EdgeAccess

CANOGA PERKINS

9145E10G NID

Software Version 1.0

User Manual

NOTICE

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

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

CANOGA PERKINS CORPORATION
20600 Prairie Street
Chatsworth, California 91311-6008
Business Phone: (818) 718-6300
(Monday through Friday 7 a.m. - 5 p.m. Pacific Time)
FAX: (818) 718-6312 (24 hrs.)
Web Site: www.canoga.com
E-mail: fiber@canoga.com

EdgeAccess®
9145E10G NID Software Version 1.0
Software User's Manual
Product Number 6913750
Preliminary Rev. A 01/2010
TG

To reference Technical Advisories and Product Release Notes, go to the Canoga Perkins web site at http://www.canoga.com.

Preface

About the Manual

This manual provides instructions on the configuration and operation of the 9145E10G Network Interface Device (NID) version 1.0 software. The 9145E10G NID can be managed through the VT-100 terminal using the RS-232 serial port, through an Ethernet connection using a Telnet terminal emulation program, or using SNMP.

How this Manual is Organized

This document contains both information and procedures organized in roughly chronological order. Starting from an introduction to the Advanced 9145E10G software, it continues with system requirements, initial implementation, and continued operation.

The document includes the following components:

- Chapter 1, *Introduction to the 9145E10G Software* provides basic information about the software and navigation.
- Chapter 2, *Getting Started* describes how to set up and get started using the 9145E10G.
- Chapter 3, *System Configuration* describes how to configure the software management features.
- Chapter 4, *Diagnostics* describes how to configure and perform routine network diagnostics.
- Chapter 5, *Port Information* describes the User port, Network port, Multipurpose port, and the Management UTP port.
- Chapter 6, *System Alarms & Logs* describes how to configure System Alarms and Logs.
- Chapter 7, *Utilities* describes various system utilities.
- Chapter 8, *Software Upgrade* describes how to upgrade the NID software.
- *Chapeter 9, Manging Logged in Users*
- Chapter 10, *Link OAM* describes the Operations, Administration, and Maintenance functions, such as remote fault indication and remote loopback control, as specified by the IEEE 802.3ah standard.

What is New in This Document

The following changes have been made since this document was last released:

- Information that was added: **- None.** This is the first release of this software.
- Information that was changed: **- None.** This is the first release of this software.

For further information, refer to the release notes.

Optional Applications

The Performance Monitoring (PM), Service Availability Monitoring (SAM) and Protected Link Performance Monitoring (PLPM) are optional features that allow in-service monitoring of the performance attributes. Those performance attributes can be used to establish a Service Level Agreement (SLA) with different customers.

Performance Monitoring - Performance Monitoring is an optional feature for the 9145E10G that allows computing of performance attributes within a service instance. Those performance attributes are Delay, Jitter, and Frame Loss Ratio.

Service Availability Monitoring - The Service Availability Monitoring optional feature monitors the availability of service instance.

Protected Link Performance Monitoring - Protected Link Performance Monitoring (PLPM) is a feature that allows two 9145E10G NIDs that are deployed on a protected link to be able to participate in Performance Monitoring and Service Availability Monitoring.

For details about these optional features, refer to the Performance and Collection System (PCS) manual P/N 6912641.

Document Feedback

Because quality is our first concern at Canoga Perkins, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Please forward your feedback to:

techsupport@canoga.com

Provide the title and version number and as much detail as possible about your issue, including the topic heading, page number, and your suggestions for improvement.

Contacting Technical Support

Contact Canoga Perkins technical support (800-360-6642), or your 9145E10G support supplier, for hardware and software support, including product repairs and part ordering. Please have the following information available:

- NID model and serial number
- NID software version
- Detailed description of the problem and specific questions
- Details from messages in system log (if available)
- Description of any troubleshooting steps already performed and results

Contents

Chapter 1

Introduction

1.0 About the 9145E10G Software

Building on the industry-leading 10/100/1G 9145E Network Interface Device (NID), the 9145E10G adds10G Speed XFP ports and maintains the same set of features and capabilities as the 9145E.

1.1 Management Access

The 9145E10G can be managed through any of several access methods.

VT-100 Terminal - The VT-100 terminal is used to manage the NID locally via the EAI-232 serial port. It is primary used to perform initial configurations is the NID before it is connected to the network.

Telnet - Once the 9145E10G has been connected to your network it can be accessed using Telnet. All commands and functions are available using standard Telnet software.

SNMP - All commands and functions are also available using an SNMP manager. The 9145E10G supports SNMP v1/v2c/v3 and many standard MIBs as well as CP proprietary MIBs.

1.2 Management Security Features

The 9145E10G has comprehensive management access security features, including SNMPv3 authorization, RADIUS, password formatting, and user access controls. You can set values and options within the software that will work with the security protocols on your network. The four network security protocols listed below are supported. In addition, the 9145E10G provides options to define strong passwords, independent of the security protocols.

SNMPv3 - SNMPv3 provides authentication and encryption of management traffic across a network.

Remote Access Dial In User Security (RADIUS) - The RADIUS server maintains user account information. At login, the 9145E10G queries the server which authenticates the username and password and sends a message to the 9145E10G 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 9145E10G to disallow the login and reject the user.

Secure Shell version 2 (SSH-2) - SSH-2 provides authentication and encryption for a secure remote Telnet connection. SSH can be configured to provide unique User Accounts.

Secure File Transfer Protocol (SFTP) - SFTP adds encryption to protect uploaded files during the file transfer process, such as for a software update.

1.3 Three Levels of Security

Most Service Provider management networks provision certain access levels to technicians, network administrators, and managers. Offering different access levels to critical applications allows network administrators to keep closer watch on the entire network.

The 9145E10G allows view-based access to be set up for user interface features and SNMP access. A capabilities file allows views to be defined in an ASCII file and downloaded to the NID. A three (3) level security system on the 9145E10G controls all user interface and SNMPv3 access.

All 9145E10G features require that the user have a certain access level. The logged in user or SNMPv3 manager's access level is used to validate and control access to the 9145E10G features. When accessing a menu item or an SNMP object, the user's access level is checked against the access level required for the feature. If the user's access level is sufficient, then the access is granted. If the user's access level is not sufficient, an error message is displayed in the status area, or an SNMP error is returned.

The three access levels are *supervisor, operator,* and *observer*.

1. In the default configuration, the *supervisor* access level is allowed complete access to all of the 9145E10G's features including configuring the 9145E10G's security system.

2. The *operator* access level is allowed access to the 9145E10G features except those relating to the 9145E10G's security system. This level can be configurable by the administrator.
3. The *observer* access level is allowed access to the 9145E10G features that do not modify the 9145E10G's configuration. This level can be configurable by the administrator.

1.4 Changing Access Level Configuration

The assignment of access levels has a default configuration built into the 9145E10G. Creating and downloading a text file called 9145E.cap to the 9145E10G can change this assignment, however. This file contains mappings between module features and the access level required to access the feature.

As an example the entry that controls access to the Maximum Frame Size setting looks like: maxFrameSize=operator. This entry indicates that to change the Maximum Frame Size, a user's account must have "operator" access level or greater.

The default *9145E.cap* file containing the 9145E10G built-in security rules is provided with the 9145E10G release. To modify the security rules, simply modify the provided *9145E.cap* file and download this modified file to the 9145E10G.

As long as the unit has not received a cap file, there is no security while managing the unit from SNMP. Security will be enforced only from the User Interface (UI) based on the Access level; Supervisor, Observer or Operator. In order to Enable security from SNMP, the User will need to download the 9145E.cap file to the unit.

The default settings are defined in the original cap file provided by Canoga Perkins.

The *9145E.cap* file is downloaded to the 9145E10G via the normal FTP/SFTP/TFTP in the same manner as downloading a firmware file to the 9145E10G. The same file may be downloaded to multiple 9145E10G's to ensure the same security rules are implemented.

If the file *9145E.cap* is not downloaded to the 9145E10G, then the built-in feature to access level mappings in the 9145E10G are used. If a feature is not present in the file "9145E.cap" that is downloaded to the 9145E10G, then the built-in feature to access level mapping is used. If errors are found in this file, these errors are displayed in the 9145E10G's System log.

Chapter 2

Getting Started

2.1 Configuring Terminal Management

When using the RS-232 Serial Port for VT-100 sessions, Canoga Perkins suggests that you use HyperTerminal or another type of terminal emulation software when using a PC.

NOTE:Microsoft Vista OS does not include HyperTerminal. If your PC uses the Windows Vista operating system, you will need to install a terminal emulation program.

To set up HyperTerminal on your PC.

NOTE: For details on using MS Windows, refer to your MS Windows documentation.

1. Select **Start**>**All Programs**>**Accessories>Communications>HyperTerminal**.
2. At the Connection Description dialog, select an icon and enter the name for the connection. Click **OK**.
3. At the **Connect To** dialog, select the **Connect Using** menu. Select the **COM** port and click **OK**.
4. Select the Port Settings tab from the **COM Properties** dialog. Make the following selections:
   a. Bits per second: 9600 bps
   b. Data bits: 8
   c. Parity: None
   d. Stop bits: 1
   e. Flow control: None
6. Click **OK**.
7. Go to File->Properties->Settings and change the *Emulation* setting from *Auto detect* to *VT100*.
8. HyperTerminal connects to the system and the VT100 terminal emulation starts.

2.2 Setting Up SNMP Network Management

The 9145E10G communicates with CanogaView or your Network Management Platform either in-band, via the User or Network port, or out of band, via the Management UTP port.

NOTE: The Management UTP port is not available on all model numbers

2.2.1 About MIBs

To communicate with the 9145E10G using SNMP, standard Management Information Bases (MIBs) are required on your Network Management Platform. Refer to "Supported MIBs" on page 10 for a list of MIBs.

Additionally, Canoga Perkins Private MIBs are needed on the Management Platform to manage tasks specific to the Canoga Perkins 9145E10G. The Canoga Perkins Private MIBs are available for download in the Client Support area of the Canoga Perkins web site. Go to www.canoga.com then click on **Client Support**.

NOTE: When logging in to the client site or secure site you will need to register using the serial number of the 9145E10G.

2.2.2 9145E10G Set-up

There are several TCP/IP and SNMP parameters that need to be configured before accessing the 9145E10G from CanogaView or your Management Platform. These parameters include TCP/IP Address, Authorized Host List and Privileges. These parameters are initialized using a VT-100 Terminal connected to the RS-232 Serial Port. Refer to "System Configuration Menu" on page 11 for details on configuring these parameters.

2.3 Management User Interface

The Management User Interface for the 9145E10G provides a menu driven interface for setup, monitoring, and diagnostics. You can access the screens directly by connecting to the serial port of the 9145E10G or using Telnet.

A typical screen (Figure 2-1.) 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.

NOTE:Status screens do not have selectable items.

Use the following methods to navigate screens:

Space bar - When a menu item is highlighted, press the **Space** bar to cycle through all options for that item.

Tab - Press the **Tab** key to move the highlight to the next column.

Enter - Press the **Enter** key to select the highlighted option for a menu item or to go to the next line.

Escape - Press the **Esc** key once to cancel an action or to return to the previous screen.

To select an item from a screen menu enter the menu item number. For example you would press **6** and **Enter** to select "Utilities" as shown in Figure 2-1..

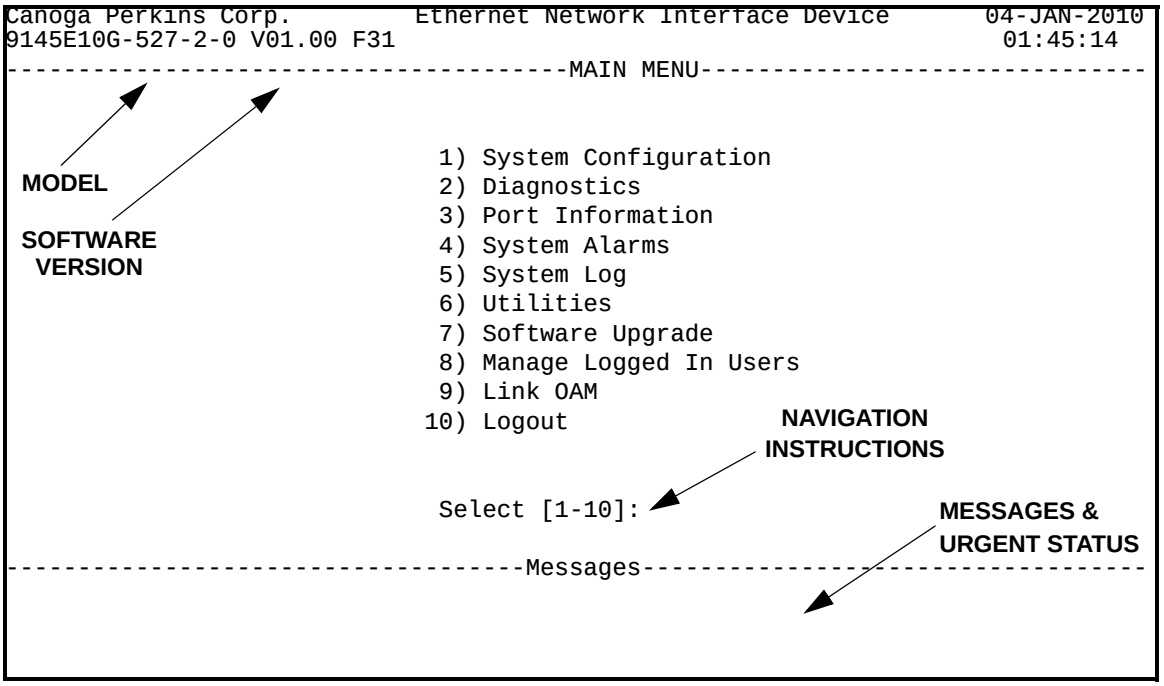

Figure 2-1. General Screen Format

2.4 Login

The first screen is the Login Screen (Figure 2-2.). Type your Username and press **Enter**. The Password prompt will then appear. Type your Password and press **Enter**. If the Username or Password are incorrect, you will return to the Username Prompt and the message *Invalid Username/Password entered* will be displayed.

CAUTION: Default username is admin and the default password is admin (lower case). Canoga Perkins strongly recommends you change the Default Username and Password during your initial configuration session. Should you lose both your Username and Password, the unit will need to be returned to Canoga Perkins for Factory Service and reset.

When you successfully log in, the Main Menu (Figure 2-3.) opens. Use the Main Menu to access all 9145E10G functions, including setup, diagnostics, and reports.

Refer to "Account Configuration" on page 28 and "Password Configuration" on page 26 for information about configuring you account and changing your password.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-------------------------------------MAIN MENU------------------------------


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









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

Figure 2-2. Login Screen

2.5 Main Menu

Following is a brief description of the Main Menu items.

1. System Configuration - The System Configuration menu is used to view and set values for system information and TCP/IP management communications parameters.

2. Diagnostics - The Diagnostics menu is used to set up various troubleshooting tests, including Loopback, Latency/Jitter, PING tests, or VLAN Loopback, and to configure and run the Performance Monitoring (PM), Service Availability Monitoring (SAM), and Protected Link Performance Monitoring (PLPM).

3. Port Information - The Port Information menu is used to ascertain the current conditions for all ports in the 9145E10G, to set and view the configuration information for specific ports, check Link Status and Layer 2 Statistics.

4. System Alarms - The System Alarms screen is used to view current alarm conditions.

5. System Log - The System Log screen displays a list of recent traps, alarms, and events.

6. Utilities - The Utilities menu is used to set-up and display basic functional information.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------------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) Link OAM
                             10) Logout


                              Select [1-10]:


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

Figure 2-3. Main Menu

7. Software Upgrade - The Software Upgrade screen is used to download and install new firmware using TFTP, swap firmware banks, and reset the 9145E10G.

8. Manage Logged In Users - The Manage Logged In Users screen is used by the administrator to view current users, and to terminate user sessions when required.

9. LINK OAM - The OAM menu is used to set, change, and view various link layer operational, administration and maintenance (OAM) functions.

10. Logout - Logout terminates your current session.

2.6 Supported MIBs

This section lists all supported MIBs including Standard MIBs and the Canoga Perkins MIBs.

Table 2-1. Standard MIBs

dot3oam.my	entitymib.my
hcnum.my	hcrmon.my
ifmib.my	iftype.my
inetaddress.my	ping.my
rmon.my	rmon2.my

Table 2-2. Canoga Perkins MIBs

cp9145estatus.my	cplicense.my	cpradius.my
cpaccounts.my	cploopback.my	cpsecurity.my
cpdot3oam.my	cpmgmtstatus.my	cpsfpstatus.my
cpentitynaming.my	cpnpa.my	cpsntp.my
cpentity.my	cppbvc.my	cpstatus.my
cpfanstatus.my	cpping.my	cpsysinf.my
cphosttb.my	cpportconfig.my	cpsyslog.my
cpifmib.my	cpportpbittrans.my	cpsystemlog.my
cpipconfig.my	cpportvlanrules.my	cptrapconfig.my
cplatency.my	cpportvlantrans.my	cptraptb.my
cpplpm.my	cppowersupply.my	cpvlanloopback.my

Chapter 3

System Configuration

3.0 System Configuration Menu

The System Configuration menu (Figure 3-1.) allows you to access the screens and menus necessary to configure various Management, IP, security, and alarm settings. The following section describes each item of the System Configuration menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------SYSTEM CONFIGURATION------------------------
                              1) IP/SNMP Agent Configuration
                              2) Trap Configuration
                              3) Security Configuration
                              4) Account Configuration
                              5) System Information
                              6) RADIUS Client Configuration
                              7) SNTP Client Configuration
                              8) SYSLOG Client Configuration
                              9) Hardware Information

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

Figure 3-1. System Configuration Menu

3.1 IP/SNMP Agent Configuration

The IP/SNMP Agent Configuration menu (Figure 3-2.) configures the Management IP, Test IP, and Auxiliary IP settings; and is used to add, edit, or delete Host Table and Trap Table entries.

