Filters

Port Filters enables the N525 to filter certain management and control Ethernet frames from the data stream. To configure the N525 for Filtering, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [2], "Port Configuration," and press <Enter>. At the Port Configuration Menu, type [4], "Port Filters” and press <Enter>.



```
---------------------------------PORT FILTERS---------------------------------
                                        Local               Remote
                                                            Offline

 1) PVST+ BPDU Filter                   Disabled
 2) User Port Manager MAC Filter        User Port Enabled
 3) User Port Test Network Filter       User Port Enabled
 4) 802.3ah OAM PDU Filter              Disabled
 5) UDLD Filter                         Disabled
 6) Management VLAN Filter              Disabled

                                  Select [1-6]:




-----------------------------------Messages-----------------------------------
```

2. At the Port Filters Menu, type the number for an item and press <Enter>. Pressing <Space> cycles through the options for that item, pressing <Enter> selects the option. Pressing <Tab> moves between Local and Remote xxxx columns. When connected to a remote N525 and SBMC is enabled, you can configure options on the remote N525.

   a. **PVST + BPDU Filter**
   The N525 discards PVST and BPDU frames received on the specified port. Choices are Disabled, User Port Enabled, Ext Port Enables and Both Ports Enabled

   b. **User Port Manager MAC Filter**
   The N525 blocks management traffic from being sent to the User port. Choices are User Port Enabled (management frames blocked) and Disabled.

   c. User Port Test Network Filter
   The N525 blocks Test Traffic from being sent to the User port. Choices are User Port Enabled (test frames blocked) and Disabled.

   d. 802.3ah OAM PDU Filter
   The N525 blocks 802.3ah OAM PDU frames from being sent to the User port. Choices are User Port Enabled and Disabled.

   e. UDLD Filter
   The N525 blocks UDLD frames from being sent to the User port. Choices are User Port Enabled and Disabled.

   f. **Management VLAN Filter**
   The N525 blocks management traffic received on the specified port. Choices are Disabled, User Port Enabled, Ext Port Enables and Both Ports Enabled

3. To return to the Main Menu, press <Esc>.

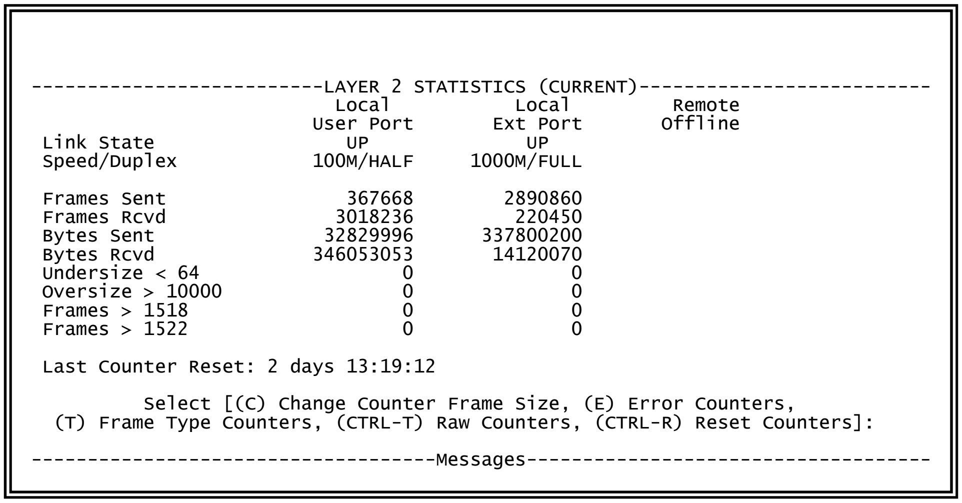
View Port Statistics

You can view these groups of statistics for Ethernet Packets sent through the N525:

- Layer 2 Statistics
  - Link State
  - Speed/duplex
  - Frames Sent and Rcvd
  - Bytes Sent and Rcvd
  - Undersize (<64)
  - Oversize (>10000)
  - Frames > 1518
  - Frames > 1522
- Layer 2 Error Statistics
  - Link State
  - Frames Sent and Rcvd
  - Collisions
  - Alignment Errors
  - Undersize (<64)
  - Oversize (>10000)
  - Fragments
  - CRC Errors
  - Jabber Events
  - Dropped
- Layer 2 Frame Type Statistics
  - Link State
  - Frames Sent and Rcvd
  - Rx and Tx Broadcasts
  - Rx and Tx Multicasts
  - VLAN Tagged
  - Pause Frames
  - Rx and Tx Management
- RMON Group 1 Statistics
  - Drop Events
  - Octets Rcvd
  - Packets Rcvd
  - Broadcasts Rcvd
  - CRC/Align Errors
  - Undersize
  - Oversize
  - Fragments
  - Jabbers
  - Collisions
  - Packet Sizes 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518

To display the Layer 2 Statistics, follow these steps:

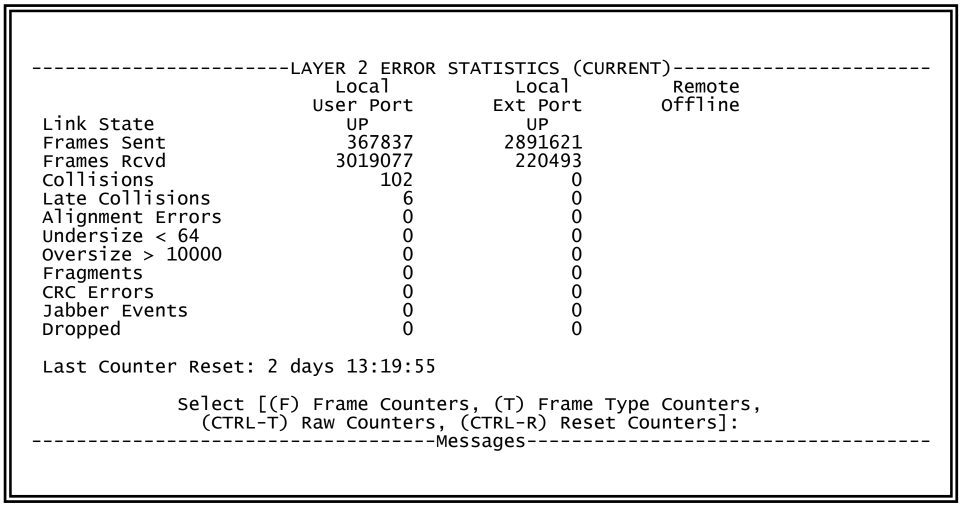
1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [3], "Layer 2 Statistics," and press <Enter>. The Layer 2 Statistics screen appears.



```
--------------------------LAYER 2 STATISTICS (CURRENT)--------------------------
                           Local            Local          Remote
                         User Port        Ext Port        Offline
 Link State                 UP               UP
 Speed/Duplex            100M/HALF     1000M/FULL

 Frames Sent               367668         2890860
 Frames Rcvd              3018236          220450
 Bytes Sent              32829996       337800200
 Bytes Rcvd             346053053        14120070
 Undersize < 64                 0               0
 Oversize > 10000               0               0
 Frames > 1518                  0               0
 Frames > 1522                  0               0

 Last Counter Reset: 2 days 13:19:12

          Select [(C) Change Counter Frame Size, (E) Error Counters,
  (T) Frame Type Counters, (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:

------------------------------------Messages------------------------------------
```

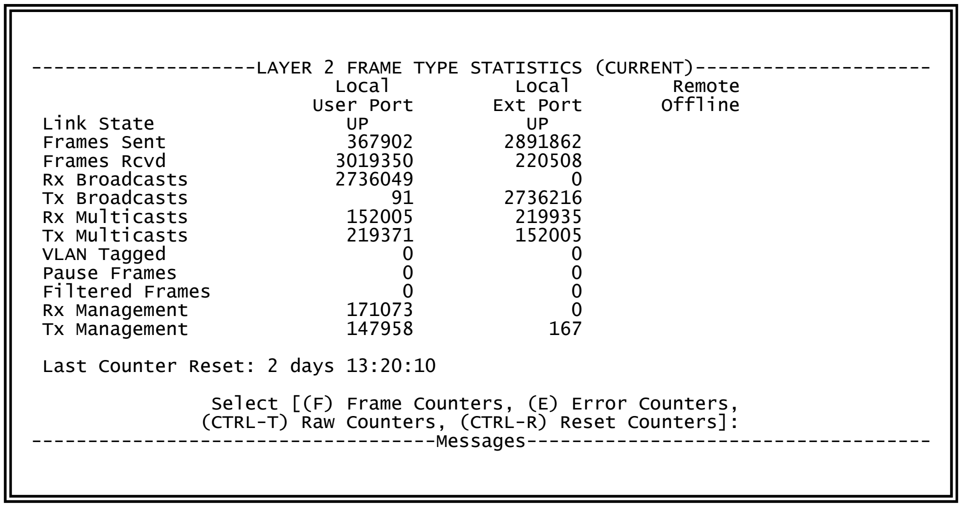
2. The last Frames Counter's (1522 in the example above) size is configurable. Type [C] and press <Enter> to configure this counter. Valid Frame size is from 1 to 10000.