The Management IP, Test IP, and Auxiliary IP Addresses are used for managing and conducting testing on a TCP/IP network.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------IP/SNMP AGENT CONFIGURATION---------------------


                            1) Management IP Configuration
                            2) Auxiliary IP Configuration
                            3) Host Table
                            4) Trap Table


                                   Select [1-4]:









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

Figure 3-2. IP/SNMP Agent Configuration Menu

3.1.1 Management IP Configuration

The Management IP Configuration menu (Figure 3-3.), is used to configure the management IP of the 9145E10G, including the subnet mask, gateway, and management VLAN. It is also used to configure which ports can be used for management access. See your network administrator for information and help with determining the appropriate parameters.

1. **Manager IP Address -** Used to set the 9145E10G Manager IP Address.
   Subnet Mask - Used to set the 9145E10G Manager IP Subnet Mask.
   Default Gateway - Used to set the IP Address of the Default Gateway.

2. **Manager Port -** Used to select the port(s) to allow Management Communication access. Options include: Both User and Net Ports, Net Port Only, User Port Only, Management UTP Port Only, or No Ports Allowed.

3. **Manager VLAN Tagging -** Used to enable or disable the use of a Management VLAN. The tags are 802.1Q compliant with an ether type of 0x8100.

4. **Manager VLAN ID -** When Manager VLAN Tagging is Enabled, this is used to set VLAN Tag ID between 0 and 4094. The default settings is 0.

CAUTION: The Manager IP Address, Subnet Mask, and Gateway address can be changed when locally or remotely connected. If changing the Management IP Configuration via remote access, you will be automatically disconnected when the Gateway address is changed. You will need to reconnect using the updated Manager IP Address, Subnet Mask, and Gateway address.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G10G-527-2-0 V01.00 F31                                         01:45:14
-------------------------------MANAGEMENT IP CONFIGURATION--------------------
 In-band Manager MAC Address      00 40 2A 02 2C D8
 Manager MAC Address (In-band)    00 40 2A 02 2C D8
 Manager Port Status              UP

 1)  Manager IP Address           172.016.142.239
     Subnet Mask                  255.255.000.000
     Default Gateway              172.016.001.001
 2)  Manager Port                 Both User and Net Ports
 3)  Manager VLAN Tagging         Disabled
 4)  Manager VLAN ID              0
 5)  Test IP Address              000.000.000.000
     Test Subnet Mask             255.255.255.000
 6)  Test Port                    Both User and Net Ports
 7)  Telnet Security              Disabled
 8)  Reply to Broadcast Ping      Disabled


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

Figure 3-3. Management IP configuration Menu

NOTE: The Test IP is used for PM and SAM testing. If PM and SAM are not licensed, the Test IP address can not be entered.

5. **Test IP Address -** Used to set the IP Address for PM and SAM optional applications.
   Test Subnet Mask - Used to set the Subnet Mask for PM and SAM optional applications.

6. **Test Port -** Used to select which port(s) allow access to the Test IP address. Parameters include: Both User and Net Ports, Net Port Only, User Port Only, or No Ports Allowed.

7. **Telnet Security -** Used to enable or disable checking if the host initiating the Telnet session is listed in the host table. If Telnet Security is enabled the host must be included as part of the host table. Default is disabled, which allows access from all hosts.

8. **Reply to Broadcast Ping -** Use to enable or disable the 9145E10G to reply to ICMP packets with a broadcast IP Host Address in the Manager IP subnet. Broadcast Ping replies are an ICMP packet and are rate limited to 100pps. Default is disabled.

3.1.2 Auxiliary IP Configuration

The Auxiliary IP is an additional IP address that is provided for testing and connectivity only. It allows the 9145E10G to be PINGed without allowing Telnet or Management access that could be disruptive. The Auxiliary IP rate is limited to 500 pings per second. This allows connectivity and rudimentary performance testing from subscriber/user VLANs without compromising network security.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-------------------------------AUXILIARY IP CONFIGURATION----------------------



 1)  Auxiliary IP Address         000.000.000.000
     Auxiliary Subnet Mask        255.255.255.000
 2)  Inband Auxiliary Port        Both User and Net Ports
 3)  Auxiliary VLAN Tagging       Disabled
 4)  Auxiliary VLAN Number        0
 5)  Allow Any Vlan               Disabled
 6)  Aux IP Rate Limiting         Enabled

                                  Select [1-6]:



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

Figure 3-4. Auxiliary IP configuration Menu

Configure the parameters by typing the corresponding number and pressing **Enter**. Enter data or press the **Space Bar** to cycle through the configuration choices for the parameters described below.

1. **Auxiliary IP Address -** Sets the 9145E10G Auxiliary IP Address.
   Auxiliary Subnet Mask - Sets the 9145E10G Auxiliary IP Subnet Mask.

2. **Inband Auxiliary Port -** Describes the Auxiliary IP address ports. Allows the customer to select No Ports, User Port Only, Net Port Only, or Both User and Net Ports.

3. **Auxiliary VLAN Tagging -** Enable or Disable Auxiliary IP VLAN Tagging.

4. **Auxiliary VLAN Number -** Sets Auxiliary IP VLAN ID number (between 0 and 4094). Default is 0.

5. **Allow Any VLAN -** Enable or Disable acceptance of any VLAN number. If Auxiliary VLAN Tagging is Enabled and Allow Any VLAN is Disabled, only packets tagged with the Auxiliary VLAN Number are accepted. If Auxiliary VLAN Tagging is Enabled and Allow Any VLAN is Enabled, then any VLAN can be used with the Auxiliary IP.

6. **Aux IP Rate Limiting -** Enable or Disable Auxiliary IP Rate Limiting. The rate limiting function is used to rate limit the traffic being received from the Aux IP. The Aux IP Rate Limiting default setting is enabled. Rate limiting may be set to Disable when running a test, however, the setting will return to Enabled after five minutes. An on screen timer shows time remaining until automatic enabling. To extend Disable Time beyond five minutes, disable Rate Limiting again before Timer expiration.

Table 3-1. IP Diagnostic Function Capabilities

Function	Management IP	Test IP	Auxiliary IP
Ping	√	√	√
Latency & Jitter	√	√	√
Performance Maintenance (PM)	√	√	N/A
Service Availability Monitoring (SAM)	√	√	N/A

3.1.3 Host Table

The Host Table menu (Figure 3-5.), configures the 9145E10G to send and receive SNMP, FTP, and Telnet traffic to the Managing Host IP address, and access from specific Telnet clients when Telnet security is enabled (Figure 3-6.). Use the Host Access Table to configure access by each host including access type and privileges (SNMP, FTP, Telnet).

3.1.3.1 Adding/Editing a Managing Host IP

To add a Managing Host IP, select Add (**A**) from the Host Access Menu. To edit an existing Managing Host IP select Edit (**E**). To delete a Managing Host IP select Delete (**D**). The Edit Host Access menu (Figure 3-6.) opens.

1. Enter the Managing Host IP address to add to the Host Access list and press **Enter**.
2. Enter the IP Mask Size (default value 32). To have an entire subnet access the 9145E10G, enter the mask size for the subnet.
3. Select a Telnet access value. Choices for Telnet access are: Telnet and SSH, Telnet Only, SSH Only, or None.
4. Cycle through the FTP Access parameters FTP and SFTP, FTP Only, SFTP Only, or None using the **Space Bar.** Press **Enter** to select the parameter.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
--------------------------------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

172.016.000.000/16 All    All    Write  V1/V2c/V3 public      private     Superv









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


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

Figure 3-5. Host Access Table Menu

5. Cycle through the SNMP Access parameters Read, Write, or None using the **Space Bar.** Press **Enter** to select the parameter.
6. Cycle through the SNMP Protocol parameters V1/V2c/V3, V1/V2c, or V3 using the **Space Bar.** Press **Enter** to select the parameter.
7. Type in the desired V1/V2c Read Community and press **Enter**.
8. Type in the desired V1/V2c Write Community and press **Enter**.
9. Use **Space** to scroll through the V1/V2c Access Levels (Operator, Supervisor, or Observer). Press **Enter** to select desired setting.
10. Press **Esc** to return to the Host Access Table menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------EDIT HOST ACCESS-----------------------------

    Managing Host IP       :
    IP Mask Size           :
 1. Telnet Access          :
 2. FTP Access             :
 3. SNMP Access            :
 4. SNMP Protocol          :
 5. V1/V2c Read Community  :
 6. V1/V2c Write Community :
 7. V1/V2c Access Level    :









        Enter Managing Host IP address
------------------------------------Messages-----------------------------------
```

Figure 3-6. Add Host Access Menu

3.1.4 Trap Table

The Trap/NotificationTable menu (Figure 3-7.) is used to configure the SNMP Trap Managers. The following section describes how to add new Managers, edit existing Managers, or to delete selected Managers.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
---------------------TRAP/NOTIFICATION DESTINATION TABLE-----------------------
-
Managing              Trap       Username/            Security
Host            Port  Type       Community            Level

172.003.016.033 162   V2c-Inform private              N/A
172.003.215.147 162   V2c-Trap   public               N/A
172.016.004.053 162   V1-Trap    private              N/A
174.002.145.003 162   V3-Trap    admin                Auth/Priv
174.003.154.021 162   V3-Inform  admin                No Auth/No Priv





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


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

Figure 3-7. Trap/Notification Destination Table Menu

3.1.4.1 Adding a Host IP

To Add a Host IP, on the Trap/Notifdication Destination Table (Figure 3-7), type (**A)dd** and press **Enter**. The Edit Trap/Notification menu (Figure 3-8.) opens.

1. Type in the Host IP address to add to the Trap/Notification Destination Table, and press **Enter**.
11. Enter the Trap/Notification Port. The default value is 162 for regular SNMP managers, 163 is for CanogaView. Any port numbers from 1 to 65535 can be used to receive traps. Check with your IT manager to ensure the port setting is correct.
12. Use **Space** to select the Notification Type for this SNMP host. Selections are: V1-Trap, V2c-Trap, V2c-Inform, V3-Trap, and V3-Inform.

NOTE: Each Notification Type has a different configuration procedure. Follow the specific procedure for the Notification Type selected.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------EDIT TRAP/NOTIFICATION TYPE-----------------------

    IP Address              :
    Trap/Notification Port  :
    Notification Type       :









        Enter Managing Host IP address
-----------------------------------Messages-----------------------------------
```

Figure 3-8. Add Trap/Notification Type Menu

3.1.4.2 Editing a Host IP

To Edit a Host IP, on the Trap/Notifdication Destination Table (Figure 3-7), type Edit (**E**), use **Space** to select a Host IP address, and press **Enter**. The Edit Trap/Notification menu (Figure 3-6.) opens.

1. Type in the Host IP address to add to the Trap/Notification Destination Table, and press **Enter**.
2. Enter the Trap/Notification Port, the default value is 162 for regular SNMP managers, 163 should be for CanogaView. Any port numbers from 1 to 65535 can be used to receive traps. Check with your IT manager to ensure the port setting is correct.
3. Select the Notification Type for this SNMP host. Selections are: V1-Trap, V2c-Trap, V2c-Inform, V3-Trap, and V3-Inform.

NOTE: Each Notification Type has a different configuration procedure. Follow the specific procedure for the Notification Type selected.

4. **If V1-Trap or V2c-Trap was selected** (Figure 3-9.):
   a. Enter the Community Name.
   b. Press **Enter**.
   c. Press **Esc** to return to the Trap/Notification Destination Table menu (Figure 3-7.).

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
---------------------TRAP/NOTIFICATION DESTINATION TABLE-----------------------

    IP Address              : 172.002.145.003
    Trap/Notification Port  : 162
    Notification Type       : V1-Trap (or V2c-Trap)

 1. Community Name          :









        Enter the trap community name [32 characters maximum]                 -
-----------------------------------Messages-----------------------------------
```

Figure 3-9. V1-Trap or V2c-Trap Notification Type Parameter

5. **If V2c-Inform was selected** (Figure 3-11.):
   a. Enter the Community Name.
   b. Accept or revise the Retries parameter (default is 3).
   c. Accept or revise the Timeout in Seconds parameter (default is 5).
   d. Press **Enter** and then press **Esc** to return to the Trap Table menu (Figure 3-7.).

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------EDIT TRAP/NOTIFICATION TYPE------------------

    IP Address              : 172.002.015.032
    Trap/Notification Port  : 125
    Notification Type       : V2c-Inform

 1. Community Name          : Private
 2. Retries                 : 5
 3. Timeout in Seconds      : 30









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

Figure 3-10. V2c-Inform Notification Type Parameter

6. **If V3-Trap was selected** (Figure 3-11.):
   a. Use the **Space Bar** to select the Security Name and press **Enter**.
   b. Use the **Space Bar** to select the Security Level (No Auth/No Priv, Auth/No Priv, or Auth/Priv) and press **Enter**.
   c. Press **Esc** to return to the Trap Table menu (Figure 3-7.).

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------EDIT TRAP/NOTIFICATION TYPE-----------------

    IP Address              : 172.002.015.032
    Trap/Notification Port  : 125
    Notification Type       : V2c-Inform

 1. Community Name          : Private
 2. Retries                 : 5
 3. Timeout in Seconds      : 30









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

Figure 3-11. V3-Trap Notification Type Parameter

7. **If V3-Inform was selected** (Figure 3-12.):

   a. Type in the Security Name and press **Enter**.

   b. Type in the SNMP Engine ID and press **Enter**.

   c. Cycle through the Authentication Protocol setting (MD5, SHA, or None) using the **Space Bar.** Press **Enter** to accept the setting.

   d. Type in the Authentication Password and press **Enter**. Type in the password again and press **Enter**. The Authentication Key will automatically be entered (It can be modified to match the SNMP manager's key if needed.).

   e. Cycle through the Privacy Protocol settings (DES or None) using the **Space Bar** and press **Enter** to accept the setting.

   f. Type in the Privacy Password, if required, and press **Enter**, then type in the password again and press **Enter**. The Privacy Key will automatically be entered (It can be modified to match the SNMP manager's key if needed.).

   g. Cycle through the Security Levels (No Auth/No Priv, Auth/No Priv, or Auth/Priv) using the **Space Bar** and press **Enter** to accept the setting.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------------EDIT TRAP/NOTIFICATION TYPE----------------------

    IP Address              : 174.003.154.021
    Trap/Notification Port  : 162
    Notification Type       : V3-Inform

 1. Security Name           : admin
 2. Engine ID
  : 1478502698564231852145
 3. Authentication Protocol : None
 4. Authentication Password : N/A
 5. Authentication Key      : N/A
 6. Privacy Protocol        : N/A
 7. Privacy Password        : N/A
 8. Privacy Key             : N/A
 9. Security Level          : No Auth/No Priv
10. Retries                 : 3
11. Timeout in Seconds      : 5

                                 Select [1-11]:
---------------------------------Messages-------------------------------------
```

Figure 3-12. V3-Inform Notification Type Parameter

h. Accept the Retries entry or modify it by using **Backspace** and typing the new value and press **Enter** (default is 3).

i. Accept the Timeout in Seconds entry or modify it by using **Backspace** and typing the new value and press **Enter** (default is 5).

j. Press **Esc** to return to the Trap Table menu (Figure 3-7.).

3.1.4.3 Deleting a Host IP

To Delete a Host IP, select Delete (**D**) use the Space Bar to select a Host IP address, and press **Enter**.

3.2 Trap Configuration

Trap configuration defines how various alarms events are handled. Traps can be configured to be logged, sent to the SNMP managers in the Trap Notification/Destination Table, or both logged and sent for each event. Traps can also be set to Disabled.

Trap Config Item	Traps Affected	MIB Location
Master Trap Control	All	
User Port Link Traps	linkUp (User Port)	ifmib.my
	linkDown (User Port)	ifmib.my
Network Port Link Traps	linkUp (Network Port)	ifmib.my
	linkDown (Network Port)	ifmib.my
Remote Fault Traps	cp9145E10GPortRemoteFaultReceived	cp9145E10GStatus.my
	cp9145E10GPortSendingRemoteFault	cp9145E10GStatus.my
	cp9145E10GPortRemoteFaultCleared	cp9145E10GStatus.my
Link Loss Forwarding Traps	cp9145E10GPortLLFActivated	cp9145E10GStatus.my
Cold Start Traps	coldStart	v2-mib.my
Authentication Traps	cpAuthenticationFailure	cpMgmtStatus.my
Diagnostic Traps	cpPortLoopbackOn	cpLoopback.my
	cpPortLoopbackOff	cpLoopback.my
Entity Configuration Traps	entConfigChange	EntityMib.my
Fan/Power/ Temperature Traps	cpMainBoardVoltageLevelsOK	cpStatus.my
	cpMainBoardVoltageLevelsOutOfRange	cpStatus.my
	cpDyingGasp	cpPowerSupply.my
	cpPowerSupplyFailed	cpPowerSupply.my
	cpPowerSupplyOverHighLimit	cpPowerSupply.my
	cpPowerSupplyUnderLowLimit	cpPowerSupply.my
	cpPowerSupplyOK	cpPowerSupply.my
	cpFanOK	cpFanStatus.my
	cpFanSlow	cpFanStatus.my
	cpFanFailed	cpFanStatus.my
	cpTemperatureOverHighThresholdAlarm	cpStatus.my
	cpTemperatureHighThresholdAlarmCleared	cpStatus.my
	cpTemperatureWarningApproachingHigh-Threshold	cpStatus.my

Trap Config Item	Traps Affected	MIB Location
	cpTemperatureHighThresholdWarning-Cleared	cpStatus.my
	cpTemperatureAlarmUnderLowThreshold	cpStatus.my
	cpTemperatureLowThresholdAlarmCleared	cpStatus.my
	cpTemperatureWarningApproachin-gLowThreshold	cpStatus.my
	cpTemperatureLowThresholdWarning-Cleared	cpStatus.my
XFP Traps	cpXfpRemoved	cpXfpStatus.my
	cpXfpInsertedInvalid	cpXfpStatus.my
	cpXfpInsertedValid	cpXfpStatus.my
	cpXfpTxOk	cpXfpStatus.my
	cpXfpTxWarning	cpXfpStatus.my
	cpXfpTxFailure	cpXfpStatus.my

The System Log contains the log of all enabled Trap events.

1. To configure Traps, select Trap Configuration (**2**) from the System Configuration menu. The Trap Configuration menu (Figure 3-13.) opens.

8. Select the number of the trap group to change and press **Enter**. Cycle through the Log Only, Send Only, Both Log And Send, or Disabled parameters using the **Space Bar**.

The Master Trap Control setting will override all other trap settings. For example, if the Master Trap Control is set to Log Only, rather than set to Both Log And Send (as shown), all the other traps will only log alarm events, regardless of the individual trap settings. If the Master Trap Control is set to Log And Send, the individual traps will perform according to their individual settings. Setting the Master Trap Control setting to Disabled will disable all traps.

9. Press **Enter** to close the editing function and then press **Esc** to return to the System Configuration menu.

NOTE: The setting of the Master Trap Control will override all other trap settings.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-------------------------------TRAP CONFIGURATION-----------------------------

        1) Master Trap Control           Log Only

        2) User Port Link Traps          Both Log and Send
        3) Netdwork Port LInk Traps      Both Log and Send
        4) Remote Fault Traps            Both Log and Send
        5) Link Loss Forwarding Traps    Both Log and Send

        6) Cold Start Traps              Both Log and Send
        7) Authentication Traps          Both Log and Send
        8) Diagnostic Traps              Both Log and Send
        9) Entity Configuration Traps    Both Log and Send
       10) Fan/Power/Temperature Traps   Both Log and Send
       11) XFP Traps                     Both Log and Send


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

Figure 3-13. Trap Configuration Menu

3.3 Security Configuration

The 9145E10G can be configured for Strong passwords. Use the Security Configuration Menu to set or change the Password Configuration and the Lockout/Logout Configuration. From the System Configuration menu select Security Configuration (**3**). The Security Configuration menu (Figure 3-14.) opens.

3.3.1 Password Configuration

Select the Password Configuration item to change by typing the corresponding number. Press **Enter** to close the editing function and then press **Esc** to return to the System Configuration menu. The 9145E10G permits strong passwords as follows:

1. **Minimum Length** - Specifies the minimum number of alpha-numeric characters of a password. Enter a value between 0 and 15. A setting of 0 will allow you to log in without a password.
2. **Minimum Alpha Characters** - Specifies the minimum number of alpha characters a password must contain. Valid alpha characters are a-z (lower case) and A-Z (capitalized). Enter a value between 0 and 15.
3. **Minimum Numeric Characters** - Specifies the minimum number of numeric characters a password must contain. Valid numeric characters are 0-9. Enter a value between 0 and 15.
4. **Minimum Punctuation Characters** - Specifies the minimum number of punctuation characters a password must contain. Valid punctuation characters are any non-space,

non-alpha, and non-numeric characters.Enter a value from 0 through 15 Valid punctuation characters include:

! @ # $ % ^ & * ( ) _ + - , < .

= ~ ‘ ; : ‘ “ [{] } \ | > / ?

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
---------------------------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-----------------------------------
```

Figure 3-14. Security Configuration Menu

5. **Maximum Consecutive Character Types** - Specifies the number of alpha, numeric, or punctuation characters that can be used consecutively. Enter a value from 1 through 15.
6. **Maximum Same Character** - Specifies the maximum number of times that any character may be repeated within the password. This includes alpha, numeric or punctuation character types. Enter a value between 0 and 15.
7. **Allow Username In Password** - Determines if the user's account name can be within any part of the password. Use **Space** to cycle between Enabled and Disabled.
8. **Password Expiration Time** - The number of days until the password expires and a new one is required. Enter a value between 1 and 365. A setting of 0 disables this feature. If the password expires, the Supervisor will have to reset the password.

CAUTION: If the Supervisor password has expired, the 9145E10G NID will have to be sent to Canoga PerkinsTechnical Support to be reset.

9. **Password Reuse Count** - The number of password expirations a user must wait until a password can be reused. When set to 0, the user can reuse their current password with no count limitation. When set to 1, a password can be reused after one password reset.

3.3.2 Lockout/Logout Configuration

Select the Lockout/Logout Configuration item you want to change by typing the corresponding number. Press **Enter** to close the editing function and then press **Esc** to return to the System Configuration menu.

1. **Lockout After Failed Attempts** - The number of attempts a user may make before the account becomes disabled. The Lockout Type field controls the lockout behaviors. Enter a value between 1 and 15. A setting of 0 will disable this feature.
2. **Lockout Type** - The options are *Hard* or *Timed*. Timed requires the user to wait a specified number of minutes before a retry. Hard requires the System Administrator to unlock the account. Use the **Space Bar** to select Timed or Hard.

   Lockout Time - The number of minutes that a user must wait before a retry. Enter a value between 0 and 30.
3. **Display Lockout Message** - Specify if a message will be displayed when an account has been locked. Refer to the Lockout Message in option 13. Use the **Space Bar** to select Enabled or Disabled.
4. **Lockout Message** - Specifies the text to be displayed if option 12 is Enabled. The message should be customized to list the person to contact in case an account is disabled. Enter a text message of up to 30 characters.
5. **Lockout Craft Port** - Specifies whether the RS-232 serial port interface on the device should be locked to prevent using the serial interface to access the system. Use the **Space Bar** to select Enabled or Disabled.
6. **Inactivity Logout Time** - Specifies the number of minutes of inactivity before a user is automatically logged out. Enter a value between 1 and 30. A setting of 0 will disable this feature.

3.4 Account Configuration

Use the Account Configuration menu to add new accounts, edit existing accounts, or to delete accounts. There must be at least one Supervisor account. The 9145E10G NID allows up to 24 accounts. Four telnet sessions may take place at the same time. Only one FTP session may take place at any time.

NOTE: Any action that affects the network configuration of the 9145E10G (i.e., resetting the IP address) will disconnect all telnet sessions.

From the System Configuration menu select Account Configuration (**4**). The Account Configuration menu (Figure 3-15.) opens.

1. Username - The name of the new account you wish to add to the user list.

2. Account State - Specifies whether the account is enabled or disabled.

3. Access From - Determines from where the user can access this account.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------ACCOUNT CONFIGURATION---------------------------

            Account   Access         Access                                Locked
Username    State     From           Level       Description              Out

admin       Enabled   UI/SNMPv3      Supervisor  Default Account          No
Obs         Enabled   UI/SNMPv3      Operator                             No
Ope         Enabled   UI             Operator                             No









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

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

Figure 3-15. Account Configuration Menu

4. **Access Level -** Specifies the security level required to access this account.

5. **Description -** Term used to describe the account type.

6. **Locked Out -** Indicates if the Supervisor has locked the user out of the system.

3.4.1 Three Levels of Security

A three (3) level security system on the 9145E10G controls all user interface and SNMPv3 access. The three access levels are *supervisor*, *operator*, and *observer*.

Most Service Provider management networks provision certain access levels to technicians, network administrators, and managers. Offering different access levels to critical applications allows network administrators to keep closer watch on the entire network.

All 9145E10G features require a certain access level for access. The logged in user or SNMPv3 manager's access level is used to validate and control access to the 9145E10G features. When accessing a menu item or an SNMP object the user's access level is checked against the access level required for the feature. If the user's access level is sufficient, then the access is granted. If the user's access level is not sufficient, an error message is displayed in the status area or an SNMP error is returned.

In the default configuration, the *supervisor* access level is allowed complete access to all of the 9145E10G's features including configuring the 9145E10G's security system. The *operator* access level is allowed access to the 9145E10G features except those relating to the 9145E10G's security system. This level can be configurable by the administrator.

The *observer* access level is allowed access to the 9145E10G features that do not modify the 9145E10G's configuration. This level can be configurable by the administrator. Feature Access Level Configuration The assignment of access levels has a default configuration built into the 9145E10G. Creating and downloading a text file called *9145E.cap* to the 9145E10G can change this assignment, however. This file contains mappings between module features and the access level required to access the feature. As an example the entry that controls access to the Maximum Frame Size setting looks like: maxFrameSize=operator

This entry indicates that to change the Maximum Frame Size, a user's account must have *operator* access level or greater.

This *9145E.cap* file is downloaded to the 9145E10G via the normal FTP/SFTP/TFTP in the same manner as downloading a firmware file to the 9145E10G. The same file may be downloaded to multiple 9145E10G's to ensure that each is following the same security rules.

3.4.2 Add or Edit an Account

To add an account select Add (**A**). The Edit User Account screen (Figure 3-16.) will open with all positions blank. When the account information has been entered successfully, press **Esc** to return to the Account Configuration menu.

To edit an account select Edit (**E**) and use the **Space Bar** to select an account. The Edit User Account screen (Figure 3-16.) will open with all positions populated.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------EDIT USER ACCOUNT----------------------------
    Username                       : Obs
 1. Account State                  : Enabled
 2. Access From                    : UI/SNMPv3
 3. Access Level                   : Operator
 4. Description                    :
 5. UI Password                    : ***************
 6. UI Password Expires            : No
    UI Password Expires in (days)  : 0
 7. Allow UI Lockout Of User       : Yes
 8. Allow UI Logout Of User        : Yes
 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-----------------------------------
```

Figure 3-16. Edit User Account Screen

1. **Username -** The name of the new account you wish to add to the user list. Enter a name of up to 10 characters.

7. **Account State** - Specifies whether the account is active. Use **Space** to cycle between Enabled and Disabled.

8. **Access From** - Determines from where the user can access this account. Use **Space** to cycle between UI, SNMPv3, and UI/SNMPv3.

NOTE: SNMP only cannot FTP.

9. **Access Level** - Specifies the security level required to access this account. Use the **Space Bar** to cycle between Observer, Operator, and Supervisor.

10. **Description** - Term used to describe the account type. Enter descriptive text up to 17 characters.

11. **UI Password** - A password is only required if Access From is set to UI or UI/SNMPv3. Type the desired password and press **Enter**. Reenter the password. Passwords are limited to 15 characters.

12. **UI Password Expires** -Determines whether the password will expire and required to be changed. Use the **Space Bar** to select Yes or No.

    Password Expires in (days) - Establishes the number of days each password can be used before a new password is required. Enter a number between 1 and 365. A setting of 0 will require a new password each time the account is opened.

13. **Allow UI Lockout Of User** - Gives Supervisors the ability to lock users out of the system. Use the **Space Bar** to select Yes or No.

14. **Allow UI Logout Of User** - Gives Supervisors the ability to log users off the system. Use the **Space Bar** to select Yes or No.
15. **UI Login Locked State** - Determines the current state of the UI Login. Use the **Space Bar** to cycle between Locked and Unlocked.
16. **SNMPv3 Authentication Protocol** - Sets the authentication protocol for SNMPv3 access. Use the **Space Bar** to cycle between None, MD5, and SHA.
17. **SNMPv3 Authentication Password** - Used to enter the SNMPv3 authentication password. This password is not stored. It is used to generate the SNMPv3 authentication key. Type the desired password and press **Enter**. Reenter the password. The password is required to be between 8 and 15 characters. This field will be passed over if the SNMPv3 authentication protocol is set to **None**.

    SNMPv3 Authentication Key - Displays the computed SNMPv3 authentication key. This is a field that is shared with an SNMPv3 management application to allow authenticated protocol exchanges.
18. **SNMPv3 Privacy Protocol** -The privacy protocol used for SNMPv3 access. Use the **Space Bar** to cycle between None and DES.
19. **SNMPv3 Privacy Password** - Used to enter the SNMPv3 privacy password. This password is not stored. It is used to generate the SNMPv3 privacy key. Type the desired password and press **Enter**. Reenter the password. The password is required to be between 8 and 15 characters. This field will be passed over if the SNMPv3 Privacy Protocol is set to None.

    SNMPv3 Privacy Key - Displays the computed SNMPv3 privacy key. This is a field that must be shared with an SNMPv3 management application to allow private SNMPv3 protocol exchanges.

3.4.3 Delete an Account

NOTE:An account cannot be deleted while the user is logged in. In addition, you cannot delete the last supervisor account.

Before attempting to delete an account make sure the user is logged out. Use the following procedure to delete an account.

1. Select Delete (**D**) and press **Enter**. The first User Account will be highlighted.
2. Use the **Space Bar** to scroll through the user names to select the account.
3. When deletions are completed, press **Esc** to return to the System Configuration menu.

3.5 System Information

The System Information screen is used to add or edit administrative and circuit information, such as the name of the 9145E10G, contact, location, customer, circuit, equipment codes and Common Language Equipment Identification (CLEI) information.

System Name, Contact, and Location are the same as the MIB-II variables sysName, sysLocation, sysContact.

1. From the System Configuration menu, select System Information (**5**) and press **Enter**. The System Information screen (Figure 3-17.) opens.
4. Type the number of the parameter to enter information about, then press **Enter**.
5. Type in new information or edit existing information.
6. To return to the Main Menu, press **Esc**. When finished, use **Enter** to save the settings, then **Esc** to return to the System Configuration menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------SYSTEM INFORMATION------------------------------
 1. System Name         :
 2. Contact             :
 3. Location            :
 4. Customer            :
 5. Information         :
                        :
 6. Circuits            :
                        :
 7. Service Code        :
 8. Date-in-Service     :
 9. Date-Out-of-Service :
10. Equipment Type      :
11. Equipment Code      :
12. Vendor              : Canoga Perkins
13. CLEI                :
14. Mfg Date            : 10/01/2009

                                   Select [1-14]:
-----------------------------------Messages-------------------------------------
```

Figure 3-17. System Information Screen

1. System Name - The system name can be up to 25 characters long. It is displayed in the header under *Ethernet Network Interface Device*. If you are running multiple telnet sessions, you will be able to identify the NID you are viewing.
2. Contact - up to 25 characters
3. Location - up to 25 characters
4. Customer - up to 25 characters
5. Information - two lines, up to 40 characters each

6. Circuits - two lines, up to 25 characters each
7. Service Code - up to 10 characters
8. Date-in-Service - [mm/dd/yyyy] - displays when the 9145E10G was placed into service
9. Date-Out-of-Service - [mm/dd/yyyy] - displays when the 9145E10G was last taken out of service
10. Equipment Type - up to 10 characters
11. Equipment Code - up to 10 characters
12. Vendor - up to 25 characters
13. CLEI - Common Language Equipment Identification (CLEI) up to 10 characters
14. Mfg Date - [mm/dd/yyyy] - an editable date field

3.6 RADIUS Client Configuration

RADIUS (Remote Authentication Dial-In User Service) software support is provided for User Authentication.

RADIUS provides the ability to have user interface accounts to be maintained and authenticated by a RADIUS server. The RADIUS server also maintains user account information:

AccessFrom - Where the account can be used.

AccessLevel - The security access level for the user.

Description - The account description.

LogoutUser - Whether or not the user can be forcefully logged out.

When a user enters a username and password and RADIUS has been configured, the username and password is sent to the RADIUS server and is validated there. If valid, then the RADIUS server sends an accept message along with the above account information and the 9145E10G RADIUS client allows the user in with this configuration.

The RADIUS server may send a reject message in which case the user is not logged in. The RADIUS server may also send a challenge message if it has been configured to do so in which case the user is prompted for additional authentication information at which time the RADIUS server will then send an accept or reject message. This is the RADIUS client configuration:

Up to two RADIUS servers can be configured. The RADIUS server that is consulted is determined by the server priority. The server with the lowest priority number is consulted first. If it does not respond, then the other RADIUS server is consulted (if configured). If both servers are configured with the same priority then a round-robin access is used; first one RADIUS server will be consulted and the next request will be sent to the other RADIUS server first. The server priorities are relative. That is, you could configure one server with priority 10 and the other with 20. The values of the numbers do not matter, just the relative values of the numbers (in this case 10 being less than 20). This is done to allow you to easily change the server priorities without having to edit both entries. If you had configured the servers with 10 and 20, you could make the server with 20 have higher priority simply by changing its priority to 5; no need to change the one with 10.

1. **RADIUS Client Mode:**

   Options: RADIUS then Local, Local then RADIUS, or None

   RADIUS then Local says that when a user tries to log in, the username and password is passed to the configured Primary RADIUS Server first for authentication. If there is no connectivity to the Primary RADIUS Server, the RADIUS Client attempts to authenticate the login request on the Secondary RADIUS Server. If there is no connectivity to the Secondary RADIUS Server, the 9145E10G can then use the local database.

   Local then RADIUS says that when a user tries to log in, the local user accounts database is consulted to try to authenticate the user. If the user cannot be authenticated by the local accounts database, then the RADIUS Server is consulted to authenticate the user.

   None says that the RADIUS server is never used and all user access is authenticated by the local user accounts database.

2. **RADIUS Server IP Address:** The IP address of the RADIUS server. If 0.0.0.0 then this server configuration will not be used.

   RADIUS Server Shared Secret: 16 character secret that is shared by the RADIUS server and the RADIUS client to encrypt sensitive RADIUS traffic on the wire. The value entered here must match what is configured into the RADIUS server.

   RADIUS Server Retries: The number of attempts to authenticate a user using this RADIUS server before giving up or using the alternate RADIUS server if configured. 0 - 10

   RADIUS Server Timeout: The time in seconds before assuming that the RADIUS server did not reply and retrying a request if so configured. 1 - 30

   RADIUS Server Priority: The RADIUS server priority in relation to the alternate RADIUS server if configured. The server with the lower priority will be consulted first to authenticate a user. Servers with the same priority operate in a round-robin fashion alternating requests to each server. 1 - 255

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------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-----------------------------------
```

Figure 3-18. RADIUS Client Configuration screen

3. **RADIUS Server IP Address** - Provides the IP address of the RADIUS server. Use **Backspace** to remove an existing IP address and type in a new IP address.