3. To display the Error Statistics screen, type [E]; "Error Counters" and press <Enter>.



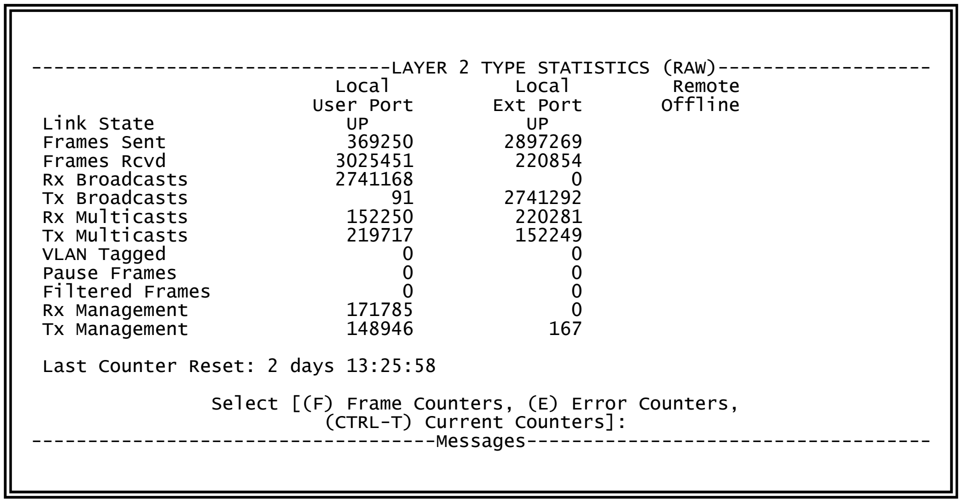
```
-----------------------LAYER 2 ERROR STATISTICS (CURRENT)-----------------------
                           Local            Local          Remote
                         User Port        Ext Port        Offline
 Link State                 UP               UP
 Frames Sent               367837         2891621
 Frames Rcvd              3019077          220493
 Collisions                   102               0
 Late Collisions                6               0
 Alignment Errors               0               0
 Undersize < 64                 0               0
 Oversize > 10000               0               0
 Fragments                      0               0
 CRC Errors                     0               0
 Jabber Events                  0               0
 Dropped                        0               0

 Last Counter Reset: 2 days 13:19:55

             Select [(F) Frame Counters, (T) Frame Type Counters,
               (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:
------------------------------------Messages------------------------------------
```

4. To display the Frame Type Statistics screen, type [T]; "Frame Type Counters" and press <Enter>.



```
--------------------LAYER 2 FRAME TYPE STATISTICS (CURRENT)---------------------
                           Local           Local         Remote
                         User Port       Ext Port       Offline
 Link State                 UP              UP
 Frames Sent                367902        2891862
 Frames Rcvd               3019350         220508
 Rx Broadcasts             2736049              0
 Tx Broadcasts                  91        2736216
 Rx Multicasts              152005         219935
 Tx Multicasts              219371         152005
 VLAN Tagged                     0              0
 Pause Frames                    0              0
 Filtered Frames                 0              0
 Rx Management              171073              0
 Tx Management              147958            167

 Last Counter Reset: 2 days 13:20:10

                Select [(F) Frame Counters, (E) Error Counters,
               (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:
------------------------------------Messages------------------------------------
```

5. To display the Raw Counters screen, type [R]; "Raw Counters" and press <Enter>.



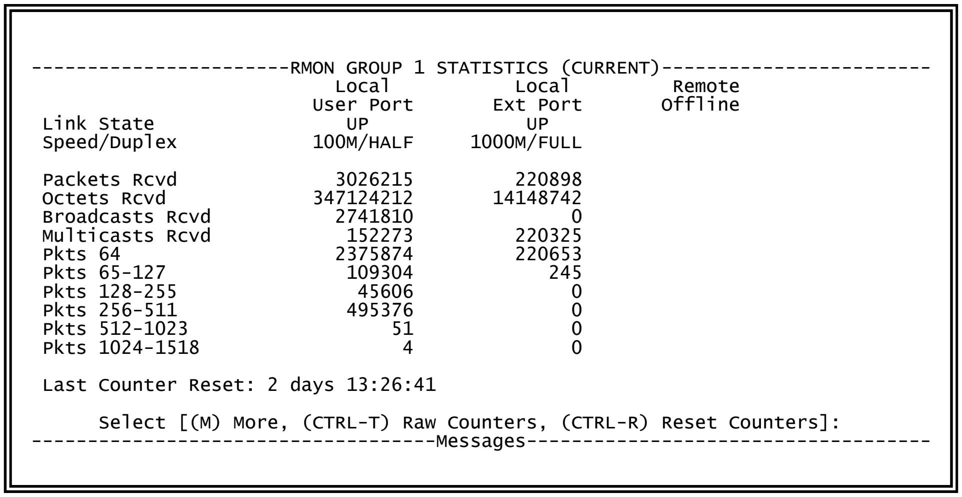
```
--------------------------------LAYER 2 TYPE STATISTICS (RAW)-------------------
                           Local           Local         Remote
                         User Port       Ext Port       Offline
 Link State                 UP              UP
 Frames Sent                369250        2897269
 Frames Rcvd               3025451         220854
 Rx Broadcasts             2741168              0
 Tx Broadcasts                  91        2741292
 Rx Multicasts              152250         220281
 Tx Multicasts              219717         152249
 VLAN Tagged                     0              0
 Pause Frames                    0              0
 Filtered Frames                 0              0
 Rx Management              171785              0
 Tx Management              148946            167

 Last Counter Reset: 2 days 13:25:58

                Select [(F) Frame Counters, (E) Error Counters,
                          (CTRL-T) Current Counters]:
------------------------------------Messages------------------------------------
```

6. To reset the counters, press <Ctrl-R>.

7. When you finish checking the statistics, press <Esc> to return to the Main Menu.

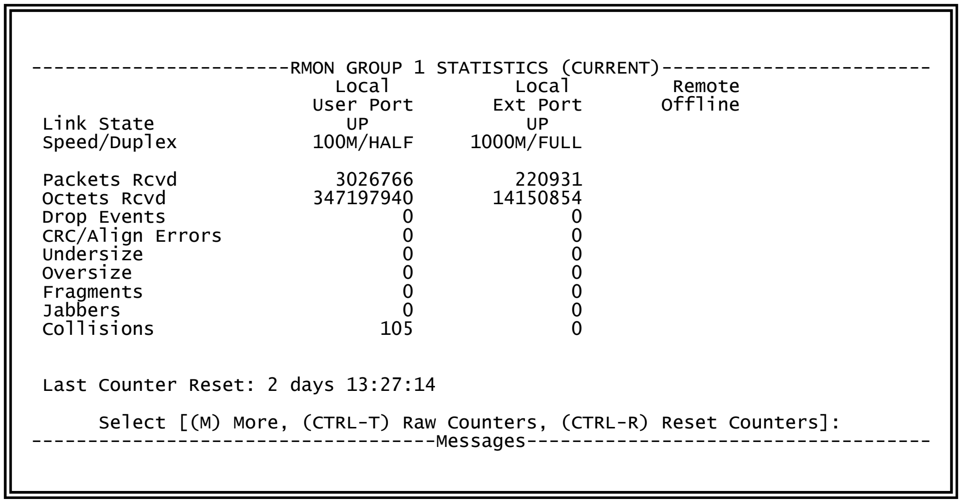
The RMON Group 1 Statistics report shows statistics for data transfers on the N525. To view RMON Group 1 statistics, follow these steps:

1. From the Main Menu type [3], "Port Information," and press <Enter>. At the Port Information Menu, type [4], "RMON Group 1 Statistics," and press <Enter>. The RMON Group 1 Statistics screen displays.



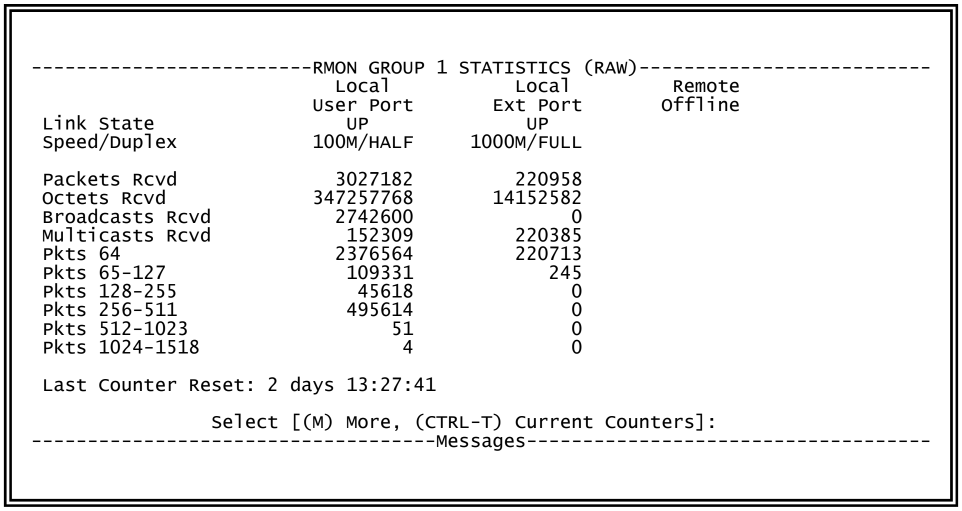
```
-----------------------RMON GROUP 1 STATISTICS (CURRENT)------------------------
                           Local           Local          Remote
                         User Port       Ext Port       Offline
 Link State                 UP              UP
 Speed/Duplex            100M/HALF     1000M/FULL

 Packets Rcvd              3026215         220898
 Octets Rcvd             347124212       14148742
 Broadcasts Rcvd           2741810              0
 Multicasts Rcvd            152273         220325
 Pkts 64                   2375874         220653
 Pkts 65-127                109304            245
 Pkts 128-255                45606              0
 Pkts 256-511               495376              0
 Pkts 512-1023                  51              0
 Pkts 1024-1518                  4              0

 Last Counter Reset: 2 days 13:26:41

      Select [(M) More, (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:
-----------------------------------Messages------------------------------------
```

2. To display additional parameters, press “M”.



```
-----------------------RMON GROUP 1 STATISTICS (CURRENT)------------------------
                           Local           Local          Remote
                         User Port       Ext Port       Offline
 Link State                 UP              UP
 Speed/Duplex            100M/HALF     1000M/FULL

 Packets Rcvd              3026766         220931
 Octets Rcvd             347197940       14150854
 Drop Events                     0              0
 CRC/Align Errors                0              0
 Undersize                       0              0
 Oversize                        0              0
 Fragments                       0              0
 Jabbers                         0              0
 Collisions                    105              0


 Last Counter Reset: 2 days 13:27:14

      Select [(M) More, (CTRL-T) Raw Counters, (CTRL-R) Reset Counters]:
-----------------------------------Messages------------------------------------
```

3. To display the Raw information, press <Ctrl-T>.



```
-------------------------RMON GROUP 1 STATISTICS (RAW)--------------------------
                           Local           Local           Remote
                         User Port       Ext Port       Offline
 Link State                 UP              UP
 Speed/Duplex            100M/HALF     1000M/FULL

 Packets Rcvd              3027182         220958
 Octets Rcvd             347257768       14152582
 Broadcasts Rcvd           2742600              0
 Multicasts Rcvd            152309         220385
 Pkts 64                   2376564         220713
 Pkts 65-127                109331            245
 Pkts 128-255                45618              0
 Pkts 256-511               495614              0
 Pkts 512-1023                  51              0
 Pkts 1024-1518                  4              0

 Last Counter Reset: 2 days 13:27:41

                Select [(M) More, (CTRL-T) Current Counters]:
------------------------------------Messages------------------------------------
```