   RADIUS Server Shared Secret - This is the security question the user must answer before remote access is allowed. Use **Backspace** to remove an existing question and type in a new question. Questions are limited to 16 characters.

   RADIUS Server Retries - Specifies the number of times a user can enter the wrong Shared Secret response before they are locked out of the system. Enter a value between 0 and 10.

   RADIUS Server Timeout - Specifies the length of time, in seconds, the server will wait for a response before it times out. Enter a value between 1 and 30.

   RADIUS Server Priority - Determines the order in which the RADIUS servers are consulted. Enter a value between 1 and 255.

3.7 SNTP Client Configuration

Use the SNTP Client Configuration screen to configure the 9145E10G to use a primary and secondary SNTP Server to automatically set the date and time. An accurate date and time in the 9145E10G 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.

- For accuracy within a large network, you can set up the 9145E10G to synchronize the system date and time to an SNTP server.
- The time and date can be set manually. Refer to "Set Date and Time" on page 76 for information to set the date and time manually.

To configure SNTP, select SNTP Client Configuration (**7**) from the System Configuration menu and press **Enter**. The Simple Network Time Protocol (SNTP) Client Configuration screen (Figure 3-19.) opens.

On the SNTP client Configuration screen, type the number of the SNTP setting to change and then press **Enter**.

Use the **Space Bar** to cycle through predetermined settings, and press **Enter**.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------SNTP CLIENT CONFIGURATION----------------------------
 1. SNTP Client UTC Offset (hours)     : 0
 2. SNTP Client Observe DST            : Disabled
    SNTP Client DST Starts At          : 01/01/1970 00:00
    SNTP Client DST Ends At            : 01/01/1970 00:01
 3. SNTP Client Sync Interval (minutes): 5
 4. SNTP Client Delay Time (seconds)   : 0

 5. SNTP Server IP Address 1           : 0.0.0.0
    SNTP Server Retries 1              : 3
    SNTP Server Timeout 1 (seconds)    : 5
    SNTP Server Priority 1             : 1
 6. SNTP Server IP Address 2           : 0.0.0.0
    SNTP Server Retries 2              : 3
    SNTP Server Timeout 2 (seconds)    : 5
    SNTP Server Priority 2             : 1

                                    Select [1-6]:
----------------------------------Messages-----------------------------------
```

Figure 3-19. SNTP Client Configuration Screen

1. **SNTP Client UTC Offset (hours)** - Set the difference, in hours, between the local time of the 9145E10G and Coordinated Universal Time (UTC), which is similar to Greenwich Mean Time (GMT); Range is -12 to 12
2. **SNTP Client Observe DST** - Enables/Disables Daylight Savings Time (Summer Time) and the date and time it starts and ends.
3. **SNTP Client Sync Interval (minutes)** - Set how often, in minutes, that the 9145E10G tries to synchronize its time to the SNTP server; Range is 0 (attempt to synchronize at bootup, only) to 1440 (once daily)
4. **SNTP Client Delay Time (seconds)** - Sets the delay for the initial SNTP request. If not zero, the request will be sent at a random interval within the delay time. This is used to prevent multiple NID requests at the same time in the event that all NIDs power down and power up at the same time.
5. **SNTP Server IP Address** - Two SNTP servers can be configured
   - IP Address: Set the address for the SNTP server. IP address 0.0.0.0 indicates no server.
   - Retries: How many times the 9145E10G tries to synchronize before trying the alternate server. 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 9145E10G alternates tries between the servers.

When entries are completed, press **Esc** to return to the System Configuration menu.

3.8 SYSLOG Client Configuration

Use the SYSLOG Client Configuration screen to configure the 9145E10G to send log messages to a SYSLOG Server. From the System Configuration menu, select SYSLOG Client Configuration (**8**) and press **Enter**. The SYSLOG Client Configuration screen (Figure 3-20.) opens.

On the SYSLOG Client Configuration screen, type the number of the SYSLOG setting to change and press **Enter**. When entries are completed, press **Esc** to return to the System Configuration menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------SYSLOG CLIENT CONFIGURATION--------------------------


 1. Syslog Server IP Address : 000.000.000.000
    Syslog Server Port       : 514
    Syslog Server Mask       : Debug

 2. Syslog Server IP Address : 000.000.000.000
    Syslog Server Port       : 514
    Syslog Server Mask       : Debug









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

Figure 3-20. SYSLOG Client Configuration screen

1. **Syslog Server IP Address -** Configure the IP address of the Syslog server. Two Syslog servers can be configured.

2. **Syslog Server Port -** Configure the Syslog Server port. The standard syslog port is 514. The port setting should match with the Syslog server UDP port setting (1 - 65535).

3. **Syslog Server Mask -** Define the level of severity of the messages to be send. There are eight (8) levels of severity as defined in RFC 3164. The severity levels from highest to lowest are:

   - Emergency:
   - System is unusable.
   - Alert:
   - Action must be taken immediately.

- Critical:
- Critical Condition.
- Error:
- Error Condition.
- Warning:
- Warning Condition.
- Notice:
- Normal but significant condition.
- Informational:
- Informational messages.

4. **Debug: -** Debug level messages. If you specify Debug, then all messages are sent about the 9145E10G. If you specify Error, then all errors that are Emergency, Alert and Critical are sent.

3.9 Hardware Information

The Hardware Information screen displays information about the 9145E10G, including the full model number of the 9145E10G, hardware revision level, serial number, power supplies, and port information. From the System Configuration menu, select Hardware Information (**9**) and press **Enter**. The Hardware Information screen (Figure 3-21.) opens.

NOTE: Parameters and values cannot be changed in this screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------HARDWARE INFORMATION------------------------

 NID Model Number          9145E10G-527-2-0
 NID Hardware Rev.         A2
 NID Serial Number         20091009660

 Optic Information    User Port          Network Port       Multipurpose Port
 Model Number         XFP1-3465          XFP1-3465          SFP1-0045
 Wavelength           1550nm SM          1550nm SM          850nm MM
 Connector Type       Duplex LC          Duplex LC          Duplex LC
 Data Rate            10000Mbps          10000Mbps          1000Mbps
 Maximum Line Length  40km               40km               N/A
 Maximum Loss Budget  N/A                N/A                7.5dB

 Power Supply A            AC 120/240
 Power Supply B            AC 120/240

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

Figure 3-21. Hardware Information screen

Chapter 4

Diagnostics

4.0 Diagnostic Functions

From the Main menu (Figure 2-3.), select (2) Diagnostics menu. The Diagnostics menu (Figure 4-1.) opens. The Diagnostics functions to set up loopback, VLAN loopback, latency and jitter testing, and PING tests, are configured and initiated here. The following paragraphs describe each item on the Diagnostics menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------------DIAGNOSTICS-----------------------------



                              1) Loopback Setup
                              2) Latency/Jitter Test
                              3) PING Generation
                              4) VLAN Loopback
                              5) Network Performance


                                    Select [1-5]:





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

Figure 4-1. Diagnostics Menu

4.1 Loopback Setup

The Loopback Setup screen is used to configure and initiate loopback diagnostics. Packets are looped back at the User or Network port based on the Loop Test MAC address of the 9145E10G; all packets not addressed to the Loop Test MAC Address are dropped. The 9145E10G can be configured to swap origination and destination MAC addresses of the test packets and to recalculate the CRC of the looped packet when the MAC addresses are swapped, so the loopback packet can successfully navigate through the network back to the test originator.

At the Diagnostics menu, select Loopback Setup (**1**) and press **Enter**. The Loopback Setup screen (Figure 4-2.) opens. Type the number of the function to change, and press **Enter**. Cycle through the available settings using the **Space Bar.** Once the setting has been selected, press **Enter** to lock it. Continue to modify the settings as required. To return to the Diagnostics menu, press **Esc**.

NOTE: Do not swap the source and destination and recalculate the CRC.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------------------LOOPBACK SETUP----------------------------


 Loop Test MAC Address:         00 40 2A 03 9D 61


 1) Loopback State              Disabled

 2) Swap MAC Address
    at Loopback Point?          Yes

 3) Recalculate CRC
    at Loopback Point?          Yes



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

Figure 4-2. Loopback Setup Screen

4.2 Latency/Jitter Test

The Latency/Jitter Test screen, is used to initiate tests that measure network latency, inter-frame jitter and frame loss from the local 9145E10G to a remote unit. At the Diagnostics menu, select Latency/Jitter Test (**2**) and press **Enter**. The Latency/Jitter Test screen (Figure 4-3.) opens.

NOTE: If the remote unit is a 9145, 9145E, or 9145E10G the latency and jitter test results are more accurate since the time spent in the control plane of the remote unit iscanceled out.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------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
   Far End PBit Sent  0/Rcvd ?             Local PBit Sent  ?/Rcvd ?
   Far End DSCP Sent  0/Rcvd ?             Local DSCP Sent  ?/Rcvd ?

   1) To IP Addr    0.0.0.0                5) Packet Timeout sec (1-10) 3
   2) From IP Addr  Auto Selection         6) Packet Priority (0-7)     0
   3) Test VLAN             0              7) Packet DSCP Code (0-63)   0
   4) Test Packets per sec   1             8) Packet DF Bit             Clear
               9) Test Duration min:sec (0=forever)  0
              10) Min Test Payload Size (40 - 9950)  40
              11) Max Test Payload Size (40 - 9950)  40
              12) Start/Stop Test

                                Select [1-12]:
-----------------------------------Messages-----------------------------------
```

Figure 4-3. Latency/Jitter Test Screen

Beneath the Maximum Latency and Maximum Jitter test results are the Far End P-Bit Sent/Rcvd, Local P-Bit Sent/Rcvd, Far End DSCP Sent/Rcvd, and Local DSCP Sent/Rcvd. This data is used to determine if the programmed Packet Priority or DSCP was changed during the Round Trip between the local 9145E10G and the destination 9145E10G (far end). Only a 9145, 9145E, or 9145E10G destination can provide the Far End PBit/DSCP function.

NOTE: If the DF Bit is clear, the actual maximum packet size is 8192. The DF Bit must be set for oversized packets greater than 1518 (payload size greater than 1472) to be sent or the packet will be fragmented (sent as multiple packets of size 1518).

The leg of the trip (Local to Far End or Far End to Local) on which the P-Bit remarking or DSCP change is occurring will be identified. It is assumed that each Latency/Jitter test that is initiated will take a particular path, so each round trip overwrites the previous round trip values.

1. **Test IP Addr/VLAN -** The destination IP address and VLAN for the currently test or the last test completed.

2. **Round Trip Packets: -** Number of completed round trips.

3. **Test Duration: -** The length of time the test has been running, or the length of the last test run.

4. **Dropped Packets: -** Number of packets sent which received no response.

5. **Minimum Latency (ms) -** Time in ms for the shortest round trip.

6. **Minimum Jitter (ms) -** Smallest absolute time difference between 2 round trips.

7. **Average Latency (ms) -** Computed by adding all the round trip latencies and dividing by the number of completed round trips.

8. **Average Jitter (ms) -** Computed by adding all the absolute time differences between successive round trips and dividing by the number of completed round trips minus 1.

9. **Maximum Latency (ms) -** The highest time interval for a successful round trip.

10. **Maximum Jitter (ms) -** The highest absolute time difference between 2 successful round trips.

11. **Far End PBit Sent -** This is the programmed priority value entered in the far end device..

12. **Far End PBit Rcvd -** This is the priority as it was received at the destination 9145/9145E/9145E10G.

13. **Local PBit Sent -** The programmed priority value is put back into the packet at the far end for the return trip.

14. **Local PBit Rcvd -** This is the priority as it was received at the end of the Round Trip.

15. **Far End DSCP Sent -** This is the programmed DSCP.

16. **Far End DSCP Rcvd -** This is the DSCP that was received at the destination 9145/9145E/9145E10G.

17. **Local DSCP Sent -** The programmed DSCP value is put back into the packet at the far end for the return trip.

18. **Local DSCP Rcvd -** This is the DSCP that was received at the end of the Round Trip.

Type the number of the function you wish to change, and press **Enter**. Once the settings have been entered, select 12 and press **Enter** to begin or end testing. Press **Esc** to return to the Diagnostics menu. Configuration items are as follows:

1. **To IP Address** - Enter the remote agent IP Address.
2. **From IP Address** - Select the originating IP address that the 9145E10G will place into the test packets. Use **Space** to scroll through Auto Selection, Management IP, Test IP, and Aux IP.

   The Auto Selection setting will start first with the Test IP. If the To IP Address is in the Test Network Subnet, the Test IP will be used in the packet. If the Test IP is not available or the To IP Address is not in the Test Network Subnet, the Aux IP is checked. If the Aux IP is not available or the To IP Address is not the Aux Network Subnet, the Manager IP is used. Any address can be used with the Manager IP since it has access to the Default Gateway.

   If the From IP Address is specified as the Test IP or the Aux IP, and the To IP Address is not located in the matching subnet, the destination is unreachable. An error message is displayed when the Start Test command is given.
3. **Test VLAN** - The test packets will carry this VLAN Tag. The Test VLAN can only be changed if the From IP Address is set to the Test IP, or the if Aux Allow Any VLAN is enabled.
4. **Test Packets per sec** - Controls the number of packets that will be sent for every second the test runs. Settings are: 1, 2, 5, 10, 20, 50 or 100.
5. **Packet Timeout sec (1 - 10)** - Set the packet timeout for this test, from 1 to 10 seconds. If a response is not received within this time limit, the packet will be considered dropped.
6. **Packet Priority** - Set packet Priority Code Point (PCP) from 0 to 7, with 0 being the highest priority.
7. **Packet DSCP Code (0 - 63)** - The Differentiated Services Code Point (DSCP) code used to classify packets in a Diffserv network. Other network devices that support Diffserv use the DSCP code in the IP header to select a per hub behavior (PHB) for the packet and provide the appropriate QoS treatment.
8. **Packet DF Bit** - The DF (Don't Fragment) Bit is an identifier in the packet that determines if this packet can be fragmented to smaller packets.
9. **Test Duration min:sec** - Sets the amount of time the test will run in minutes and seconds. A setting of 0 will allow the test to run forever.
10. **Min Test Payload Size (40 - 9950)** - Set the minimum test size, in bytes. The 9145E10G sends test packets ranging in size from the minimum packet setting to the maximum packet setting (sweep), if they are different. The minimum payload size must be less than, or equal to, the maximum payload size. If a sweep is being performed, the size will be incremented by 1 byte for each message sent until the maximum test payload size is reached, the decremented by 1 byte for each message sent until the minimum payload size is reached, then repeated as necessary.
11. **Max Test Payload (40 - 9950)** - Set the maximum test payload size, in bytes. The maximum payload size must be equal to, or greater than, the minimum payload size.
12. **Start/Stop Test -** Start and Stop testing.

4.3 PING Generation

The PING Generation screen (also available from the Utility menu) is used to determine if a destination is reachable from the NID. From the Diagnostics menu, type **3** and press **Enter**. The PING Generation screen (Figure 4-4.) opens.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------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 - 9950) : 40
             6) Ping DF Bit                   : Clear
             7) Start Pinging

                             Select [1-7]:





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

Figure 4-4. PING Generation Screen

1. At the PING Generation screen, select Ping to Address (**1**). Enter the destination IP address and press **Enter**.
2. Select (2) to change the Ping from Address. Use the **Space Bar** to cycle through Test IP (if available), Mgr IP, Aux IP, and Auto Selection. Type **Enter** to lock in a selection. The Auto Selection setting will start first with the Test IP.

   If the Ping to Address is in the Test Network Subnet, the Test IP will be used in the ping packet. If the Test IP is not available or the Ping to Address is not in the Test Network Subnet, the Aux IP is checked. If the Aux IP is not available or the Ping to Address is not the Aux Network Subnet, the Manager IP is used. Any address can be used with the Manager IP since it has access to the Default Gateway.

   If the Ping from Address is specified as the Test IP or the Aux IP, and the Ping to Address is not located in the matching subnet, the destination is unreachable. An error message is displayed when the Start Pinging command is given.
3. Select (3) to enter the Ping Count from 1 to 255 (0 = forever).
4. Select (4) to enter the Ping VLAN ID. The VLAN ID is only writable if the Ping from Address is the Test IP, or the Aux IP if Aux Allow Any VLAN is enabled.

5. Select (5) to enter the Ping Payload Size between 40 and 9950. To send packets greater than 1518 (payload size greater than 1472), the DF (Don't Fragment) bit must be set or the packet will be fragmented (sent as multiple packets of size 1518).
6. Select (6) to change the Ping DF Bit setting. See the Ping Payload size for explanation.

4.4 VLAN Loopback

The VLAN Loopback feature provides the capability for Layer 2 per VLAN loopback. It includes a loopback responder and a loopback initiator (Layer 2 Ping). The frame format and message processing is 802.1ag compatible. Any vendor having implemented the 802.1ag standard can loop back the 9145E10G initiated loopback message and vise versa.

Using the loopback initiator, the 9145E10G can perform a Layer 2 Ping test. For the loopback responder, the 9145E10G implements a set of default values so it can loop back any VLAN ID and any MD level, and the Ethertype will be defaulted to the standard 0x8902.

The user may change the Ethertype via UI, Telnet or SNMP. Both IEEE 802.3 and LLC SNAP formats are supported. The 9145E10G loopback responder responds to both formats. For the loopback initiator, the user selects which format to use.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
--------------------------------VLAN LOOPBACK--------------------------------


                              1) 802.1AG Loopback Configuration
                              2) VLAN Loopback Statistics
                              3) L2 Ping Generator

                                  Select[1-3]









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

Figure 4-5. VLAN Loopback

To configure 802.1ag Loopback, type 1 and press Enter. The 802.1ag Loopback Configuration screen (Figure 4-6) opens.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------802.1AG LOOPBACK CONFIGURATION-----------------------


          1) Administration State           Enabled
          2) VLAN ID (1-4094)               1-4094
          3) MD Level (0-7)                 0-7
          4) Ether Type (4 Hex Digits)      8902

              Select[1-4]:









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

Figure 4-6. 802.1ag Loopback Configuration

1. **Administration State -** To enable or disable the loopback responder, type 1 and press **Enter**. Cycle between Enable and Disable. Press **Enter** to confirm the setting.

2. **VLAN ID -** This is the VLAN ID to match for responding to LBMs (Loopback Messages initiated by another agent).

To enter a VLAN ID or a range, type 2 and press **Enter**. Use Backspace to remove the current setting, then type in the VLAN ID or range. Press **Enter** to confirm the setting.

3. **MD Level -** This is the Maintenance Domain (MD) Level to match for responding to LBMs.

To change the Maintenance Domain (MD) Level, type 3 and press **Enter**. Use Backspace to remove the current setting, then type in the new setting. Press **Enter** to confirm the setting.

4. **Ether Type -** This is the ethertype to match for responding to LBMs. 0000 indicates any ethertype except IP ethertype (0x800). The default is 8902.

To change the Ether Type, type 4 and press **Enter**. Use Backspace to remove the current setting, then type in the new setting. Press **Enter** to confirm the setting. Press **Esc** to return to the VLAN Loopback menu.

4.4.1 VLAN Loopback Statistics

To view current VLAN loopback statistics, type 2 and press **Enter**. The VLAN Loopback Statistics (Current) screen (Figure 4-8) opens. Press **Ctrl+S** to clear the current counters. Press **Ctr+T** to view the raw counters.

Press ESC to return to the Loopback Configuration screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------VLAN LOOPBACK STATISTICS (CURRENT)-----------------------


                                        User Port           Net Port

     LBM Transmitted:                   0                   0
     LBM Received:                      0                   0
     LBM Mismatched:                    0                   0
     LBR Transmitted:                   0                   0
     LBR Received:                      0                   0
     LBR Out Of Sequence:               0                   0
     LBR Unexpected:                    0                   0

      Enter Control-R to Clear, Control-T to Raw Counter, ESC to Exit:




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

Figure 4-7. VLAN Loopback Statistics Screen

1. **LBM Transmitted: -** Total LBMs (LoopBack Messages) transmitted since last statistics clear.

2. **LBM Received: -** Total valid LBMs received since last statistics clear.

3. **LBM Mismatched: -** Total LBMs received that mismatched the configuration and were discarded since last statistics clear.

4. **LBR Transmitted: -** Total LBRs (LoopBack Responses) transmitted since last statistics clear.

5. **LBR Received: -** Total valid LBRs received since last statistics clear.

6. **LBR Out Of Sequence: -** Total LBRs received that were out of sequence since last statistics clear.

7. **LBR Unexpected: -** Total LBRs received that were unexpected.

4.4.2 L2 Ping Generator

To set up the L2 Ping generator, type **3** and press **Enter**. The L2 Ping Generator screen (Figure 4-9) appears. Run the test by selecting 13. This will give you all the statistics that are described below.

1. **Destination MAC Address -** MAC address that the LBMs will be sent to.
2. **VLAN ID: -** VLAN ID to be put in the LBM.
3. **VLAN Priority: -** Priority to be put in VLAN tag.
4. **Ethertype: -** Ethertype to be put in the LBM.
5. **MD Level: -** MD level to be put in the LBM.
6. **Egress Port: -** Port that the LBMs will be sent out.
7. **Frame Count: -** Number of LBMs to be sent out.
8. **Frame Size: -** Frame size of the LBM to be built, excluding 4 bytes CRC.
9. **Frame Interval: -** Time interval between two LBMs to be sent out. 0-500 in 10 ms intervals may be specified. 0 indicates as fast as possible.
10. **Frame Format: -** Frame to be sent out in IEEE 802.3 or LLC SNAP format.
11. **Start L2 Ping: -** Start to send out the LBM and verify the responses. The status will be shown. You may stop the testing by entering the ESC key.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------L2 PING GENERATOR------------------------------
               1) Destination MAC Address            00-00-00-00-00-00
               2) VLAN ID (1-4094)                   1
               3) VLAN Priority (0-7)                0
               4) Ethertype (4 Hex digits)           8902
               5) MD Level (0-7)                     7
               6) Egress Port                        Net
               7) Frame Count (1-99999999)           1
               8) Minimum Frame Size (60-9996)       60
               9) Maximum Frame Size (60-9996)       1514
              10) Incremental Size (0-256)           0
              11) Frame Time Interval (0-500 10ms)   0
              12) Frame Format                       IEEE 802.3
              13) Start L2 Ping

                  Select[1-13]:

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

Figure 4-8. L2 Ping Generator Statistics Screen

After starting a Layer 2 Ping, the following statistics will appear on the bottom half of the screen:

1. **First Transaction ID: -** Transaction identifier for the first LBM sent out in this test.
2. **LBM Transmitted: -** Number of LBMs sent out in this test.
3. **LBR Received: -** Number of valid LBRs been received in this test.
4. **LBR Out Of Sequence: -** Number of LBRs been received in this test, which are out of sequence.
5. **LBR Unexpected: -** Number of unexpected LBRs received during this test.

4.5 Network Performance

The Canoga Perkins' Performance Collection System (PCS) is a suite of tools that permits the monitoring and collection of network performance attributes, namely Frame Delay (FD), Frame Delay Variation (FDV), Frame Loss Ratio (FLR), and Availability. Network performance and availability reports may be generated to determiney if the service objectives were met. Below is a brief description of the three netwrok perfromance functions. For detailed instructions on setting up and using these functions, please reference the CanogaView Service Level Agreement User Guide, product number 6912641.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------NETWORK PERFORMANCE------------------------------

                              1) Profile
                              2) Address List
                              3) Test Distribution Connection
                              4) Trap Configuration
                              5) Statistics
                              6) PM Scheduler
                              7) PM Test Results
                              8) PM Manual Test
                              9) SAM Scheduler
                             10) SAM Results Log
                             11) Protected Link PM




                              Select [1-11]:                                -
----------------------------------Messages-----------------------------------
```

Figure 4-9. Network Performance Screen

Chapter 5

Port Information

5.0 Port Description

The Port Information screen (Figure 5-1.) provides a description and a graphic depiction of the User, Network, Multipurpose and Management ports for the 9145E10G, 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 and settings.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
--------------------------------PORT INFORMATION------------------------------
 ____________________________________________________________________________
|  Canoga Perkins                                          mgmt utp            |
|  _________________   _________________   _________________    _____         |
| |                 | |                 | |lnk spd lnk spd|            o lnk/act |
| |                 | |                 | | o   o   o   o |    off     o spd     |
| |  _____          | |  _____          | |          _____ |                     |
| | |     | o lnk   | | |     | o lnk   | | _____   |     ||  _______   Y power   |
| | |_____| o spd   | | |_____| o spd   | ||_____| |_____||  \:::::/   R status  |
| |      xfp        | |      xfp        | |  sfp     utp  |                     |
| |   USER PORT     | | NETWORK PORT    | | MULTIPURPOSE  |          9145E10G-527|
|_|_________________|_|_________________|_|_________________|______________________|


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

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

Figure 5-1. Port Information Screen

5.1 Link Status

Link Status informs you of the current link status of the User, Network, and Management UTP ports of the 9145E10G and provides information on User and Network Port XFP transmit (Tx) and receive (Rx) power. From the Port Information screen (Figure 5-1.), select Link Status (**1**) and press **Enter.** The Link Status screen (Figure 5-2.) opens. The Link Status screen provides transmissions counters for each port. These counters illustrate how many LinkDown/LinkUp transitions have occurred at each port. To reset the counter, press CTRL-R. Press **Esc** to return to the Port Information screen.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------------------LINK STATUS-----------------------------------
                              Link State       Transitions
                              ----------       -----------
 User Port                    Link Up               0
 Network Port                 Link Up               0
 MP Port (Gig)                Admin Up              0
 MGMT UTP Port                Admin Down            0

 Optic Status:
    User XFP Rx Power         No Power
    User XFP Tx Power         -2.0dBm
    Network XFP Rx Power      -2.2dBm
    Network XFP Tx Power      -2.6dBm
    MPP SFP Rx Power          -4.8dBm
    MPP SFP Tx Power          No Power


      CTRL-R to Reset the Link State Transition count or ESC to go back
-------------------------------------Messages-----------------------------------
```

Figure 5-2. Link Status Screen

5.2 Port Configuration

Use the Port Configuration functions to obtain hardware information, view and modify the functional and VLAN configurations, manage the various port filters, and to add, delete, and edit VLAN controls.

At the Port Information screen (Figure 5-1.), select Port Configuration (**2**) and press **Enter.** The Port Configuration screen opens. The following paragraphs describe each item on the Port Configuration menu. Press **Esc** to return to the Port Information screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------PORT CONFIGURATION-----------------------------



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

                              Select [1-5]:





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

Figure 5-3. Port Configuration Menu

5.2.1 Hardware Information

The Hardware Information screen (Figure 5-4.) provides 9145E10G hardware information such as Model number, hardware revision, and serial number for the 9145E10G.

To review hardware information, select Hardware Information (**1**) from the Port Configuration menu. This is an informational screen only.

5.2.2 Functional Configuration

From the Port Configuration menu, select the Functional Configuration (**2**) and press **Enter**. The Functional Configuration screen opens. The Functional Configuration screen (Figure 5-5.) displays the User and Network port speed and duplex information, and allows the customer to set the functions listed below.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------HARDWARE INFORMATION-----------------------

 NID Model Number          9145E10G-527-2-0
 NID Hardware Rev.         A2
 NID Serial Number         20091009660

 Optic Information    User Port          Network Port       Multipurpose Port
 Model Number         XFP1-3465          XFP1-3465          SFP1-0045
 Wavelength           1550nm SM          1550nm SM          850nm MM
 Connector Type       Duplex LC          Duplex LC          Duplex LC
 Data Rate            10000Mbps          10000Mbps          1000Mbps
 Maximum Line Length  40km               40km               N/A
 Maximum Loss Budget  N/A                N/A                7.5dB

 Power Supply A            AC 120/240
 Power Supply B            AC 120/240

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

Figure 5-4. Hardware Information Menu

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------------FUNCTIONAL CONFIGURATION--------------------

  User Port Speed/Duplex          Link Down
  Net Port Speed/Duplex           10000M/Full
  MP Port Speed/Duplex (Gig)      Admin down
  MGMT UTP Port Speed/Duplex      Admin down

  1) User Port Setting            10000M Full
  2) Net Port Setting             10000M Full
  3) RMTF                         Disabled
  4) LLF                          Disabled
  5) Flow Control                 Disabled
  6) Maximum Frame Size           10000



                                  Select [1-6]:
-------------------------------------Messages----------------------------------
```

Figure 5-5. Functional Configuration Menu

1. **User Port Setting** - This sets the port to either Disabled or Enabled at 10G Full speed.

2. **Net Port Setting** - This sets the port to either Disabled or Enabled at 10G Full speed.

3. **RMTF** - Remote Fault (RMTF) allows an alarm to be transmitted to the link partner to indicate loss of signal on receive. When a link loss is detected, the port stops transmitting service traffic on the port and begins to transmit the Remote Fault signal so the connected link knows the link is no longer operational.

    a. A port that is receiving Remote Fault is treated as if the link is down for purposes of Link Loss Forwarding and alarming. Even though the link is still up, only Remote Fault is being received and service traffic is not flowing. Once the link fault is corrected, Remote Fault transmission is automatically terminated and service traffic flow will resume.

    b. Use the Space Bar to cycle between User Port Enabled, Net Port Enabled, Both Ports Enabled, and Disabled.

4. **LLF** - Enables or disables Link Loss Forwarding (LLF). Link Loss Forwarding allows the 9145E10G to signal attached equipment that a link has gone down by bringing down the attached link.

    a. If User->Network is selected, if the User Port link is down, the Network Port will be disabled.

    b. If Network->User is selected, the User Port will be disabled if the Network Port goes down.

    c. If Both Directions is selected, either port can bring down the other port. LLF can only be active in one direction at a time, however. When the original link is restored, the partner link is also restored.

    d. Use the Space Bar to cycle between User->Network, Network->User, Both Directions, or Disabled.

5. **Flow Control** - Flow Control is not Supported in the 9145E10G.

6. **Maximum Frame Size -** Sets the maximum allowable Ethernet Frame size the 9145E10G will forward for both ports. Frames exceeding the Maximum Frame Size will be counted as Oversize Packets and will be dropped. Frames destined for the 9145E10G Manager are exempt from the limit. Enter the Maximum Frame Size between 1518 and 10000.

5.2.3 VLAN Configuration

From the Port Configuration menu, select VLAN Configuration (**3**) and press **Enter.** The VLAN Configuration screen (Figure 5-6.) opens. Use the VLAN Configuration menu to display and configure the VLAN parameters. When all VLAN functions have been set, press **Esc** to return to the Port Configuration menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-------------------------------VLAN CONFIGURATION-----------------------------



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


                              Select [1-3]:









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

Figure 5-6. VLAN Configuration Menu

5.2.3.1 VLAN Rules

From the VLAN Configuration screen, select VLAN Rules (**1**) and press **Enter** to access the VLAN Rules screen. Use the VLAN Rules screen (Figure 5-1) to configure the VLAN parameters listed below.

Type the item number to change and press **Enter**. Use **Tab** or **Enter** to change columns. Use the **Space Bar** to cycle between Yes and No. Type VLAN IDs and Priorities into the designated areas. Press **Enter** to accept changes. When all VLAN parameters have been set, press **Esc** to return to the VLAN Configuration menu. **NOTE: *Service frames*** do not include traffic destined to the 9145E10G Management host.

1. **Drop Untagged Packets?** - The 9145E10G will discard all Service frames received on the User or Network port that do not have a VLAN Tag. Selecting *Yes* discards packets.

2. **Drop Packets with VLAN Tag not matching VLAN Tag A?** - The 9145E10G discards all Service frames received on the User or Network port that do not have a VLAN Tag matching VLAN Tag A. Selecting *Yes* discards packets.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------------VLAN RULES----------------------------------
                                   User Port   Net Port
 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 - 4094)           0          0
 8)  Tag B VLAN ID (0 - 4094)           0          0
           Priority (0 - 7)             0          0
 9)  Tag C VLAN ID (0 - 4094)           0          0
           Priority (0 - 7)             0          0
                                  Select [1-9]:
-----------------------------------Messages-----------------------------------
```

Figure 5-7. VLAN Rules Screen

3. **Remove outermost VLAN Tag?** - Removes the outermost VLAN Tag from packets received on the User or Network port. Takes no action on untagged packets. *Yes* removes outermost tag.

4. **Add VLAN Tag B to Untagged Packets only?** - *Yes* adds VLAN Tag B to all untagged packets received on the User or Network port.

5. **Add VLAN tag C to tagged packets only?** - *Yes* adds VLAN Tag C to all tagged packets received on the User or Network port.

6. **Add VLAN Tag C to Tagged Packets only using P-Bits of outermost VLAN tag?** - *Yes* adds VLAN Tag C to all tagged packets received on the User or Network port, using the same priority bit as the inner tag of the packets.

7. **Tag A VLAN ID (0-4094)** - Sets VLAN ID for Tag A. The ID range 0 - 4094 is valid.

8. **Tag B VLAN ID (0-4094)** - Sets VLAN ID for Tag B. The ID range 0 - 4094 is valid.

9. **Priority (0 - 7)** - Sets P-Bit of VLAN Tag B. Values of 0-7 are Valid.

10. **Tag C VLAN ID (0-4094)** - Sets VLAN ID for Tag C. ID setting of 0 - 4094 are valid.

11. **Priority (0 - 7)** - Sets P-Bit of VLAN Tag C. Values of 0-7 are Valid.

5.2.3.2 Port VLAN ID Translation Table

The 9145E10G has the ability to translate customer VLAN Tag IDs on Service frames. Use the Port VLAN ID Translation Table to configure outgoing packets to receive a new tag based on the current outermost tag. The tag is changed in both directions.

To Configure VLAN Translations, from the VLAN Configuration menu, select Port VLAN Translation Table (**2**) and press **Enter**. The Port VLAN ID Translation Table (Figure 5-1.) opens.

1. **Enable VLAN Translation - -** Type 1 and press Enter. Use the Space Bar to cycle between Yes and No.

2. **Add/Delete/Modify VLAN Translation -** Type **2** and press **Enter**. Type in the In VLAN number and press **Enter.** Then type in the Out VLAN number and press **Enter**. The In VLAN/Out VLAN number combination will be added to the list on the screen, in numerical order.