4. To reset the counters, press <Ctrl-R>.

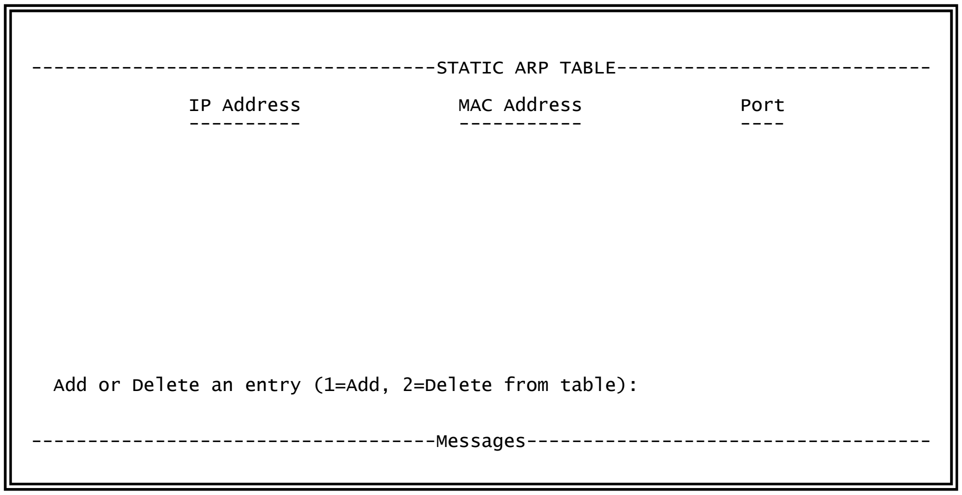
5. When you finish checking the statistics, press <Esc> to return to the Main Menu.

Displaying the Static and Dynamic ARP Tables

The Static ARP Table lets you manually configure or change specific IP and MAC addresses. The Dynamic ARP table displays learned IP and MAC addresses and allows deletion of specific address from the Table. Address are displayed by the N525 port (User for Extension) that the Address is received.

To view, set, or remove a static ARP address, follow these steps:

1. From the Utilities Menu, type [7], "Static ARP Table," and press <Enter>.



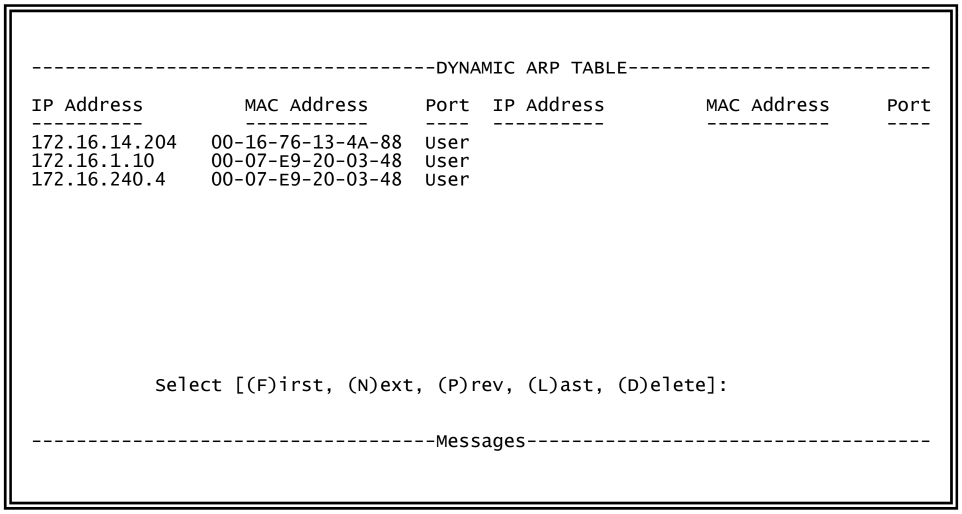
```
------------------------------------STATIC ARP TABLE-----------------------------
              IP Address              MAC Address              Port
              ----------              -----------              ----








  Add or Delete an entry (1=Add, 2=Delete from table):

------------------------------------Messages------------------------------------
```

2. At the prompt, type [1] to add a port, or type [2] to delete a port. Enter the IP Address (xxx.xxx.xxx.xxx), MAC Address (xx-xx-xx-xx-xx-xx.) and the Port (press <space> to select User or Ext).

3. To return to the Main Menu, press <Esc>.

To display the dynamic ARP Table, follow these steps:

1. From the Utilities Menu, type [8], "Dynamic ARP Table," and press <Enter>.



```
-----------------------------------DYNAMIC ARP TABLE--------------------------

IP Address         MAC Address     Port  IP Address         MAC Address     Port
----------         -----------     ----  ----------         -----------     ----
172.16.14.204   00-16-76-13-4A-88  User
172.16.1.10     00-07-E9-20-03-48  User
172.16.240.4    00-07-E9-20-03-48  User









           Select [(F)irst, (N)ext, (P)rev, (L)ast, (D)elete]:

-----------------------------------Messages-----------------------------------
```

2. <F>irst, <N>ext, <P>rev and <L>ast displays various pages of the table when the number of entries exceed 1 or more screen. To Delete an entry in the Table, page until the address appears on the screen, then type [D] and press <Enter>. The first entry on the screen will be highlighted. Press <space> until the address to delete is highlighted and press <Enter>.

3. To return to the Main Menu, press <Esc>.

Chapter 4
Maintenance and Troubleshooting

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.

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

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

Plan to use a cable management system to ensure trouble-free operation and maintenance tasks.

1. 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 greater than 15 times the cable diameter (based on Federal Standard FS-1037C).

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

Check Optical Power Levels

To ensure the proper performance levels, measure the fiber link loss, or link attenuation, for all fiber links. Each N525 is shipped with a document that lists the output power for each laser transmitter. To determine link attenuation, use either the N525 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 N525 turns on automatically when it is powered up.

Measuring 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 N525.
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 N525. 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 N525 Tx output value to determine the power expected at the remote cable end, which is the input power at the remote receiver.

Measuring Receiver Input Power

If you know the link attenuation, skip this section. Otherwise, follow these steps to use the N525 to measure the link attenuation.

1. At the local site, connect the fiber link cable to Tx on the N525.
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 optical receiver. This power level must be within the sensitivity range listed on the data sheet for the optical receiver.
4. Subtract the remote receive power level from the transmitter output power at the local site. The result provides the link loss, in dB.

   Note: *If you cannot determine the Rx sensitivity, contact Canoga Perkins Technical Support Department for assistance.*

Measuring Fiber Link Attenuation

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

Measure optical fiber links at the shortest wavelength of operation to determine the limiting factor in the loss budget. Each device that transmits to a N525 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 N525s.

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 N525 and the local device. (Each fiber connection can generate 0.5 dB of additional loss.)

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

To measure attenuation:

1. Connect the transmit fiber to the local and remote N525s/optical device.

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

Troubleshooting

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

Whenever there is a significant signal loss, first check the fiber path and the minimum bend radius for 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.

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 1 in Chapter 3 lists the front panel LED functions and indications.

Use the System Alarms screen to view alarms and faults on the N525 and its remote partner. To view alarm status, follow these steps:

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.

New Installation

On new installations, make sure that all steps in Chapter 2 are complete, and then follow these steps:

1. Check that the STA LED is green.

2. Check that the fiber type (multimode or single mode) matches the N525 Optical Interface. A listing of the N525's Interface modules and their media types (UTP, Single Mode, Multimode) is in Chapter 5.

3. Make these checks:
    a. All fiber cabling is of the same type; do not mix multimode and single mode cables.
    b. The fiber optic cable is within the specifications and loss budget of the optic interface module.
    c. The line length between the N525 and the remote link does not exceed the allowable loss budget or overdrive limit.
    d. All host modules in the link are turned on.
    e. All fiber cables are connected Tx to Rx and Rx to Tx.

Fiber Optics Problems

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

Configuration Problems

If a configuration error appears and you have difficulty isolating the fault, you can reset all configurable settings to default except for the time and date, password, BOOTP setting, and TELNET timeout. Then restart your configuration process. To reset the N525's configuration to default, follow these steps:

1. At the Main Menu, type [6], "Utilities," and press <Enter>.`

2. At the Utilities Menu, type [2], "Reset Configuration To Default," and press <Enter> follow the prompts on the screen.

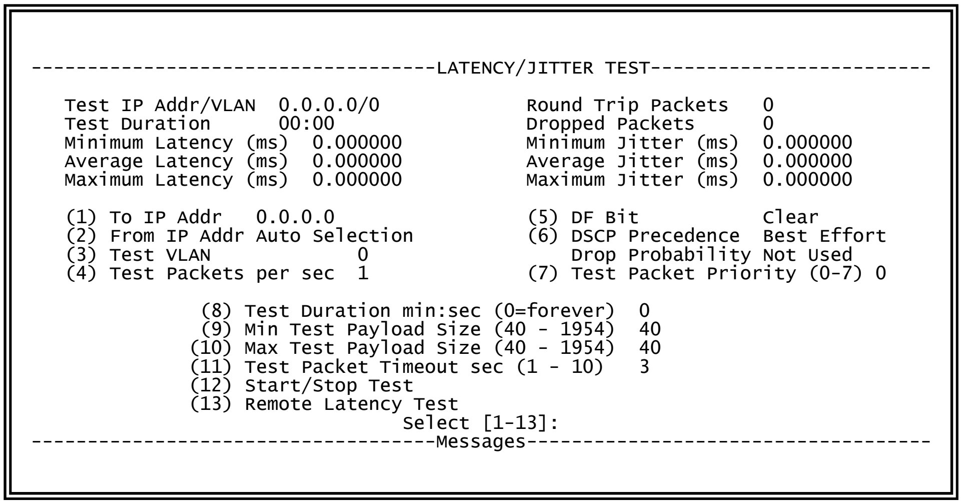
3. To return to the Main Menu, press <Esc>.

Running Diagnostics

When you set up a new connection, you can verify the link connectivity using Ping prior to sending data. The Latency and Jitter Test verifies quality of the link.

Latency and Jitter Testing

Latency/Jitter Testing measures and reports performance and quality of the link between N525s. Results reported include the numbers of packets that completed a round trip or were lost and the minimums, average, and maximums for latency and jitter. To initiate Latency and Jitter Testing, follow these steps:



```
-----------------------------------LATENCY/JITTER TEST-------------------------

   Test IP Addr/VLAN  0.0.0.0/0              Round Trip Packets   0
   Test Duration      00:00                  Dropped Packets      0
   Minimum Latency (ms)  0.000000            Minimum Jitter (ms)  0.000000
   Average Latency (ms)  0.000000            Average Jitter (ms)  0.000000
   Maximum Latency (ms)  0.000000            Maximum Jitter (ms)  0.000000

   (1) To IP Addr   0.0.0.0                  (5) DF Bit           Clear
   (2) From IP Addr Auto Selection           (6) DSCP Precedence  Best Effort
   (3) Test VLAN             0                   Drop Probability Not Used
   (4) Test Packets per sec  1               (7) Test Packet Priority (0-7) 0

               (8) Test Duration min:sec (0=forever)  0
               (9) Min Test Payload Size (40 - 1954)  40
              (10) Max Test Payload Size (40 - 1954)  40
              (11) Test Packet Timeout sec (1 - 10)   3
              (12) Start/Stop Test
              (13) Remote Latency Test
                                Select [1-13]:
-----------------------------------Messages------------------------------------
```

1. From the Diagnostics Menu, type [2], "Latency/Jitter Test," and press <Enter>. The Latency/Jitter Test screen appears.

2. Type the number for parameter you want to change. Type the value to set, and press <Enter>. Test IP Address/VLAN: Where the N525 sends the packets

    a. **To IP Addr**
    Sets remote N525's IP address

    b. **From IP Addr**
    Sets if the local N525's management or alternate IP is to be used. Mgmt, Alternate or Automatic

    c. **Test VLAN**
    VLAN Tag number of the VLAN to test

    d. **Test Packets per sec**
    The number of test packets to send each second

e. **DF Bit**
Sets if the network can fragment Test Packets. Set allows fragmentation, Clear does not allow fragmentation

f. **DSCP Precedent**
Sets IP Packet priority. Options are: Best Effort, Class 1, Class 2, Class 3, Class 4, Internet Control, Network Control, Not Used. Pressing <space> cycles through the options. Press <Enter> to select option.
Drop Probability
Sets IP packet Discard Priority. Options are Low, Medium, High, not used

g. **Test Packet Priority**
Sets VLAN frame priority. 0 to 7

h. **Test Duration min:sec**
Test duration in minutes and seconds, 0 for a continuous test

i. **Min Test Packet Size**
Sets minimum packet size. 40 to 1472 bytes

j. **Max Test Packet Size**
Sets maximum packet size. Must be equal to or greater than the Minimum Packet Size. The N525 increments packet size from the minimum to the maximum when the next packet is sent during a test. When the maximum size has been sent, the size is reset to the minimum size and the incrementing continues. Maximum packet size is from 40 to 1472 bytes.

k. **Test Packet Timeout**
How long to wait for a test packet to return

l. **Start/Stop Test**
Starts the test or stops the test prior to automatic completion or when in Continuous (Duration setting of 0).

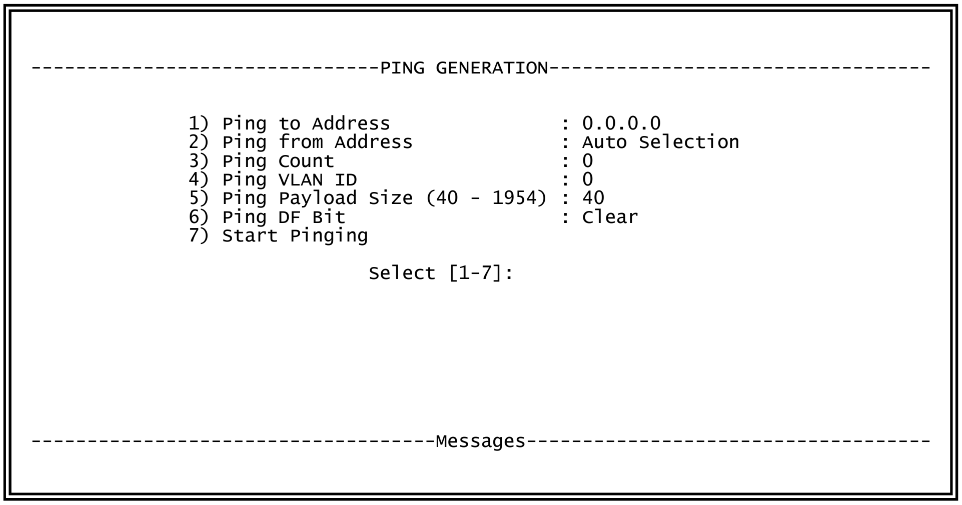
m. **Remote Latency Test**
Initiates and configures Latency and Jitter testing on a Remote N525 when SBMC is enables.

3. When the Latency/Jitter test is finished running, press <Esc> to return to the Diagnostics Menu.

Ping Testing

To verify network connectivity with another IP device such as another N525, an Ethernet Switch, or a user host, you can use the N525 to send a Ping to the IP address for that device. Use the Ping Generation screen to send the Ping. To set up and send a Ping, follow these steps:

1. From the Diagnostics Menu, type [3], "PING Generation," and press <Enter>
   OR From the Utilities Menu, type [6], "PING Generation," and press <Enter>



```
-------------------------------PING GENERATION----------------------------------

              1) Ping to Address              : 0.0.0.0
              2) Ping from Address            : Auto Selection
              3) Ping Count                   : 0
              4) Ping VLAN ID                 : 0
              5) Ping Payload Size (40 - 1954) : 40
              6) Ping DF Bit                  : Clear
              7) Start Pinging

                              Select [1-7]:






------------------------------------Messages------------------------------------
```

2. Configure the N525 Ping test from the Ping Menu.

   a. **Ping to Address**
   Destination IP Address

   b. **Ping from Address**
   IP address of Local N525. Selections are Management, Alternate, Auto Selection

   c. **Ping Count**
   Number of Ping packets to send. 0 send a continuous test (press <esc> to terminate test)

   d. **Ping VLAN ID**
   VLAN Tag ID for Ping packets

   e. **Ping Payload Size <40 – 1954>**
   Length, in bytes, of the Ping packet payload. 40 to 1954 bytes.

   f. **Ping DF Bit**
   Determines if the network can fragment the Ping packet. Set allows fragmentation, Clear does not.

3. To start the Ping test, type [7]. The N525 waits to send the next Ping until after the current Ping is received or times out. The N525 displays results for each Ping which includes the destination IP address, Sequence Number, round trip time (in milliseconds) and the Time to Live (TTL).

A good connection appears similar to this with all requests returned:

```
Pinging 216.109.112.135 with 64 bytes.
    Reply from 216.109.112.135 Seq #0 time = 63.496 ms TTL=47
    . . .
    Reply from 216.109.112.135 Seq #5 time = 63.120 ms TTL=48
    6 packets transmitted, 6 packets received, %0.000 packet loss
    round-trip min/avg/max = 63.120/65.862/75.810 ms
    Press any key to continue.
```

A faulty connection can appear similar to this with one or more requests timed out:

```
Reply from 216.109.112.135 Seq #4 time <70 ms TTL=47
Request timed out
Request timed out
Reply from 216.109.112.135 Seq #12 time <70 ms TTL=47
Reply from 216.109.112.135 Seq #13 time <70 ms TTL=48
14 packets transmitted, 10 packets received, %28.571 packet loss
round-trip min/avg/max < 70.000/71.000/80.000 ms
Press any key to continue.
```

4. To terminate the Ping test, press <Esc>.

Loopback Diagnostics

Use Loopbacks to diagnose a fault on the optical link. The N525 supports four loopback modes that you can set at the local site for both the Local and Remote N525s. These modes loop the data through either the physical layer (PHY) on the User side or the FPGA when looping to the remote user link, or the FPGA when looping to the local user link.

- **Local-Local Mode**
  Local-Local Mode loops data received on the local User port Rx through the FPGA to the User port Tx. Data is not sent out the Extension port Tx and incoming data on the Extension port Rx is ignored. See Figure 22. To set this mode, set the Loopback State for the Local Module to Local.

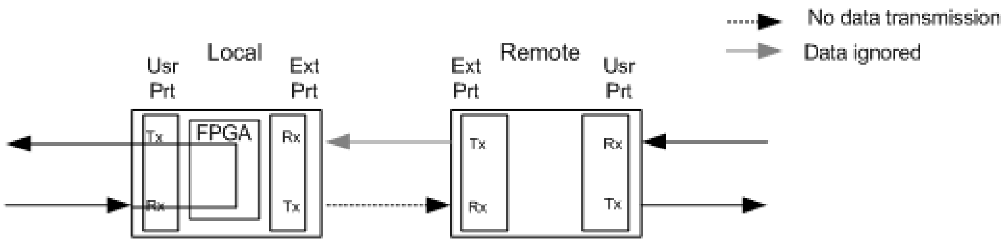


Figure 24 - Local-Local Loopback Mode

- **Local-Remote Mode**
  Local-Remote Mode loops data received on the Extension port Rx through the User side PHY to the Extension port Tx. Data is not sent out the remote User port Tx and incoming data on the remote User port Rx is ignored. See Figure 23. To set this mode, set the Loopback State for the Local Module to Remote.

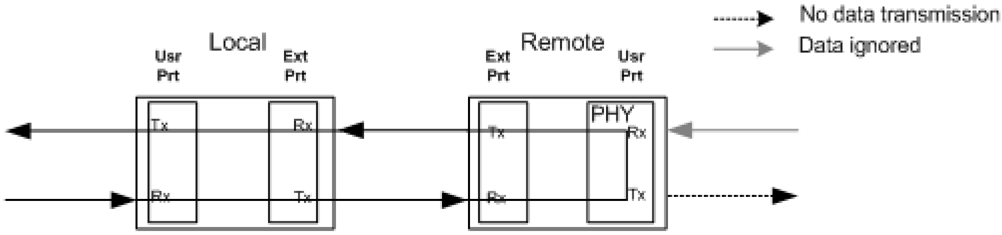


Figure 25 - Local-Remote Loopback Mode

- **Remote-Local Mode**
  Remote-Local Mode loops data received on the User port Rx through the FPGA to the User port Tx. Data is not sent out the remote Extension port Tx and incoming data on the remote Extension port Rx is ignored. See Figure 24. To set this mode, set the Loopback State for the Remote module to Local.