3. **Check If VLAN In Translation Table -** Type **3** and press **Enter**. Type in the VLAN number. A message will open at the bottom of the screen, saying either *VLAN xx is not in the table* or *VLAN xx is mapped to VLAN xx*.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------PORT VLAN ID TRANSLATION TABLE----------------------
                            Page 1 of 3 Total 91 entries
  User <=> Network    User <=> Network    User <=> Network    User <=> Network
  ----------------    ----------------    ----------------    ----------------
   10 <=> 1000          20 <=> 1010          30 <=> 1020        40 <=> 1030
   11 <=> 1001          21 <=> 1011          31 <=> 1021        41 <=> 1031
   12 <=> 1002          22 <=> 1012          32 <=> 1022        42 <=> 1032
   13 <=> 1003          23 <=> 1013          33 <=> 1023        43 <=> 1033
   14 <=> 1004          24 <=> 1014          34 <=> 1024        44 <=> 1034
   15 <=> 1005          25 <=> 1015          35 <=> 1025        45 <=> 1035
   16 <=> 1006          26 <=> 1016          36 <=> 1026        46 <=> 1036
   17 <=> 1007          27 <=> 101           37 <=> 1027        47 <=> 1037
   18 <=> 1008          28 <=> 1018          38 <=> 1028        48 <=> 1038
   19 <=> 1009          29 <=> 1019          39 <=> 1029        49 <=> 1039
      1) Enable VLAN Translation:     Yes
      2) Add/Delete/Modify VLAN Translation
      3) Check If VLAN In Translation Table
                                  Select [1-3]:
  CTRL-D: page down, CTRL-U: page up, CTRL-T: toggle view from user/network
-----------------------------------Messages-----------------------------------
```

Figure 5-8. Port VLAN ID Translation Table

5.2.3.3 P-Bit Translation Table

The 9145E10G can change the P-Bit setting in VLAN ID tags on Service frames to change their priority status in the network. To change incoming Priority Bit Translations, type **3** and press **Enter**. The P-Bit Translation Table (Figure 5-9.) opens.

1. To modify the P-Bit translation data, type the number of the P-Bit you wish to translate, from 1 to 8, and press **Enter**. Enter the P-Bit value and press **Enter**. Use **Tab** to switch between ports. The P-Bit will be changed on the ingress direction for the port. Press **Enter** to confirm changes. Press **Enter** to confirm changes.

2. To Enable or Disable P-Bit translation, type **9**, press **Enter**, and use the **Space Bar** to select between Yes and No. Use **Tab** to switch between ports.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------P-BIT TRANSLATION TABLE-------------------------


                                   User Port   Net Port

 1) Incoming P-Bit 0 translated to     0          0
 2) Incoming P-Bit 1 translated to     1          1
 3) Incoming P-Bit 2 translated to     2          2
 4) Incoming P-Bit 3 translated to     3          3
 5) Incoming P-Bit 4 translated to     4          4
 6) Incoming P-Bit 5 translated to     5          5
 7) Incoming P-Bit 6 translated to     6          6
 8) Incoming P-Bit 7 translated to     7          7

 9) P-Bit Translation Enabled?         No         No

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

Figure 5-9. P-Bit Translation Table

5.2.4 Port Filters

Use Port Filters to set filters on the User and Network ports to filter certain management and control Ethernet frames from the data stream and control traffic coming in or out of specific ports.

To configure the port filters, select Port Filters (**4**) from the Port Configuration menu and press **Enter**. The Port Filters screen (Figure 5-10) opens. To set the port filters, type the filter item number, 1 through 6, and press **Enter**.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------------PORT FILTERS--------------------------------



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


                                  Select [1-6]:





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

Figure 5-10. Port Filters Screen

1. **PVST+ BPDU Filter** - When enabled, the 9145E10G will discard PVST+ BPDU frames received on the specified port. Use the **Space Bar** to select User Port Enabled, Net Port Enabled, Both Ports Enabled, or Disabled.

2. **User Port Manager MAC Filter** - When enabled, the 9145E10G will block packets entering the unit which have the unit's MAC address as the source MAC Address. This prevents spoofing of Management frames. Use the **Space Bar** to cycle between User Port Enabled and Disabled.

3. **User Port Test Network Filter** - When enabled, the 9145E10G will inspect and discard all packets entering its User port that have a source IP address on the same subnet mask as the Test network. This prevents spoofing of test packets. Use the **Space Bar** to cycle between User Port Enabled and Disabled.

4. **802.3ah OAM PDU Filter** - When enabled, the 9145E10G will block 802.3ah OAM PDU frames from being generated from or passed through the unit. If the user intends to use OAM, this filter must be disabled. Use the **Space Bar** to cycle between Enabled and Disabled.

5. **UDLD Filter** - When enabled, the 9145E10G will block Cisco Systems proprietary tagged and untagged UDLD frames from passing through the unit. Use the **Space Bar** to cycle between Enabled and Disabled.

6. **Management VLAN Filter** - When enabled, the 9145E10G will block traffic that is tagged with the Management VLAN on the specified port. This will not affect management packets that are addressed to the 9145E10G. Use the **Space Bar** to cycle between Disabled, User Port Enabled, Net Port Enabled and Both Ports Enabled.

5.2.5 Port Based VLAN Control

The Port Based VLAN Control screen (Figure 5-11.) is used to specify which VLANs, if any, are allowed to pass through each port. The 9145E10G can be configured to support up to 100 VLANs.

From the Port Configuration screen, select Port Based VLAN Control (**5**) and press **Enter**. The Port Based VLAN Control screen (Figure 5-11.) opens. The default setting is All VLANs Allowed. In order to specify which VLANs will be included or excluded, use the Add, Add Range, Delete, and Delete Range controls at the bottom of the screen. Use **Esc** to return to the Port Based VLAN Control screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------PORT BASED VLAN CONTROL----------------------------
Port Based VLAN Control List:

     2        12      22      32      42      54      64      75      85
     3        13      23      33      43      55      65      76      86
     4        14      24      34      44      56      66      77      87
     7        17      27      37      49      59      69      80      90
     8        18      28      38      50      60      71      81      91
     9        19      29      39      51      61      72      82      92
    10        20      30      40      52      62      73      83
    11        21      31      41      53      63      74

                          PBVC Mode: Disabled

Select [(1) PBVC Mode, (2) Add, (3) Add Range, (4) Delete, (5) Delete Range]:

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

Figure 5-11. Port Based VLAN Control Screen

1. **PBVC Mode** - This setting determines which ports are enabled. Use the **Space Bar** to select User Port Enabled Only, Net Port Enabled Only, Both Ports Enabled, or Disabled. A setting of Disabled will allow all VLANs to pass through both ports.

2. **Add** - This function is used to add one VLAN ID at a time to the screen list. Enter the VLAN ID you want to add and press **Enter**. The value must be between 2 and 4094.

3. **Add Range** - This function is used to add a group of VLAN IDs to the screen list. Enter the group of VLAN IDs you want to add and press **Enter**. The value must be between 2 and 4094.

4. **Delete** - This function is used to remove one VLAN ID at a time from the screen list. Enter the VLAN ID you want to remove and press **Enter**. The value must be between 2 and 4094.

5. **Delete Range** - This function is used to remove a group of VLAN IDs from the screen list. Enter the group of VLAN IDs you want to remove and press **Enter**. The value must be between 2 and 4094.

5.3 Layer 2 Statistics

To view Layer 2 statistics, select Layer 2 Statistics (**3**) from the Port Information screen (Figure 5-1.) and press **Enter**. The Layer 2 Statistics screen (Figure 5-12.) opens. Use the controls as listed to view the Layer 2 Statistics screen. Press **Esc** to return to the Port Information screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------LAYER 2 STATISTICS (CURRENT)-------------------------

                         User Port       Net Port       MPP Port
 Link State             ** DOWN **         UP         ** DOWN **
 Speed/Duplex               N/A       10000M/FULL         N/A

 Frames Sent                     0         105466              0
 Frames Rcvd                     0       31806714              0
 Bytes Sent                      0       13305612              0
 Bytes Rcvd                      0    43479287658              0
 Frames > 1518                   0              0              0
 Frames > 1522                   0              0              0
 Line Rate Utilization           0%             0%             0%

 Last Counter Reset: 1 day 18:34:08

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

Figure 5-12. Layer 2 Statistics Screen

1. **Change Counter Frame Size -** The 9145E10G has a programmable counter for frames greater than the programmed size. Type **C** and press **Enter**. Type in the desired frame size, between 64 and 10,000, and press **Enter** to accept change.

2. **Error Counters -** Type **E** and press **Enter** to view the Layer 2 Error Statistics screen (Figure 5-13.).

3. **Frame Type Counters -** Type **T** and press **Enter** to view the Layer 2 Frame Type Statistics screen (Figure 5-14.).

4. **Raw Counters -** These are the total counters since the last time the 9145E10G was reset. Press **Ctrl+T** to view raw layer 2 statistics.

5. **Reset Counters -** Press **Ctrl+R** to reset the counters. The counters are reset independently of the raw counters. The raw counters can not be cleared.

6. **Frame Counters -** Press F (available on Layer 2 Error Statistics and Layer 2 Frame Type Statistics menus) to return to the Layer 2 Statistics screen.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------LAYER 2 ERROR STATISTICS (CURRENT)-----------------------
                         User Port       Net Port       MPP Port
 Link State             ** DOWN **         UP         ** DOWN **
 Frames Sent                     0         106335              0
 Frames Rcvd                     0       31827656              0
 Collisions                      0              0              0
 Late Collisions                 0              0              0
 Alignment Errors                0              0              0
 Undersize < 64                  0              0              0
 Oversize > 10000                0              0              0
 Fragments                       0              0              0
 CRC Errors                      0              0              0
 Jabber Events                   0              0              0
 Dropped                         0              0              0

 Last Counter Reset: 1 day 18:36:20

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

Figure 5-13. Layer 2 Error Statistics Screen

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
--------------------LAYER 2 FRAME TYPE STATISTICS (CURRENT)--------------------
                         User Port       Net Port       MPP Port
 Link State             ** DOWN **         UP         ** DOWN **
 Frames Sent                     0         107119              0
 Frames Rcvd                     0       31844414              0
 Rx Broadcasts                   0        1867551              0
 Tx Broadcasts                   0              0              0
 Rx Multicasts                   0         113056              0
 Tx Multicasts                   0            682              0
 VLAN Tagged                     0              0              0
 Pause Frames                    0              0              0
 Filtered Frames                 0              0              0
 Rx Management                   0          88546              0
 Tx Management                   0         107119              0

 Last Counter Reset: 1 day 18:38:07

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

Figure 5-14. Layer 2 Frame Type Statistics Screen

5.3.1 Layer 2 Counter Definitions

The following are definitions of the counters encountered on the Layer 2 Error Statistics screen (Figure 5-13.) and Layer 2 Frame Type Statistics screens (Figure 5-14.).

5.3.1.1 Layer 2 Statistics

Frames Sent - reports the total number of frames sent from the interface since the last reset (Raw) or the last counter reset (Current).

Frames Rcvd - reports the total number of valid frames received on the interface since the last reset (Raw) or the last counter reset (Current).

Bytes Sent - reports the total number of bytes transmitted from the interface since the last reset (Raw) or the last counter reset (Current).

Bytes Rcvd - reports the total number of valid bytes received on the interface since the last reset (Raw) or the last counter reset (Current).

Frames > 1518 - reports the number of frames received on the interface that had a length (excluding framing bits, but including the CRC) of 1519 or higher.

Frames > Limit - reports the number of frames received on the interface that had a length that exceeded the user-defined Frame Size.

Line Rate Utilization - This is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.

5.3.1.2 Layer 2 Error Statistics Screen

Frames Sent - reports the total number of frames sent from the interface since the last reset (Raw) or the last counter reset (Current).

Frames Rcvd - reports the total number of valid frames received on the interface since the last reset (Raw) or the last counter reset (Current).

Collisions - reports the number of collisions that the interface encountered when attempting to transmit a frame over a half duplex connection. The 9145E10G is full duplex, so this counter will always show 0.

Late Collisions - reports the number of collisions that the interface encountered later than 512 bit-times into the frame when attempting to transmit a frame over a half duplex connection. The 9145E10G is full duplex, so this counter will always show 0.

Alignment Errors - reports the number of frames received on the interface that had a non-integral number of octets and a bad CRC. The interface will discard the frame.

Undersize < 64 - reports the number of frames received on the interface that were less than 64 bytes in length (excluding framing bits, but including the CRC), and were otherwise well formed. The interface will discard the frame.

Oversize > MaxFrameSize- reports the number of frames received on the interface that had a length (excluding framing bits, but including the CRC) greater than the Maximum Frame Size set for the unit, inclusive.

See the Functional Configuration screen for information on how to set the Maximum Frame Size. The interface will discard the frame.

Fragments - reports the number of frames received on the interface that were not an integral number of bytes in length or that had a bad CRC, and were less than 64 bytes in length (excluding framing bits but including the CRC). The interface will discard the frame.

CRC Errors - reports the number of frames received on the interface that had a length (excluding framing bits, but including the CRC) of between 64 and the Maximum Frame Size, inclusive, but had a bad CRC. The interface will discard the frame.

Jabber Events - reports the number of frames received on the interface that had a length greater than 1518 and had a bad CRC. This follows the definition in the RMON RFC.

Dropped - reports the number of frames that the interface was unable to transmit due to buffer overflow, link failure, or due to some of the filter settings.

5.3.1.3 Layer 2 Frame Type Statistics

Frames Sent - reports the total number of frames sent from the interface since the last reset (Raw) or the last counter reset (Current).

Frames Rcvd - reports the total number of valid frames received on the interface since the last reset (Raw) or the last counter reset (Current).

Rx Broadcasts - reports the number of broadcast frames received on the interface.

Tx Broadcasts - reports the number of broadcast frames transmitted by the interface.

Rx Multicasts - reports the number of multicast frames received on the interface.

Tx Multicasts - reports the number of multicast frames transmitted by the interface.

VLAN Tagged - reports the number of VLAN tagged frames received on the interface.

Pause Frames - reports the number of PAUSE frames received by the interface.

Filtered Frames - reports the number of frames received on the interface that were dropped due to filtering rules.

Rx Management - reports the number of frames received on the interface that were passed to the 9145E10G manager.

Tx Management - reports the number of frames received from the 9145E10G manager that were passed to the interface.

5.4 RMON Group 1 Statistics

To view Remote Monitoring Specification (RMON) statistics, select RMON Group 1 Statistics (**4**) from the Port Information screen (Figure 5-1.) and press **Enter**. The RMON Group 1 Statistics screen (Figure 5-15.) opens.

Follow the instructions at the bottom of the RMON Group 1 Statistics screen to view the information listed below. Press **Esc** to return to the Port Information screen.

1. **Select More -** Type **M** and press **Enter** to page through all available screens. By clicking on (M) More you will see a second screen with additional RMON stats parameters.

2. **Raw Counters -** Type **Ctrl+T** to view the raw RMON Group 1 Statistics.

3. **Reset Counters -** Press **Ctrl+R** to reset the counters. The counters are reset independently of the raw counters. The raw counters can not be cleared.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------RMON GROUP 1 STATISTICS (CURRENT)-----------------------

                         User Port       Net Port       MPP Port
 Link State             ** DOWN **         UP         ** DOWN **
 Speed/Duplex               N/A       10000M/FULL         N/A

 Packets Rcvd                   0       31917675              0
 Octets Rcvd                    0    43615136511              0
 Broadcasts Rcvd                0        1872480              0
 Multicasts Rcvd                0         113395              0
 Pkts 64                        0        2081339              0
 Pkts 65-127                    0         348965              0
 Pkts 128-255                   0         538912              0
 Pkts 256-511                   0         300446              0
 Pkts 512-1023                  0         229461              0
 Pkts 1024-1518                 0       28418552              0

 Last Counter Reset: 1 day 18:45:02

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

Figure 5-15. RMON Group 1 Statistics Screen

5.4.1 RMON Group 1 Statistics

1. **Packets Rcvd -** reports the total number of packets (including bad packets, broadcast packets, and multicast packets) received.

2. **Octets Rcvd -** reports the total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).

3. **Broadcasts Rcvd -** reports the total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

4. **Multicasts Rcvd -** reports the total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

5. **Pkts 64 -** reports the total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

6. **Pkts 65-127 -** reports the total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

7. **Pkts 128-255 -** reports the total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

8. **Pkts 256-511 -** reports the total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

9. **Pkts 512-1023 -** reports the total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

10. **Pkts 1024-1518 -** reports the total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

11. **Drop Events -** reports the total number of events in which packets were dropped by the probe due to lack of resources. Note that this number is not necessarily the number of packets dropped; it is just the number of times this condition has been detected.

12. **CRC/Align Errors -** reports the total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

13. **Undersize -** reports the total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

14. **Oversize -** reports the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

15. **Fragments -** reports the total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).

NOTE: It is entirely normal for Fragments to increment. This is because it counts both runts (which are normal occurrences due to collisions) and noise hits.

16. **Jabbers -** reports the total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The allowed range to detect jabber is between 20 ms and 150 ms.

17. **Collisions -** reports the best estimate of the total number of collisions on this Ethernet segment.

Chapter 6

System Alarms & Logs

6.0 System Alarms

Use the System Alarms Screen to view alarms and faults on the 9145E10G.

To view alarm status, select System Alarms (**4**) from the Main Menu and press **Enter**. The System Alarms Screen (Figure 6-1.) opens. Press **Esc** to return to the Main Menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------------SYSTEM ALARMS-----------------------------
                                   Link         Remote Fault  Optic Transmitter
 User Port                      *** Down ***       No               OK
 Network Port                   Up                 No               OK
 MP Port (Gig)                  Disabled           N/A              N/A
 MGMT UTP Port                  *** Down ***

 Link Loss Fwd User->Net        No
 Link Loss Fwd Net->User        No

 AC 120/240 PS A Status         OK    5.22 Volts Output (4.83 < OK < 5.49)
 AC 120/240 PS B Status         Bad   0.00 Volts Output (4.83 < OK < 5.49)
 Main Board Voltages            All mainboard voltages OK
 Fan Status                     Both Fans Ok
 Temperature Status             OK 29.5C  (0.0C < OK < 70.0C)


                       Hit 'ESC' to return to previous menu
----------------------------------Messages-------------------------------------
```

Figure 6-1. System Alarm Screen

6.1 System Log

The System Log lists all events that occurred since the last power-up or since the log was last cleared. The log lists items with the most current item at the top. As events fill the System Log, older events drop off. The Event Types include:

1. **System -** involves system-level resources
2. **Trap -** also reported to the Network Manager
3. **Security -** shows security information and violations. An asterisk (*) Local event indicates that the user has an account defined on the local User Account screen.
4. **Config -** shows configuration changes and username of entity that made the change.

To view the System Log, select System Log (**5**) from the Main Menu and press **Enter**.

To page through the entries, type **F** for the first page, type **N** for the next page, type **P** for the previous page or type **L** for the last page. To go to a specific event number (for example: entry number 2457) type **G**, and then type the entry number. To clear the system log, type **C**.To return to the Main Menu, press **Esc**.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------SYSTEM LOG-----------------------------------
Description                    Type      Username   Local  Date/Time
           Displaying 839 to 846 of 846 filtered entries, 846 total
Changed SNTP DST ends at: 30-JAN-2010 00:00:00
                               Config    SYSTEM       *    14-JAN-2010 21:03:35.90
Changed SNTP server 1 IP: 172.16.1.10
                               Config    SYSTEM       *    14-JAN-2010 21:03:35.00
Changed SNTP server 2 IP 172.16.14.200
                               Config    SYSTEM       *    14-JAN-2010 21:03:35.20
System time set by SNTP: 15-JAN-2010 11:23:01
                               System    SYSTEM       *    15-JAN-2010 11:23:01.20
Changed Syslog destination IP 1: 172.16.14.200
                               Config    SYSTEM       *    15-JAN-2010 11:23:56.00
Changed Syslog destination mask 1: Error
                               Config    SYSTEM       *    15-JAN-2010 11:23:56.00
Changed Syslog destination IP 2: 172.16.1.10
                               Config    SYSTEM       *    15-JAN-2010 11:23:56.10
Changed Syslog destination mask 2: Critical
                               Config    SYSTEM       *    15-JAN-2010 11:23:56.10
Select [(F)irst, (N)ext, (P)rev, (L)ast, (G)oto, (C)lear, (S)elect Filter]:
----------------------------------Messages--------------------------------------
```

Figure 6-2. System Log Screen

6.1.1 Log Display Filter Configuration

Sometimes it would be helpful to only look at events that occurred around a certain date, configuration undertaken by a particular user, just view trap events, etc. The 9145E10G has a flexible System Log Display Filter to turn off display of log items that are not of interest to the user.

NOTE:If the Master filter is set to OFF, no filter changes will be applied.

The Log Display Filter Configuration screen (Figure 6-3.) allows the customer to reconfigure the log display filter settings. From the System Log screen, type **S** and press **Enter**. The Log Display Filter Configuration screen opens. Type the item number of the filter configuration to modify and press **Enter**. Use the **Space Bar** to cycle On/Off and Show/Hide. Type in the Date/Time Filter Starts and Date/Time Filter Ends time(s), if desired. Type **16** to change filters 4 through 15 to Show. Type **17** to change filters 4 through 15 to Hide. To return to the System Log, press **Esc**.

NOTE:Show All and Hide All settings override the settings for items 4 - 15.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------LOG DISPLAY FILTER CONFIGURATION-----------------------
                         1. Master Filter:                On
 Date/Time Filters:      2. Date/Time Filter Starts At:   18/01/2010 12:30:00
                         3. Date/Time Filter Ends At:     22/01/2010 14:30:00
 User Name Filters:      4. "SYSTEM":                     Show
                         5. "admin":                      Show
                         6. Others:                       Hide
 User Type Filters:      7. Local:                        Show
                         8. Others:                       Show
 Event Type Filters:     9. System:                       Show
                        10. Security:                     Show
                        11. Trap:                         Hide
                        12. Configuration Change:         Show
                        13. Action:                       Show
                        14. Configuration File Change:    Hide
                        15. OAM Event:                    Show
                        16. Show All Event Types
                        17. Hide All Event Types

                               Select[1-17]:
---------------------------------Messages-------------------------------------
```

Figure 6-3. Log Display Filter Configuration screen.

Chapter 7

Utilities

7.0 Utilities Menu

Use the Utilities menu to setup and display basic information.

Select Utilities (**6**) from the Main Menu and press **Enter**. The Utilities Menu (Figure 7-1.) opens. The paragraphs below describe how to display and modify each feature listed on the Utilities menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
---------------------------------------UTILITIES------------------------------

              1) Set Date and Time
              2) Reset Configuration To Default
              3) Change Password
              4) VT100 Baud Rate                 9600
              5) PING Generation
              6) Static ARP Table
              7) Dynamic ARP Table
              8) License Manager


                           Select [1-8]:




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

Figure 7-1. Utilities Menu

7.1 Set Date and Time

To set the correct date and time, type **1** and press **Enter**. Type the current date & time in DD/MM/YYYY HH:MM:SS format. Press **Enter** to confirm the setting. Note that SNTP will overwrite the setting on the next poll if SNTP is enabled.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------------UTILITIES------------------------------

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


                        Date :

    Type Current Date & Time (e.g., DD/MM/YYYY HH:MM:SS),
    and Hit 'Enter' to validate

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

Figure 7-2. Set Date and Time

7.2 Reset Configuration To Default

To reset the configuration to the default settings, type **2** and press **Enter**. At the bottom of the Utilities menu after "Reset configuration with factory default values and reset module?", type **Y** and press **Enter.** All values, with the exception of Manager IP Address, Subnet Mask, Default Gateway, Management Port, VLAN State, VLAN Number, Test IP and Subnet Mask, and User and Network Port settings will be returned to factory settings and the system will be reset.

NOTE:During reset all host connections will be terminated.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------------UTILITIES------------------------------

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


    Reset configuration with factory default values and reset module?:

    Enter 'Y' or 'N' and Hit return.

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

7.3 Change Password

To change your current password, from the Utilities menu, type **3** and press **Enter**. The Change Password screen (Figure 7-3.) opens.

1. Type in the current password and press **Enter**.
2. Type in the new password and press **Enter**.
3. Retype the new password and press **Enter**.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------CHANGE PASSWORD--------------------------------




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









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

Figure 7-3. Change Password Screen

7.4 VT100 Baud Rate

To change the VT100 baud rate, from the Utilities menu, type **4** and press **Enter**. The baud rate setting will be highlighted. Use the **Space Bar** to select 9600 or 19200. Press **Enter** to confirm setting.

7.5 PING Generation

From the Utilities menu, type **5** and press **Enter**. The PING Generation screen (Figure 7-4.) opens.

PING Generation is also available from the Diagnostics menu. See the chapter on Diagnostics for information on how to set up the Ping Generation screen.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------------PING GENERATION--------------------------------


             1) Ping to Address               : 172.16.142.197
             2) Ping from Address             : Auto Selection
             3) Ping Count                    : 25
             4) Ping VLAN ID                  : 0
             5) Ping Payload Size (40 - 9950) : 65
             6) Ping DF Bit                   : Clear
             7) Start Pinging

                             Select [1-7]:





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

Figure 7-4. PING Generation screen

7.6 Static ARP Table

The Static ARP table is used to define mapping between IP address and MAC address, and assign them to a port, thus bypassing the ARP mechanism. A maximum of 10 static ARP entries are available.

From the Utilities menu, type **7** and press **Enter**. The Static ARP Table screen (Figure 7-5.) opens.

1. **Add an Entry** - To add an entry to the static ARP table, type **1** and press **Enter**.

   - Type in the IP address and press **Enter**.
   - Type in the Mac address and press **Enter**.
   - Type in the port number and press **Enter**.

The address information will be added to the table.

2. **Delete an Entry** - To delete an entry from the Static ARP Table, type **2** and press **Enter**. The first table entry will be highlighted. Use **Space** to scroll down the entries. Press **Enter** to delete the highlighted entry. Press **Esc** to return to the Utilities menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------STATIC ARP TABLE--------------------------

     IP Address                MAC Address                Port
     ----------                -----------                ----
    92.168.1.102             45-54-25-88-74-22            User
    94.148.1.156             46-57-55-81-73-21            Mgmt
    45.122.4.121             44-52-44-23-76-98            Net
    97.198.3.246             67-76-65-56-45-54            User
    94.133.1.765             68-63-22-19-76-55            Net


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

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

Figure 7-5. Static ARP Table Screen

7.7 Dynamic ARP Table

The Dynamic ARP table lists currently active IP and MAC addresses for various 9145E10G ports. Dynamic ARP entries expire after 10 minutes, unless a message exchange takes place. From the Utilities menu, type **7** and press **Enter**. The Dynamic ARP Table screen (Figure 7-6.) opens. Use **F** (first), **N**, (next), **P** (previous) and **L** (last) to page through the entries. Type **D** (delete) to remove a highlighted entry from the table. Press **Esc** to return to the Utilities menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
--------------------------------DYNAMIC ARP TABLE-------------Display 0 - 0 of 0

  IP Address       MAC Address    Port   IP Address       MAC Address   Port
--------------- ----------------- ----  -------------- ----------------- ----
  92.168.1.102     45-54-25-88-74-22  User
  94.133.1.765     68-63-22-19-76-55  Ext
  45.122.4.121     44-52-44-23-76-98  Mgmt
  97.198.3.246     67-76-65-56-45-54  User
 94.148.1.156      46-57-55-81-73-21  User





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

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

Figure 7-6. Dynamic ARP Table Screen

7.8 License Manager

NOTE: If you are attempting to enable a disabled license, contact Canoga Perkins for a license key. Be sure to have the Feature name and 9145E10G Serial number available.

The License Manager screen allows the user to enable and disable the optional licenses available for the 9145E10G.

From the Utilities menu, type **8** and press **Enter**. The License Manager screen (Figure 7-7.) opens. Type **E** to enable or **D** to disable licenses. The first license entry will be highlighted. Use the **Space Bar** to cycle through the available licenses. Press **Enter** to enable or disable a license. Press **Esc** to return to the Utilities menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
--------------------------------LICENSE MANAGER--------------------------------


  Feature                Description                                State
  PM                     Performance Monitor                        Disabled
  SAM                    Service Availability                       Disabled
  PLPM                   Protected Link Performance Monitor         Disabled









                    Select [(E)nable],[(D)isable] Feature:

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

Figure 7-7. License Manager Screen

NOTE: Refer to the respective manuals for information about PM, SAM, and PLPM.

Chapter 8

Software Upgrade

8.0 Flash Memory

CAUTION: Swap Bank and Software Reset or Swap Bank After Download and Reset could disrupt service if the new software version has a different FPGA version.

Each 9145E10G has two flash memory banks that store software. The Active Flash Memory bank holds the software that is currently in use. The Inactive Flash Memory bank holds the new software from a download, or the older version of software from a previous upgrade. Software can be downloaded into the Inactive Flash Memory bank without disrupting the normal operation of the 9145E10G. Downloading software into the Inactive Memory bank is a background operation and will not disrupt services.

From the Main Menu, select Software Upgrade (**7**) and press **Enter**. The Software Upgrade screen (Figure 8-1.) opens. The Software Upgrade screen displays the time since the last restart time, the active firmware version, the backup firmware version, and the bootcode.

The Software Upgrade screen provides functions to reset the software, swap active flash memory banks, swap flash memory banks after a download and reset, and get a new file with TFTP.

8.1 Software Reset

To reset the software, type **1** and press **Enter**. Reset will be highlighted. Press **Enter**. The software will reset. All users will be logged off the system. Software resets will not affect payload traffic, as long as new software is not being loaded.

8.2 Swap Bank & Reset

The customer can elect to exchange the current software being executed with the software stored in the inactive flash memory bank. This process will swap flash memory banks (active > inactive, inactive > active) and reset the 9145E10G to activate the setting. The software in the inactive flash memory bank will become active and the active flash memory bank will become inactive when the 9145E10G resets.

NOTE: All users will be logged off during the 9145E10G reset. If the new software version has a new FPGA version, payload traffic through the 9145E10G Could be affected during the FPGA reprogramming.

To swap banks and reset the 9145E10G, type **2** and press **Enter**. Swap will be highlighted. Press **Enter**. The flash memory banks will be swapped and the 9145E10G will reset.

NOTE:The software on the new inactive flash memory bank will remain in memory and not be deleted.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------SOFTWARE UPGRADE-------------------------

    Time Since Last Restart 03:23:15

                         Version        File Name                  File Size

    Active Firmware      00.00  9145E-A00(CL31)-00-00.ZIP          3008191
    Inactive Firmware    50.08  9145E-A30-50-08.ZIP                3049460
    Bootcode             02.31  9145E-B00-02-31.BIN                 339018

    1)  Software Reset      Reset
    2)  Swap Bank & Reset   Swap
    3)  Swap Bank after
        download and reset  Yes

    4)  Get New File with TFTP

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

Figure 8-1. Software Upgrade Screen

8.3 Swap Bank After Download and Reset

Option 3 allows you to select automatically swapping banks on reset after a successful download. Select Yes for automatically swap banks. Select No to have downloaded software remain in the inactive bank. This option does not generate a reset.

Type **3** and press **Enter.** Press the **Space Bar** to cycle between Yes and No.

NOTE:Users will be disconnected when the 9145E10G is reset.

The flag must be set before the download of the new software while Swap Bank after Download and reset is set. After downloading software, the message line will read *Loads xx.xx on Next Reset*.

8.4 Get Software Upgrades with TFTP

Software can be downloaded from the Canoga Perkins web site to your TFTP server. After downloading the software, move the file to a known directory to which your TFTP server has access.

To download the latest version from your TFTP server to the 9145E10G, from the Software Upgrade menu (Figure 8-1.) type **4** and press **Enter**. The TFTP Upgrade screen (Figure 8-2.) will appear.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------------TFTP SOFTWARE UPGRADE-----------------------

    Time Since Last Restart 03:27:41



    Host IP Address :               172.16.142.197
    Save in Non Volatile RAM? :     Y
    File Name: 9145E10G2.0
    File transfer to unit now ?     Y





    TFTP transfer in progress...\

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

Figure 8-2. TFTP Software Upgrade Screen

1. Enter the IP Address of the Host TFTP server or press **Enter** to accept default address.
2. Enter the file name of the software you want to download and press **Enter**.
   a. Type **Y** and press **Enter** to begin the download. Progress can be viewed in the message line.
   b. Type **N** and press **Enter** to cancel the download and return to the Software Upgrade screen.
3. When the download is complete, press **Enter** to return to the Software Upgrade screen. The new software version should appear in the *Inactive Firmware* field. If Swap Bank after download and reset was set, the message: Loads xx.xx on Next Reset will appear on the message line.

8.5 Software Upgrades Using FTP or SFTP

8.5.1 Software Download using FTP

Software upgrades can also be downloaded from the Canoga Perkins web site and installed using the computer that is the 9145E10G management host.

1. Go to the Canoga Perkins web site or contact Canoga Perkins Customer Service to obtain the latest version of the 9145E10G software and copy the file to the 9145E10G management host.

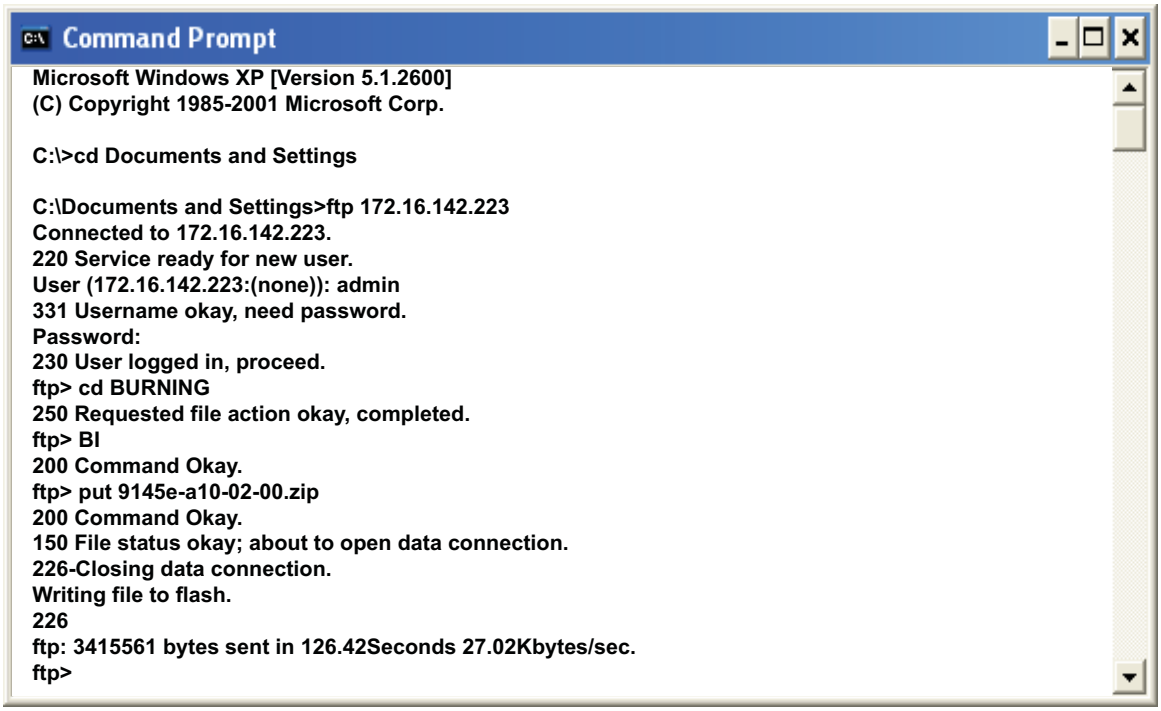

Figure 8-3. Command Prompt Screen

2. Open a Command Prompt by selecting **Start>Run**

3. Type **CMD** into the OPEN window and click **OK**. The Command Prompt screen will open (Figure 8-3.).

NOTE: Confirm that the IP address of your computer is listed in the 9145E10G host table. If not, you can not access the 9145E10G. To add the computer IP address in the host table, refer to "Host Table" on page 15.

4. If required, type **cd *directory name*** where **directory name** is the name of the directory where the software upgrade is located.