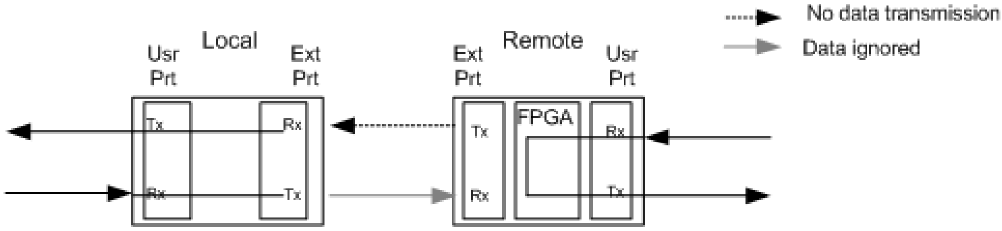


Figure 26 - Remote-Local Loopback Mode

- **Remote-Remote Mode**
  Remote-Remote Mode loops data received on the Extension port Rx through the Local User PHY to the Extension port Tx. Data is not sent out the local User port Tx and incoming data on the local User port Rx is ignored. See Figure 25. To set this mode, set the Loopback State for the Remote module to Remote.

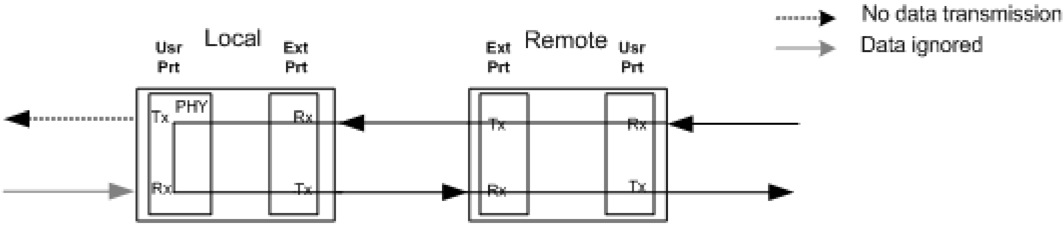


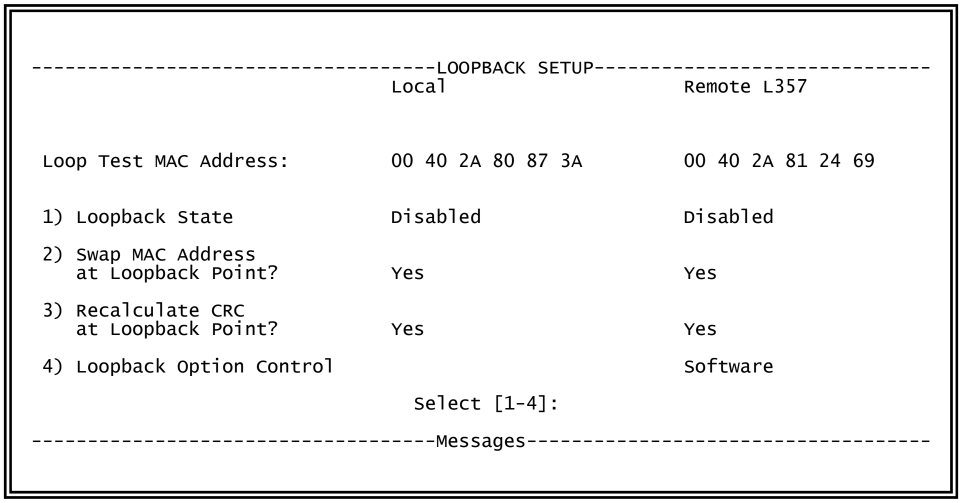
Figure 27 - Remote-Remote Loopback Mode

For loopbacks, the N525 uses a unique MAC address, the Loop Test MAC Address, which is displayed on the Loopback Setup screen. For details about using the software and accessing the Loopback Setup screen, see Chapter 4. When in loopback mode, the N525 filters the incoming packets to identify test packets identified by the MAC address.

The N525 is configurable to swap the origination and destination MAC Addresses and to Recalculate the looped frame's CRC. Test packets are returned to the source according to the selected options.

Use the Loopback Setup Menu to display current loopback status, initiate loopbacks, and configure Address Swapping and CRC Recalculation options. To run a loopback test, follow these steps:

1. At the Diagnostics Menu, type [1], "Loopback Setup," and press <Enter>. The Loopback Setup Menu appears. When the N525 is connected to a remote N525 and SBMC is enabled, the remote N525's loopback functions are controlled from the local N525.



```
------------------------------------LOOPBACK SETUP------------------------------
                                Local                     Remote L357


 Loop Test MAC Address:         00 40 2A 80 87 3A         00 40 2A 81 24 69

 1) Loopback State              Disabled                  Disabled

 2) Swap MAC Address
    at Loopback Point?          Yes                       Yes

 3) Recalculate CRC
    at Loopback Point?          Yes                       Yes

 4) Loopback Option Control                               Software
                                  Select [1-4]:

------------------------------------Messages------------------------------------
```

2. Type the number for the loopback you want to set, press <Tab> to highlight the Remote column if needed, pressing <Space> cycles through the options, then press <Enter>.

   a. **Loopback State**
   Sets Loopback Test to Disabled (off), Local, Remote, or Clear All Loopbacks

   b. **Swap MAC Address at Loopback Point?**
   Sets if the origination and destination MAC addresses are to be swapped. Yes swaps the addresses, No does not.

   c. **Recalculate CRC at Loopback Point?**
   Sets if the N525 is to recalculate the CRC when MAC addresses are swapped. Yes recalculates the CRC, No does not.

3. When you finish running Loopback, press <Esc> to return to the Diagnostics screen.

Connectivity Loss Detection

The Connectivity Loss Detection (CLD) feature enables you to detect loss of connectivity to a remote N525 in a point-to-point circuit, and to detect undesired link performance. In conjunction with CLD you can use Connection Loss Forwarding (CLF), which will shut down the User port if there is a loss of connectivity to the remote N525. CLD and CLF are disabled by default.

Note: Before enabling Connection Loss Forwarding, you should disable Link Loss Forwarding.

Note: You should configure the settings for CLD before enabling CLD.

Note: You can use CLD to detect loss of connectivity in point-to-point circuits only. Multipoint CLD is not supported.

When you enable CLD, the N525 sends Ping packets continuously to the remote N525. Loss of connectivity is determined based on a certain number of consecutive lost pings. Recovery of connectivity is determined based on a number of consecutive successful pings. Link performance is determined by round trip time (RTT) of the pings. All of these factors are configurable.

The N525 uses hardware timestamps in the Ping packets in order to measure RTT. The hardware timestamps are inserted into the Ping packets by both the local and remote N525. This allows the local N525 to exclude ICMP packet processing time when calculating RTT, which makes for highly accurate measurements.

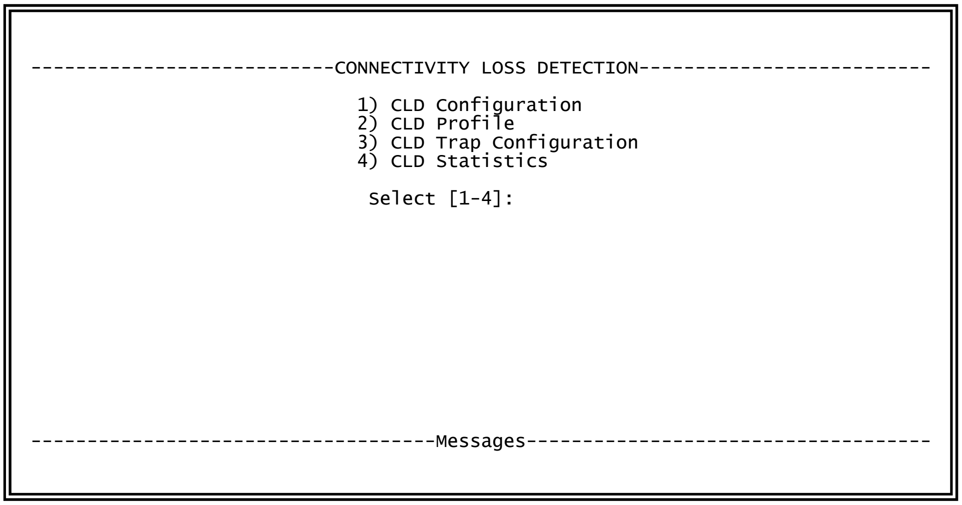
You enable CLD on each N525 individually. Typically two N525s are configured to use CLD on the link between them. Each N525 pings the Extension port of the other N525. However, if one N525 does not have CLD enabled, that N525 will still respond to the CLD pings from the other N525.

There are SNMP traps for CLD and CLF events.

Configuring CLD

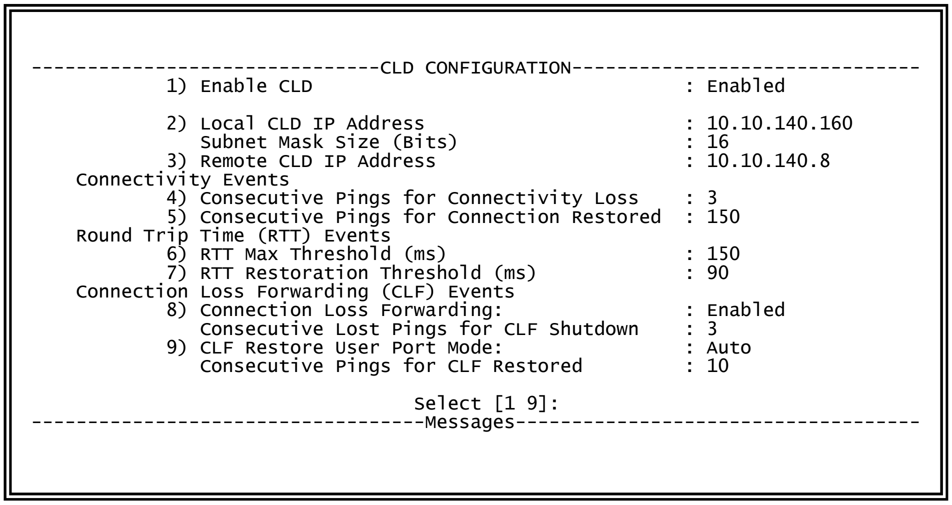
To set up CLD, follow these steps:

1. On the Diagnostics screen, type the number for "Remote Connectivity Loss Detection" and press <Enter>. The Connectivity Loss Detection screen appears. There are four submenus.



```
---------------------------CONNECTIVITY LOSS DETECTION--------------------------

                             1) CLD Configuration
                             2) CLD Profile
                             3) CLD Trap Configuration
                             4) CLD Statistics

                              Select [1-4]:









-----------------------------------Messages------------------------------------
```

2. Type 1 for "CLD Configuration" and press <Enter>. The CLD Configuration screen appears.



```
------------------------------CLD CONFIGURATION-------------------------------
            1) Enable CLD                                : Enabled

            2) Local CLD IP Address                      : 10.10.140.160
               Subnet Mask Size (Bits)                   : 16
            3) Remote CLD IP Address                     : 10.10.140.8
    Connectivity Events
            4) Consecutive Pings for Connectivity Loss   : 3
            5) Consecutive Pings for Connection Restored : 150
    Round Trip Time (RTT) Events
            6) RTT Max Threshold (ms)                    : 150
            7) RTT Restoration Threshold (ms)            : 90
    Connection Loss Forwarding (CLF) Events
            8) Connection Loss Forwarding:               : Enabled
               Consecutive Lost Pings for CLF Shutdown   : 3
            9) CLF Restore User Port Mode:               : Auto
               Consecutive Pings for CLF Restored        : 10

                                  Select [1 9]:
-----------------------------------Messages------------------------------------
```

Note: All event pairs are reported alternately. Event pair example: RTT Max Threshold/RTT Restoration Threshold.

a. **Enable CLD**
   Enable or disable CLD on this N525.

b. **Local CLD IP Address**
The IP address of this N525.
Subnet Mask Size (Bits)
The subnet mask size for the IP address.

c. **Remote CLD IP Address**
The IP address of the remote N525.

Connectivity Events

a. **Consecutive Pings for Connectivity Loss**
The number of consecutive unreachable or timed-out pings needed to declare that connectivity is lost.

b. **Consecutive Pings for Connection Restored**
The number of reachable pings needed to declare that connectivity is restored.

Round Trip Time (RTT) Events

a. **RTT Max Threshold (ms)**
The maximum round trip time in milliseconds. This defines the threshold for undesired link performance.

b. **RTT Restoration Threshold (ms)**
When the round trip time reaches this millisecond value, link performance is declared restored. An RTT Max Threshold event must have occurred previous to this. This value must be less than the value of RTT Max Threshold.

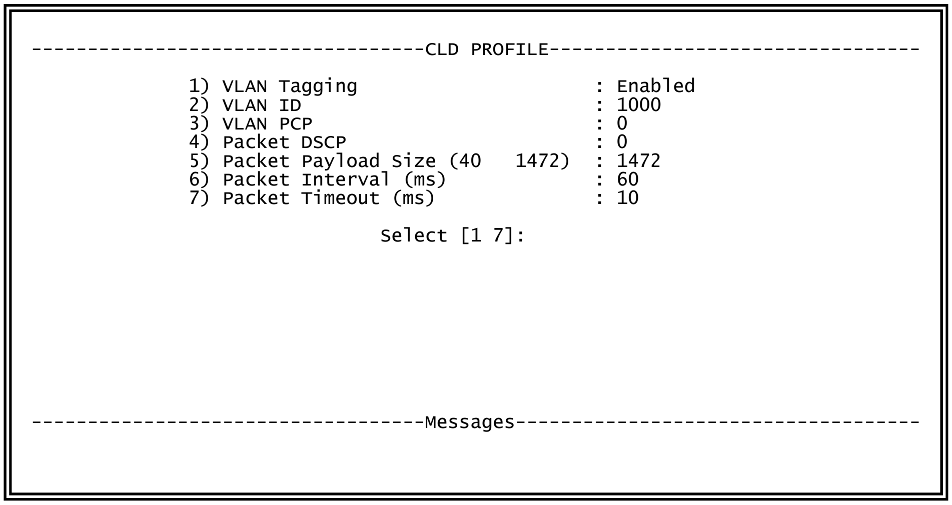
Connection Loss Forwarding (CLF) Events

a. **Connection Loss Forwarding**
Enable or disable Connection Loss Forwarding.
Consecutive Lost Pings for CLF Shutdown
The number of consecutive unreachable or timed-out pings needed to initiate a shutdown of the User port.

b. **CLF Restore User Port Mode**
How to handle CLF when the N525 connectivity is restored. If you set this to Auto, it means that CLF will be deactivated (User Port enabled) after receiving consecutive pings as configured in the **Consecutive Pings for CLF Restored** setting. Manual means that the consecutive pings setting is ignored and a Manual User Port Restore must be performed from the CLD Statistics screen. Note that the User port is automatically restored after a reset, but if CLF is enabled and consecutive lost pings are achieved again, the User port will be shut down again.
Consecutive Pings for CLF Restored
The number of reachable pings needed before the User port is enabled.

3. Press <Esc> to return to the Connectivity Loss Detection screen.

4. Type 2 for "CLD Profile" and press <Enter>. The CLD Profile screen appears.



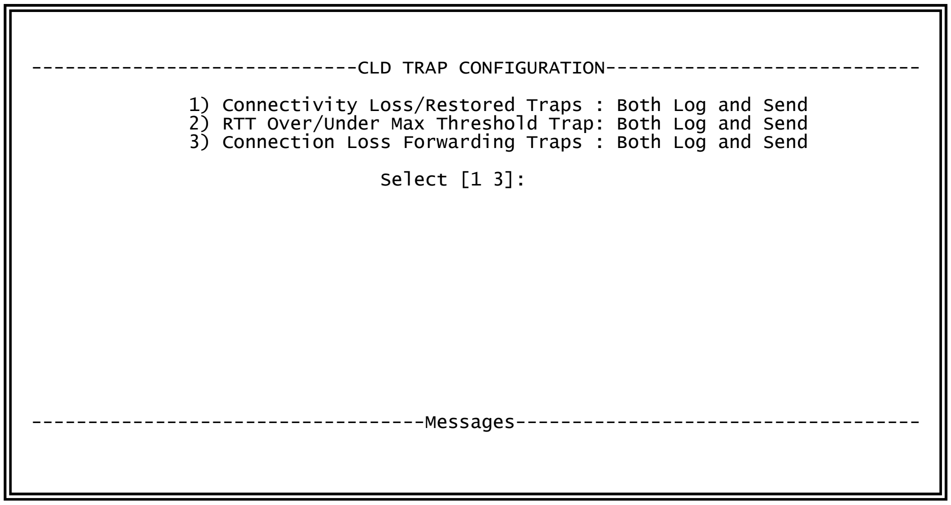
```
-----------------------------------CLD PROFILE---------------------------------

             1) VLAN Tagging                    : Enabled
             2) VLAN ID                         : 1000
             3) VLAN PCP                        : 0
             4) Packet DSCP                     : 0
             5) Packet Payload Size (40   1472) : 1472
             6) Packet Interval (ms)            : 60
             7) Packet Timeout (ms)             : 10

                              Select [1 7]:










-----------------------------------Messages------------------------------------
```

This screen has VLAN and Ping parameters.

a. **VLAN Tagging**
   Enable or disable VLAN tagging of the Ping packets used for CLD.
b. **VLAN ID**
   VLAN ID to use if VLAN tagging is enabled. 1 – 4094.
c. **VLAN PCP**
   VLAN Priority Code Point (frame priority level). 0 – 7.
d. **Packet DSCP**
   Value of the DiffServ Differentiated Services Code Point, if needed. 0 – 63.
e. **Packet Payload Size (40 - 1472)**
   Payload size of the Ping packets used for CLD.
f. **Packet Interval (ms)**
   Interval in milliseconds between each Ping packet.
g. **Packet Timeout (ms)**
   Number of milliseconds to wait before timing out a Ping packet.

5. Press <Esc> to return to the Connectivity Loss Detection screen.

6. Type 3 for "CLD Trap Configuration" and press <Enter>. The CLD Trap Configuration screen appears.



```
-----------------------------CLD TRAP CONFIGURATION----------------------------

              1) Connectivity Loss/Restored Traps : Both Log and Send
              2) RTT Over/Under Max Threshold Trap: Both Log and Send
              3) Connection Loss Forwarding Traps : Both Log and Send

                               Select [1 3]:









-----------------------------------Messages------------------------------------
```

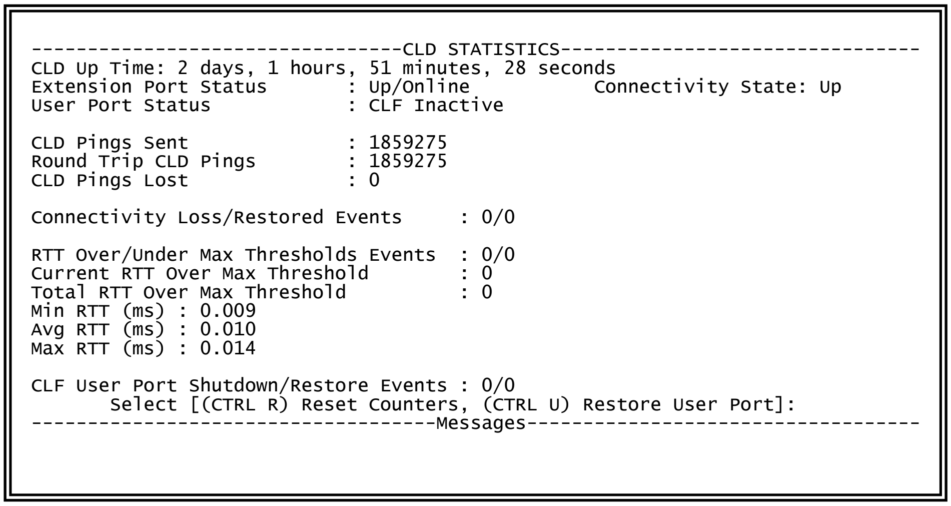
This screen is for configuring SNMP traps related to CLD. Each set of traps has these options: Both Log and Send, Log Only, Send Only, and Disabled.

a. **Connectivity Loss/Restored Traps**
   Two traps, one for loss of connectivity and one for restored connectivity.
b. **RTT Over/Under Max Threshold Trap**
   Two traps, one for undesired link performance and for restored performance.
c. **Connection Loss Forwarding Traps**
   Two traps, one for shutdown of the User port and one for enabling the User port.