5. Press **Enter**. The prompt will be relocated to that directory.

6. At the directory prompt, type **ftp** ***IP address*** Where ***IP address*** is the management IP address for the 9145E10G.
7. Press **Enter**. Service will be established.
8. Type in your 9145E10G account username and password. Press **Enter**.
9. Type in your password and press **Enter**. The ftp> prompt opens.
10. At the ftp> prompt, type ***cd BURNING*** (case sensitive) and press **Enter.**
11. At the ftp> prompt, type **bi** (for binary) and press **Enter**. This informs the 9145E10G that this will be a binary rather than a text download. Another ftp> prompt will open.
12. At the ftp> prompt, type ***put (filename)***

    Where **(filename)** is the filename of the software upgrade. The command will be accepted and the download starts.

    NOTE: The 9145E10G displays the number of bytes transferred. A separate message indicates the Flash Burning status, including percentage complete.

13. Once the software upgrade is downloaded, a notification that the data connection has been closed and that the upgrade is being written to the 9145E10G flash memory will be displayed.
14. When the upgrade has been completely written to memory, a record of the file transfer will be displayed.
15. Close the Command Prompt window.

8.5.2 Software Download using SFTP

For secure file transferring, the 9145E10G provides a Secure File Transfer Protocol (SFTP) server. The server is available to run with the SFTP client of your choice.

NOTE: Use the default settings for the SFTP Client program.

1. Start your Secure File Transfer Client and select **Quick Connect** or **Open.**
2. Enter the IP address of your 9145E10G, and your 9145E10G username.
3. A dialog opens. If this is your first time contacting the host, you will be asked if you want to use the keys. Choose **OK** and a password dialog opens.
4. Enter your password for the 9145E10G account. Type ***cd BURNING*** (case sensitive) and press **Enter** to direct the software upgrade to the proper directory in the 9145E10G.
5. Transfer the software upgrade to the BURNING directory.
6. Type in the file name and press **Enter.** If using a GUI SFTP client, you can drag and drop the upgrade file.

Chapter 9

Managing Logged In Users

9.0 Manage Logged In Users

The Manage Logged In Users function is used by the administrator to view current users, and to terminate user sessions when required. One console session and 5 telnet sessions are allowed at one time. The last remaining supervisor logged on can not be terminated.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
----------------------------MANAGE LOGGED IN USERS-----------------------------
Session    Type      Username     Access       Description
-------------------------------------------------------------------------------
           Console   AT LOGIN MENU
*  1.      Network   admin        Supervisor   Default Account
   2.      Network   admin        Supervisor   Default Account
   3.      Network   AT LOGIN MENU





  * = Current Session

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

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

Figure 9-1. Manage Logged In Users Screen

Chapter 10

Link OAM

10.0 Link Operation, Administration and Maintenance

Link Operation, Administration, and Maintenance (OAM) is defined in Section 57 of the IEEE 802.3-2005 standard. Its functions provide mechanisms for monitoring link operations at the data link pager, such as remote fault indication and remote loopback control. Link OAM provides network operators with the ability to monitor the health of the network and quickly determine the location of any failing links or fault conditions. OAM provides data link layer mechanisms that complement applications that may reside in higher layers, such as Connectivity Fault Management (CFM) 802.1ag. OAM is supported via SNMP with the standard dot3Oam.my and the Canoga Perkins proprietary cpDot3Oam.my MIB files. From the Main Menu, select Link OAM (**9**) and press **Enter**. The 802.3AH OAM menu (Figure 10-1.) opens.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-----------------------------------Link OAM MENU------------------------------



                              1) OAM Control
                              2) OAM Peer Information
                              3) OAM Statistics
                              4) OAM Event Configuration
                              5) OAM Event Log



                                  Select [1-5]:




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

Figure 10-1. 802.3AH OAM Menu

10.1 OAM Control

The OAM Control screen (Figure 10-2.) is split into two sections. The top of the screen shows status information while the bottom of the screen allows you to control and configure the OAM settings. The user selects which parameter to configure. The paragraph 10.1.13 shows the standard configuration parameters and their corresponding MIB objects.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------------------OAM CONTROL----------------------------
                                  User Port               Network Port
                                  ---------               --------------
 OAM Operational Status           Disabled                Passive Wait
 OAM Max PDU Size                 1518                    1518
 OAM Revision                     1                       1
 OAM Functions Supported          Unidirectional          Unidirectional
                                  Loopback                Loopback
                                  Link Events             Link Events

 OAM Loopback Status              No Loopback             No Loopback
 OAM Remote Link Fault            No                      No

 1) OAM Admin State               Disabled                Enabled
 2) OAM Mode                      Active                  Passive
 3) OAM Loopback Command          No Loopback             No Loopback
 4) Process Rx Loopback OAMPDU    No                      No
 5) Process Rx Link Fault Flag    Yes                     Yes
 6) Fwd Critical Event            No                      No
                                  Select [1-6]:
----------------------------------Messages-------------------------------------
```

Figure 10-2. The OAM Control Screen

10.1.1 OAM Operational Status

At initialization and also after failure conditions, the two OAM entities on the same full-duplex Ethernet link begin a discovery phase to determine what OAM capabilities may be used on that link. The following is the list of possible values:

1. **Disabled -** This value will return "disabled" if OAM is disabled on this interface via the OAM Admin State.

2. **Link Fault -** If the link has detected a fault and is transmitting OAMPDUs with a link fault indication, the value is link Fault. This value will also be returned if the interface is not operational.

3. **Passive Wait -** The passive Wait state is returned only by OAM entities in OAM Mode passive and reflects the state in which the OAM entity is waiting to see if the peer device is OAM capable.

4. **Active Send Local -** This value is used by active mode devices and reflects the OAM entity actively trying to discover whether the peer has OAM capability but has not yet made that determination.

5. **Send Local And Remote -** Reflects that the local OA entity has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device can, for whatever reason, decide that the peer device is unacceptable and decline OAM peering.

6. **Peering Locally rejected -** This message appears when the local OAM entity rejects the peer OAM entity.

7. **Send Local and remote OK -** This state shows that the OAM peering is allowed by the local device.

8. **OAM peering Remotely Rejected -** This state show that the remote OAM entity rejects the peering.

9. **Operational -** Indicate that local and remote OAM entities have accepted the peeing. And OAM is up and running.

10.1.2 OAM Max PDU Size

This is the maximum OAM PDU size that the 9145E10G will support. If the OAM maximum PDU size is different between the 9145E10G and its peers, the smaller of the two maximum OAMPDU sizes will be used between the peers.

10.1.3 OAM Revision

The revision number increments every time there is a change in the OAM configuration of the 9145E10G. The change in revision number will trigger the peer to re-evaluate whether OAM peering is allowed. OAM Revision is incremented whenever OAM Mode is changed from Active to Passive and Passive to Active.

10.1.4 OAM Functions

The following list all the feunction that are supported by the OAM implementation. Peer supported function are also communicated via the OAM protocol and could be viewed from teh OAM peer screen . The following Link OAM functions are supported in the 9145E10G R1.0 software.

NOTE: On the 9145E10G, unidirectional mode is always supported

1. **Unidirectional -** Indicates that the 9145E10G supports the transmission of OAM PDU in unidirectional mode.

2. **LoopBack -** Indicates that the 9145E10G can initiate and respond to loopback commands.

3. **Link Events -** Indicated that the 9145E10G can send and receive event notification OAMPDU.

10.1.5 OAM Loopback Status

This function returns the status and states. There are four states available: No Loopback, initiating Loopback, remote loopback, Terminating loopback.

10.1.6 OAM remote Fault

This function indicates whether a remote fault OAM PDU was sent by the peer to the 9145E10G.

10.1.7 OAM Admin State

This administrative state is what enables or disables OAM in the 9145E10G.

10.1.8 OAM Mode

There are two modes that can be configured in every port of the 9145E10G that are Passive and Active Modes. The passive mode allows to participate to the OAM but not the capability to initiate any of the Link OAM functions such as Loopback or generate critical Event while active mode allows you to run all teh OAM functions.

10.1.9 OAM Loopback Command

This command allows you to start or terminate an existing remote loopback in the 9145E10G.

10.1.10 Process Rx Loopback OAM PDU

This command allows you to control whether to process or ignore incoming OAMPDU.

10.1.11 Process Rx Link Fault Flag

This setting controls the actions taken upon reception of a Link Fault message from a connected partner. If this object is set to Yes, the Link Fault will be processed the same as Remote Fault and could trigger LLF.

10.1.12 FWD Critical Event

This setting controls whether or not a critical event is sent when the other port link goes down. Information concerning operational status, maximum OAM Protected Data Units (PDU) size, OAM revision, functions supported, loopback status, and remote link fault.

10.1.13 User interface MIB Objects

- FWD Critical Event cpDot3OamForwardCriticalEvent (cpdot3oam.my)
- OAM Admin State dot3OamAdminState (dot3oam.my)
- OAM Functions Supported dot3OamFunctionsSupported (dot3oam.my)
- OAM Loopback Command dot3OamLoopbackStatus (dot3oam.my)
- OAM Loopback Status Dot3OamLoopbackStatus (dot3oam.my)
- OAM MAX PDU Size dot3OamMaxOamPduSize (dot3oam.my)
- OAM Mode dot3OamMode (dot3oam.my)
- OAM Operational Status dot3OamOperStatus (dot3oam.my)
- OAM Remote Link Fault
- OAM Revision dot3OamConfigRevision (dot3oam.my)
- Process Rx Link Fault Flag cpDot3OamProcessRxLinkFault (cpdot3oam.my)
- Process Rx Loopback OAMPDU dot3OamloopbackIgnoreRx (dot3oam.my)

10.2 OAM Peer Information

This table contains information about the OAM peer for a particular Ethernet-like interface such as OAM Peer Status, OAM Peer MAC Address, OAM Peer Vendor, OAM Peer Vendor Info (Hex), OAM Peer Mode, OAM Peer Max PDU Size, OAM Peer Config Revision, and OAM Peer Functions Supported. As indicated in eth figure below, there is one entry in this table for each port.

From the OAM Control screen, select OAM Peer Information (**2**) and press **Enter**. The OAM Peer Information screen (Figure 10-1.) opens. Press **Esc** to return to the 802.3AH OAM menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
-----------------------------------OAM PEER INFORMATION------------------------

                                  User Port Peer          Network Port Peer

 OAM Peer Status                  Active                  Active
 OAM Peer MAC Address             00-40-2A-03-7A-E0       00-40-2A-03-7A-E8
 OAM Peer Vendor OUI              00-40-2A                00-40-2A
 OAM Peer Vendor Info (Hex)       91450100                91450100
 OAM Peer Mode                    Active                  Passive
 OAM Peer Max PDU Size            1518                    1518
 OAM Peer Config Revision         1                       1
 OAM Peer Functions Supported     Unidirectional          Unidirectional



                         Press ESC to return to previous screen



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

Figure 10-1. The OAM Peer Information Screen

10.3 OAM Statistics

The OAM Statistics screen provides the customer with information concerning OAMPDUs, Event Notifications, Loopback Requests, Variable Requests and Responses, and Unsupported Opcodes. From the OAM Control screen. Type **3** and press **Enter** The OAM Statistics screen (Figure 10-2.) opens. Press **Esc** to return to the 802.3AH OAM menu.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
----------------------------OAM STATISTICS (CURRENT)---------------------------
                                  User Port   User Port   Net Port    Net Port
                                    Sent        Rcvd        Sent        Rcvd
                                  ---------   ---------   ---------   ---------
 Information OAMPDUs                 0           0       24171           0

 Unique Event Notifications          0           0           0           0
 Duplicate Event Notifications       0           0           0           0

 Loopback Control                    0           0           0           0

 Variable Requests                 N/A           0         N/A           0
 Variable Responses                N/A           0         N/A           0
 Organization Specific OAMPDUs     N/A           0         N/A           0
 Unsupported Opcodes               N/A           0         N/A           0

 Total OAMPDUs                       0           0       24171           0

              CTRL-T to view raw counters, CTRL-R to reset OAM counters,
              TAB to view Link Event Statistics, ESC to return
----------------------------------Messages-------------------------------------
```

Figure 10-2. OAM Statistics screen

10.4 OAM Event Configuration

The OAM Event Configuration screen allows the customer to configure the errors in the OAM. From the OAM Control screen, type **4** and press **Enter** The Event Configuration screen (Figure 10-3.) opens. Press **Esc** to return to the 802.3AH OAM menu.

10.5 OAM Event Log

The OAM Event Log screen displays only OAM entries. From the OAM Control screen, type **5** and press **Enter**. The Event Configuration screen (Figure 10-4.) opens. Use **F** (first), **N** (next), **P** (previous) and **L** (last) to page through the listings. Use **G** (go to) to locate a particular event, use **D** (detail) to view the Event Log Detail Display screen (Figure 10-5.), and use **S** (select filter) to view the Filter Configuration screen (Figure 10-6.). Press **Esc** to return to the 802.3AH OAM menu.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
--------------------------------OAM EVENT CONFIGURATION------------------------
                                                   User Port         Network Port
                                                   ---------         ------------
  1) Errored Symbol Period Window                 1250000000           1250000000
  2) Errored Symbol Period Threshold                       1                    1
  3) Errored Frame Window (secs)                         1.0                  1.0
  4) Errored Frame Threshold                               1                    1
  5) Errored Frame Period Window                     1488095              1488095
  6) Errored Frame Period Threshold                        1                    1
  7) Errored Frame Seconds Window (secs)                60.0                 60.0
  8) Errored Frame Seconds Threshold                       1                    1
  9) Transmit Event Notification Count                     1                    1
 10) Event Log Frequency (in 100 ms)                     600                  600
 11) Send Errored Symbol Period Events               Enabled              Enabled
 12) Send Errored Frame Events                       Enabled              Enabled
 13) Send Errored Frame Period  Events               Enabled              Enabled
 14) Send Errored Frame Seconds Events               Enabled              Enabled
 15) Send Dying Gasp Events                          Enabled              Enabled
 16) Send Critical Events                            Enabled              Enabled
                                  Select [1-16]:
---------------------------------Messages-----------------------------------
```

Figure 10-3. Event Configuration Screen

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
-------------------------OAM EVENT LOG BRIEF DISPLAY--------------------------
Index  OUI    Type                   Location    Time Stamp        Value
------ ------ --------------------- ----------- ---------------- --------------
           Displaying 1 to 13 of 13 filtered entries, 13 total
 1     0180C2 Link Fault            Remote/Net    2 days 20:12:50            N/A
 2     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 3     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 4     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 5     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 6     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 7     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 8     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 9     0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 10    0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 11    0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 12    0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A
 13    0180C2 Link Fault            Local/Net      0 day 00:00:10            N/A

Select [(F)irst, (N)ext, (P)rev, (L)ast, (G)oto, (D)etail, (S)elect Filter]:
---------------------------------Messages-----------------------------------
```

Figure 10-4. Event Log Brief Display Screen

10.5.1 Event Log Detail Display

The Event Log Detail Display screen (Figure 10-5.) shows all events that occurred during the current session. Use **F** (first), **N** (next), **P** (previous) and **L** (last) to page through the listings. Use **G** (go to) to locate a particular event.

```
Canoga Perkins Corp.        Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                          01:45:14
--------------------------OAM EVENT LOG DETAIL DISPLAY--------------------------

           Displaying 12 to 13 of 13 filtered entries, 13 total

Index:          12                      Index:          13
Time Stamp:     0 day 00:00:10.3        Time Stamp:     0 day 00:00:10.3
OUI:            0180C2                  OUI:            0180C2
Type:           Link Fault              Type:           Link Fault
Location:       Local/Net               Location:       Local/Net
Window:         N/A                     Window:         N/A
Threshold:      N/A                     Threshold:      N/A
Value:          N/A                     Value:          N/A
Running Total:  1                       Running Total:  1
Event Total:    1                       Event Total:    1
Occurrence:     1                       Occurrence:     1


     Select [(F)irst, (N)ext, (P)rev, (L)ast, (G)oto]:
----------------------------------Messages-------------------------------------
```

Figure 10-5. Event Log Detail Display Screen

10.5.2 Display Filter Configuration

The Display Filter Configuration screen (Figure 10-6.) allows you to turn the Master filter on or off, and also to show or hide the location, port, and type filters.

1. To change the Master Filter setting, type **1** and press **Enter**. Use the **Space Bar** to select On or Off. Press **Enter** to accept the setting. Press **Esc** to return to the Event Log Display screen.

2. To change the Location, Port, and Type filter settings, type the number for the specific filter and press **Enter**. Use the **Space Bar** to select Show or Hide. Press **Enter** to accept the setting.

3. To set all of the Location, Port, and Type filter settings to Show, type **15** and press **Enter**.

4. To set all of the Location, Port, and Type filter settings to Hide, type **16** and press **Enter**.

```
Canoga Perkins Corp.         Ethernet Network Interface Device       04-JAN-2010
9145E10G-527-2-0 V01.00 F31                                           01:45:14
------------------OAM EVENT LOG DISPLAY FILTER CONFIGURATION--------------------

                        1. Master Filter:               Off
    Location Filters:   2. Local:                       Show
                        3. Remote:                      Show
    Port Filters:       4. User:                        Show
                        5. Network:                     Show
    Event Type Filters: 6. Errored Symbol Period:       Show
                        7. Errored Frame:               Show
                        8. Errored Frame Period:        Show
                        9. Errored Frame Seconds:       Show
                       10. Orgnization Specific:        Show
                       11. Link Fault:                  Show
                       12. Dying Gasp:                  Show
                       13. Critical Event:              Show
                       14. Show All Event Types
                       15. Hide All Event Types

                              Select[1-15]:
----------------------------------Messages-------------------------------------
```

Figure 10-6. Display Filter Configuration Screen

Appendix A

Acronyms

Acronyms

For a complete list of acronyms used by Canoga Perkins and the industry, refer to the Canoga Perkins Abbreviations and Acronyms Manual.

CANOGA PERKINS CORPORATION

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