CLD Statistics

To display the CLD Statistics, follow these steps:

1. On the Connectivity Loss Detection screen, type 4 for "CLD Statistics" and press <Enter>. The CLD Statistics screen appears.



```
---------------------------------CLD STATISTICS--------------------------------
CLD Up Time: 2 days, 1 hours, 51 minutes, 28 seconds
Extension Port Status       : Up/Online          Connectivity State: Up
User Port Status            : CLF Inactive

CLD Pings Sent              : 1859275
Round Trip CLD Pings        : 1859275
CLD Pings Lost              : 0

Connectivity Loss/Restored Events     : 0/0

RTT Over/Under Max Thresholds Events  : 0/0
Current RTT Over Max Threshold        : 0
Total RTT Over Max Threshold          : 0
Min RTT (ms) : 0.009
Avg RTT (ms) : 0.010
Max RTT (ms) : 0.014

CLF User Port Shutdown/Restore Events : 0/0
       Select [(CTRL R) Reset Counters, (CTRL U) Restore User Port]:
-----------------------------------Messages------------------------------------
```

a. **CLD Up Time**
The amount of time that CLD has been enabled.

b. **Extension Port Status**
Current status of the Extension port. Possible values are Up/Online, Up/Offline, Down/Offline.

c. **User Port Status**
Current status of the User port. Possible values are CLF Inactive and CLF Active.

d. **Connectivity State**
Current state of the connection between the N525s. Possible values are Up and Down.

e. **CLD Pings Sent**
The total number of CLD pings sent.

f. **Round Trip CLD Pings**
The number of CLD pings that were responded to.

g. **CLD Pings Lost**
The number of CLD pings that were not responded to.

h. **Connectivity Loss/Restored Events**
The number of Connectivity Loss and Connectivity Restored events that have occurred. Example: This will read 2/1 if there have been 2 Connectivity Loss events and 1 Connectivity Restored event.

i. **RTT Over/Under Max Thresholds Events**
The number of times the round trip time exceeded the value set for RTT Max Threshold, and the number of times after this that the RTT dropped below the value of RTT Restoration Threshold.

j. **Current RTT Over Max Threshold**
The total number of CLD pings whose RTT exceeded the threshold while the over threshold alarm is active. This is cleared when the RTT goes back to normal.

k. **Total RTT Over Max Threshold**
The total number of CLD pings whose RTT exceeded the threshold.

l. **Min RTT (ms)**
The shortest RTT seen.

m. **Avg RTT (ms)**
The average RTT.

n. **Max RTT (ms)**
The maximum RTT seen.

o. **CLF User Port Shutdown/Restore Events**
The number of times the User port was shut down due to a CLF shutdown event, and the number of times the User port was restored after a shutdown.

The counters on this screen roll over to zero after 4294967295.

2. To reset the counters, press <Ctrl-R>. To manually restore the User port from the CLF state, press <Ctrl-U>.

3. When you finish checking the statistics, press <Esc> to return to the Connectivity Loss Detection screen.

Chapter 5
Specifications

N525 Specifications

Standards:	IEEE 802.3
Dimensions:	1.72" H x 12" W x 11.75" D (44 x 341 x 298 mm)
Weight:	5.5 lb (2.5 Kg)
Operating Temperature:	0° to 50° C
Operating Humidity:	Up to 90% (non-condensing)
Power:	100 VAC to 240 VAC (auto-ranging), ~0.15 A, 50 to 60 Hz -36 VDC to -72 VDC, 0.6A

Regulatory Compliance

- ETL, cETL & LVD (UL 60950 CAN/CSA C22.2 No. 60950, EN/IEC 60950)
- EMC Directive (EN55022 Class A, EN 55024, EN 61000-3-2/-3-3)
- EN 300-386
- CE Mark
- FCC Part 15B Class A (U.S.)/ICES-003 (CAN)
- VCCI Class A (Japan)
- C-Tick (AS/NZS 3548 - Australia)
- CDRH CFR21/IEC 60825-1 (Laser Safety)
- NEBS Level 3 Certified & Tested

EIA RS-232 Port

The RS-232 presents a DCE Interface for terminal support.

Table 4 – EIA-232 Pinout

Pin Number	Signal Name	I/O
1	DCD	Output – Held High
2	RXD	Output
3	TXD	Input
4	DTR	No Connection
5	Signal GND	
6	DSR	Output – Held High
7	CTS	Input
8	RTS	Output

Pin Number	Signal Name	I/O
9	RI	Not Used, connected to GND

N525 Models and Interface Modules

Table 5 – N525 Models

Model	Description	Transmit Power	Receive Sensitivity	Overdrive
N525-4	2 Port NID Base Unit w/AC Power			
N525-5	2 Port NID Base Unit w/DC Power			
10/100/1000 Mbps UTP Interface				
9400-330	10/100/1000 BaseTx UTP			
10 Mbps Optical Interfaces				
9400-431	10BaseFL 850 nm MM 15 dB ST	-15.0, ±1.0 dBm	-33.5 dBm	≥ -14 dBm
9400-631	10BaseXD 1310 nm SM Laser 20 dB ST	Lo: -15.0, ±2.0 dBm Hi: -8.0, ±2.0 dBm	-34 dBm	≥ -8 dBm
9400-634	10BaseSD 1310 nm SM Laser 10 dB ST	-15.0, ±2.0 dBm	-34 dBm	≥ -8 dBm
9400-637	10BaseLD 1310 nm SM Laser 25 dB ST	Lo: -15.0, ±1.0 dBm Hi: -2.0, ±2.0 dBm	-34 dBm	≥ -8 dBm
9400-737	10BaseEX 1550 nm SM Laser 26 dB ST	Lo: -15.0, ±2.0 dBm Hi: -5.0, ±3.0 dBm	-34 dBm	≥ -8 dBm
100 Mbps Optical Interfaces				
9400-442	100BaseMX 1310 nm MM 11 dB SC	-20.0 to -14.0 dBm	-31 dBm	-14 dBm
9400-642	100BaseSD 1310 nm SM 10 dB SC	-20.0 to -8.0 dBm	-31 dBm	-3 dBm
9400-648	100BaseLD 1310 nm SM 26 dB SC	-5.0 to 0.0 dBm	-31 dBm	-3 dBm
9400-748	100BaseEX 1550 nm SM 26 dB SC	-2.0 to -2.0 dBm	-31 dBm	-3 dBm
100 Mbps CWDM Optical Interfaces				
9400-170	100 Mbps 1470 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-171	100 Mbps 1490 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-172	100 Mbps 1510 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-173	100 Mbps 1530 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-174	100 Mbps 1550 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-175	100 Mbps 1570 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm

Model	Description	Transmit Power	Receive Sensitivity	Overdrive
9400-176	100 Mbps 1590 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm
9400-177	100 Mbps 1610 nm SM 22 dB SC	-3.0 to +2.0 dBm	-26 dBm	-3 dBm

Note: All 100 Mbps CWDM wavelength tolerances: +4 to -3.5 nm

100 Mbps BIDI Interfaces

9400-154	Single Fiber SC 100 Mbps 1310 nm SM 20 Km	-15.0 to -7.0 dBm	-31 dBm	-3 dBm
9400-164	Single Fiber SC 100 Mbps 1550 nm SM 20 Km	-15.0 to -7.0 dBm	-31 dBm	-3 dBm
9400-184	Single Fiber SC 100 Mbps 1310 nm SM 40 Km	-8.0 to 0.0 dBm	-31 dBm	-3 dBm
9400-194	Single Fiber SC 100 Mbps 1550 nm SM 40 Km	-8.0 to 0.0 dBm	-31 dBm	-3 dBm

1000 Mbps Optical Interfaces

9400-627	1000BaseSX 850 nm MM 6 dB SC	-10.0 to -4.0 dBm	-17 dBm	-3 dBm
9400-528	1000BaseLX 1310 nm SM 7 dB SC	-11.0 to -3.0 dBm	-20 dBm	-3 dBm
9400-529	1000BaseLD 1310 nm SM 14 dB SC	-5.0 to 0.0 dBm	-20 dBm	-3 dBm
9400-628	1000BaseXD 1310 nm SM 21 dB SC	0.0 to +2.0 dBm	-21 dBm	-3 dBm
9400-728	1000BaseEX 1550 nm SM 21 dB SC	-2.0 to +1.0 dBm	-23 dBm	-3 dBm
9400-928	1000BaseEX 1550 nm SM 23 dB SC	0.0 to +2.0 dBm	-23 dBm	-3 dBm

1000 Mbps CWDM Optical Interfaces

9400-270	1000 Mbps 1470 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-271	1000 Mbps 1490 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-272	1000 Mbps 1510 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-273	1000 Mbps 1530 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-274	1000 Mbps 1550 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-275	1000 Mbps 1570 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-276	1000 Mbps 1590 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-277	1000 Mbps 1610 nm SM 22 dB SC	-3.0 to +2.0 dBm	-23 dBm	-3 dBm

Note: All 1000 Mbps CWDM wavelength tolerances: +4 to -3.5 nm

1000 Mbps BIDI Interfaces

9400-254	Single Fiber SC 1000Mbps 1310nm SM 20Km	-8.0 to -3.0 dBm	-21 dBm	-3 dBm
9400-264	Single Fiber SC 1000Mbps 1550nm SM 20Km	-8.0 to -3.0 dBm	-21 dBm	-3 dBm
9400-284	Single Fiber SC 1000Mbps 1310nm SM 40Km	-3.0 to +2.0 dBm	-23 dBm	-3 dBm
9400-294	Single Fiber SC 1000Mbps 1550nm SM 40Km	-3.0 to +2.0 dBm	-23 dBm	-3 dBm

Appendix A
Warranty Information

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

Appendix B
Acronym and Abbreviation List

DF	Do Not Fragment
CLD	Connectivity Loss Detection
FPGA	Field Programmable Gate Array
LLF	Link Loss Forwarding
LNK	Link
Mbps	Megabits per second
MDM	Modem
MMF	Multimode Fiber
NID	Network Interface Device
NPA	Network Performance Assurance
OAM	Operations And Maintenance
OADPDU	OAM Protocol Data Unit
PHY	Physical Layer
RMTF	Remote Fault
RTT	Round Trip Time
Rx	Receive signal
SBMC	SideBand Management Channel
SM	Single Mode
SMF	Single Mode Fiber
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TFTP	Trivial File Transfer Protocol
TRM	Terminal
Tx	Transmit signal

Appendix C
Configuration File Format and Fields

```
### WARNING - DO NOT MODIFY THIS HEADER ###
CfgFileBuiltWithFirmware = V05.00
CfgFileBuildDateAndTime = 02-MAR-2006 22:22:23
CfgFileUserComments =Canoga Perkins, Chatsworth, CA site.
#############################################
## The following must be modified to = "Yes" if the specified items
## are to be configured, otherwise the config items will be ignored.
ConfigureIPAddress = No
ConfigureSBMC = No
ConfigureInterface = No
#############################################
SystemName = Master ETSU
SystemLocation = 20600 Prairie St.
SystemContact = NOC
IPAddress = 172.16.85.44
SubnetMask = 255.255.0.0
DefaultGateway = 172.16.1.1
SlipIPAddress = 0.0.0.0
BootpEnabled = Disable
ReadCommunity = public
WriteCommunity = public
SNMPAuthTraps = Flag Error 2

[-HostEntry-]
## ----- <1>
HostEntry [
HostAddress = 0.0.0.0
HostAccessLevel = Enable
HostTrapCommunity =
HostTrapPort = 162
HostTelnetSNMP = 3
HostEntry ]

TFTPHostAddress = 172.16.85.100
TelnetTimeout = 0
TelnetSecEnable = Disable

[-StaticARPTable-]
## ----- <1>
StaticARPTable [
StaticArpIPAddress = 0.0.0.0
StaticArpPort = Unknown 0
StaticArpMacAddress = 00-00-00-00-00-00
StaticARPTable ]

Owner1 =
Owner2 =
TestIPAddress = 0.0.0.0
TestSubnetMask = 255.255.255.0
```

```
AuxiliaryIPAddress = 192.168.100.10
AuxiliarySubnetMask = 255.255.255.0
ModemPassword =
ModemSpeed = 192
ModemString =
RmtfFlag = Disable
LlfFlag = Disable
FlowControlFlag = Disable
UserPort = 1000M/Full
ExtPort = 100M/Full
MACAddressSwap = Enable
CRCRecalculate = Enable
sbmcFlag = Enable
MgmtVlanState = Disable
MgmtPort = Disable
MgmtVlanNumber = 1
UserVlanRule = No
UserVlanRule(1) = No
UserVlanRule(2) = No
UserVlanRule(3) = No
UserVlanRule(4) = No
UserVlanRule(5) = No
UserVlanRule(6) = No
UserVlanRule(7) = No
UserVlanTag = 0
UserVlanTag(1) = 0
UserVlanTag(2) = 0
UserPbitRule = 0
UserPbitRule(1) = 1
UserPbitRule(2) = 2
UserPbitRule(3) = 3
UserPbitRule(4) = 4
UserPbitRule(5) = 5
UserPbitRule(6) = 6
UserPbitRule(7) = 7
ExtVlanRule = No
ExtVlanRule(1) = No
ExtVlanRule(2) = No
ExtVlanRule(3) = No
ExtVlanRule(4) = No
ExtVlanRule(5) = No
ExtVlanRule(6) = No
ExtVlanRule(7) = No
ExtVlanTag = 0
ExtVlanTag(1) = 0
ExtVlanTag(2) = 0
ExtPbitRule = Disable
ExtPbitRule(1) = Enable
ExtPbitRule(2) = Flag Error 2
ExtPbitRule(3) = Flag Error 3
ExtPbitRule(4) = Flag Error 4
ExtPbitRule(5) = Flag Error 5
ExtPbitRule(6) = Flag Error 6
ExtPbitRule(7) = Flag Error 7
```

```
FramesOverX = 1522
UserVlanTagIn = 0
UserVlanTagIn(1) = 0
UserVlanTagIn(2) = 0
UserVlanTagIn(3) = 0
UserVlanTagIn(4) = 0
UserVlanTagIn(5) = 0
UserVlanTagIn(6) = 0
UserVlanTagIn(7) = 0
UserVlanTagOut = 0
UserVlanTagOut(1) = 0
UserVlanTagOut(2) = 0
UserVlanTagOut(3) = 0
UserVlanTagOut(4) = 0
UserVlanTagOut(5) = 0
UserVlanTagOut(6) = 0
UserVlanTagOut(7) = 0
ExtVlanTagIn = 0
ExtVlanTagIn(1) = 0
ExtVlanTagIn(2) = 0
ExtVlanTagIn(3) = 0
ExtVlanTagIn(4) = 0
ExtVlanTagIn(5) = 0
ExtVlanTagIn(6) = 0
ExtVlanTagIn(7) = 0
ExtVlanTagOut = 0
ExtVlanTagOut(1) = 0
ExtVlanTagOut(2) = 0
ExtVlanTagOut(3) = 0
ExtVlanTagOut(4) = 0
ExtVlanTagOut(5) = 0
ExtVlanTagOut(6) = 0
ExtVlanTagOut(7) = 0
PvstFilterFlag = Disabled
MasterSlaveFlag = Disable
AuxVlanState = Disable
AuxPort = Disable
AuxVlanNumber = 0
MaxFrameSize = 10000
MacFilterFlag = Enable
TestNetworkFilterFlag = Enable
OAMBPDUsFilterFlag = Enable
UDLDFilterFlag = Enable
MgmtVLANFilterFlag = Both Ports Enabled
EnabelAllTraps = Enable
ExtPortLinkTraps = Flag Error 2
RmtfTraps = Flag Error 2
LlfTraps = Flag Error 2
RemUserPortLinkTraps = Flag Error 2
LocUserPortLinkTraps = Flag Error 2
ConfigurationTraps = Flag Error 2
PowerSupplyTraps = Flag Error 2
ColdStartTraps = Flag Error 2
SbmcTraps = Flag Error 2
```

```
DiagnosticsTraps = Flag Error 2
SfpTraps = Flag Error 2
AuthenticationTraps = Flag Error 2
SecMinimumPasswordLength = 0
SecMinimumAlphaLength = 0
SecMinimumNumericLength = 0
SecMinimumPunctLength = 0
SecMaxConsecutiveOfType = 0
SecMaxSameChars = 0
SecUserNameInPassword = 1
SecPasswordExpirationTime = 0
SecPasswordReuseCount = 0
SecLockoutAfterAttempts = 0
SecLockoutType = Hard
SecLockoutTime = 0
SecDisplayLockoutMsg = 0
SecLockoutMsg = Account has been locked out
SecLockoutCraftPort = 0
SecInactivityLogoutTime = 0


[-UserAccounts-]
## ----- <1>
UserAccounts [
AccountUserName = admin
AccountPassword = F6FDFFE48C908DEB0F4C3BD36C032E72
AccountAccessLevel = Supervisor
AccountDescription = Upgrade Account
AccountState = 2
AccountPasswordExpires = 0
AccountPasswordExpiresTime = 0
AccountLockoutUser = 0
AccountLogoutUser = 0
AccountLockedState = 0
AccountLockoutTime = 0
AccountAccessFrom = 3
AccountSnmpv3AuthenProto = None
AccountSnmpv3AuthenKey =
000000000000000000000000000000000000000000
AccountSnmpv3PrivProt = 0
AccountSnmpv3Privkey = 00000000000000000000000000000000
AccountSyslogFilter = 0
AccountSyslogFilterBeginTime = 0
AccountSyslogFilterEndTime = 0
AccountOamlogFilter = 0
UserAccounts ]

SystemInfoName = Master ETSU
SystemInfoContact = NOC
SystemInfoLocation = 20600 Prairie St.
SystemInfoCustomer = Canoga Perkins5
SystemInfoInfo1 = N525-4
SystemInfoInfo2 =
SystemInfoCircuit1 =
SystemInfoCircuit2 =
SystemInfoServiceCode =
SystemInfoDateInService =
SystemInfoDateOutService =
SystemInfoEquipmentType =
SystemInfoEquipmentCode =
SystemInfoVendor =
SystemInfoCLEI =
SystemInfoMfgDate =


[-HostTable-]
## ----- <1>
HostTable [
HostTableIpMask = 172.16.2.93 /32
HostTableTelnetAccess = Telnet and SSH
HostTableSnmAccess = Write
HostTableSnmpProtocols = 2
HostTableSnmpReadCommunity = public
HostTableSnmpWriteCommunity = private
HostTableSnmpAccessLevel = 4
HostTableFtpAccess = 1
HostTable ]



[-TrapTables-]
## ----- <1>
TrapTables [
TrapTableKey = 172.16.85.100 163 V1-Trap
TrapTableSecurityName = public
TrapTableEngineId = 0C00000397010000402A00A941
TrapTableAuthenProto = 0
TrapTableAuthenKey =
000000000000000000000000000000000000000000
TrapTablePrivProto = 0
TrapTableSecurityLevel = 0
TrapTableRetries = 3
TrapTableTimeout = 5
TrapTablePrivKey = 00000000000000000000000000000000
TrapTables ]



[-OAM-]
## ----- <1>
OAM [
OAMAdmin = Disable
OAMMode = Passive
OAMSymbolPeriodWindow = 0
OAMSymbolPeriodThreshold = 0
OAMSymbolPeriodNotify = Enable
OAMFrameWindow = 10
OAMFrameThreshold = Enable
OAMFrameNotify = Enable
OAMFramePeriodWindow = 1488095
OAMFramePeriodThreshold = 1
OAMFramePeriodNotify = Enable
OAMFrameSecondsWindow = 600
OAMFrameSecondsThreshold = 1
OAMFrameSecondsNotify = Enable
OAMDyingGaspNotify = Enable
OAMCriticalEvent = Enable
OAMProcessRxLoopbackOAMPDU = Yes
OAMTransmitEventNotificationCount = 1
OAMProcessRxLinkFaultFlag = Yes
OAMFwdCriticalEvent = No
OAMEventLogFrequency = 600
OAM ]

## ----- <2>
OAM [
OAMAdmin = Enable
OAMMode = Active
OAMSymbolPeriodWindow = 0
OAMSymbolPeriodThreshold = 0
OAMSymbolPeriodNotify = Enable
OAMFrameWindow = 10
OAMFrameThreshold = Enable
OAMFrameNotify = Enable
OAMFramePeriodWindow = 1488095
OAMFramePeriodThreshold = 0
OAMFramePeriodNotify = Enable
OAMFrameSecondsWindow = 600
OAMFrameSecondsThreshold = 1
OAMFrameSecondsNotify = Enable
OAMDyingGaspNotify = Enable
OAMCriticalEvent = Enable
OAMProcessRxLoopbackOAMPDU = Yes
OAMTransmitEventNotificationCount = 1
OAMProcessRxLinkFaultFlag = Yes
OAMFwdCriticalEvent = No
OAMEventLogFrequency = 600
OAM ]
```

Index

CANOGA PERKINS CORPORATION

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