9145E
Network Interface Device
Product Overview

James Heney
February 2008
# Table of Contents

9145E Network Interface Device Product Overview

9145E BASE UNIT

User Port, Network Port and Multi-Purpose Port Interfaces

Console Management Interface

Ethernet 10/100BASE-TX Management Interface (OOB)

SERVICE LEVEL AGREEMENT (SLA) MANAGEMENT

What is SLA?

What is CoS?

PERFORMANCE MEASURING

Test Parameters

Test Results

SERVICE AVAILABILITY MONITORING

9145E ARCHITECTURE TRAFFIC POLICING AND FILTERING DESCRIPTION

CoS Queuing

Pre-Queue Egress Demultiplexer

Egress Multiplexer

Ingress/Egress Queues

Ingress/Egress Scheduler

Post-Queue Egress Demultiplexer

Management Classifier & Queues

Management Scheduler

Router

Pre-Queue Ingress Demultiplexer

Ingress Multiplexer

Management Interface and Sample Menus

9145E Sample Management Screens

9145E Link and SFP Status Screen

9145E VLAN Tagging Rules Screen

9145E 802.1AH OAM Configuration Screen

9145E Alarms and Traps

VLAN STACKING IMPLEMENTATION

TRAFFIC STATISTICS

Overview

Detail Listing

802.3AH OAM

LOOPBACK DIAGNOSTICS

Local-Local Mode

Local-Remote Mode

Remote-Local Mode

Remote-Remote Mode

SFP Optics Offering

SFP Optics (100 Mbps, 1 Gbps) - 9145E Advanced and Standard Models

CanogaView SEM Element Manager Architecture
9145E Network Interface Device Product Overview

The 9145E is Canoga Perkins’ second generation Ethernet NID platform. The 9145E builds on the existing 9145E by adding new features and functions required by Service Providers to deliver MEF compliant metro Ethernet services.

Leveraging customer feedback from the 9145E design, the 9145E is housed in a new enclosure befitting of a Metro Ethernet demarcation Device. The compact design minimizes the amount of space needed for rack mount and wall mount installations. Two 9145Es fits side-by-side in 1RU of rack space.

Ethernet NIDs are typically deployed at UNI, I-NNI or E-NNI points (or other strategic points) within a Service Provider (SP) network to help deliver, manage and maintain Ethernet Services or to act as test points within a MEN.

This section describes how the 9145E can be utilized as the demarcation point for SP Ethernet User-to-Network Interfaces (UNI) and External Network-to-Network Interfaces (E-NNI). Figure 1 illustrates UNI and E-NNI points within the generic framework described within the MEF 4 Technical Specification.

Application at the UNI

When deployed at the UNI, there are three main functions of the 9145E:

1) ETT: Ethernet Transport Termination
2) ETST: Ethernet Tunnel Service Termination
3) EST: Ethernet Service Termination

The first function of the 9145E is to terminate the transport. In the example above, the transport could be native Ethernet (copper or fiber), a DS1, DS3 or OC-N facility, xDSL access, etc. The 9145E supports native Ethernet transport options at this time on 10/100/1000 UTP and 100/1000 Optical interfaces. It is within the architecture of the 9145E to incorporate other network interfaces such as TDM and SONET. The UTP interface accommodates other access transport technologies (xDSL/Cable Modem, SONET, Ethernet Access Switches...)

The second function of the 9145E at the UNI is to terminate Tunnel Services. A “tunnel” is an association of an E-NNI and a UNI, where C-EVCs are all-to-one bundled at the interfaces. The NID will have the ability to terminate such tunnels at the tunnel service layer. This includes termination of Performance Monitoring (PM) of the tunnel. Taking into consideration that tunnel services are often provided by Out-of-Franchise (OOF) operators, the 9145E provides secure management access to EST functions for OOF SPs using in-band SNMPv3.
Finally, the 9145E provides termination of the Ethernet service. Service termination implies that the NID user interface implements the UNI-N functions in MEF 13 [2] and supports Ethernet service attributes as per MEF 10 [3]. Explicitly stated, the NID will be equipped with traffic management functions, performance monitoring and link layer to service layer OAM functions.

Application at the E-NNI

Figure 1 (page 15) depicts the 9145E deployed at the E-NNI. According to the MEF,

“An E-NNI is a layered interface built on a point-to-point physical link or multiple point-to-point physical links connecting two MENs where the two MENs belong to different administrative domains”.

In this example, two 9145Es are deployed in a protected link. In this case, the protection scheme is a Link Aggregation Group (LAG). The 9145Es act as “link partners” on the LAG between the two provider edge switches.

As in the application at the UNI, NIDs deployed at the E-NNI require the same ETT, ETST and EST functionality. However, because E-NNI points can consist of multiple point-to-point physical links, some additional functionality is required to support the protection scheme. For this implementation, the only protection scheme that will be considered and supported is IEEE 802.3ad. This is the simplest and most widely available form of protection for Ethernet links at this time.

Consider, for example, that there are Component EVCs (C-EVCs [4]) between both UNIs and the E-NNI point in MEN “A”. Service Providers will require PM between the UNI and the E-NNI point. Therefore, the NIDs deployed at the E-NNI point must terminate any performance monitoring protocols. The LAG at the E-NNI adds additional complexity to terminating any active measurement protocol that may be used for PM. This is because load balancing schemes in a LAG make it impossible for the NID to predict which port a round-trip measurement packet may be delivered. In the example, delivering each of the PM protocol packets to the correct NID at the E-NNI point is imperative for accurate PM metrics. An external physical link between the two NIDs can be used to accomplish this.

Also, consider that C-EVCs terminating at the E-NNI point are tunneled to the UNI point at NID3. The NIDs at the E-NNI point must have ETST functions to bundle the C-EVCs to a tunnel. It is also possible for the NIDs at the E-NNI point to run Performance Measuring for the tunnel itself.
**9145E BASE UNIT**

The 9145E Base Unit is designed with front-panel data and management ports and rear-panel power and ground connectors. The 9145E front panel is designed so that all the following ports and connectors can be offered simultaneously in one model:

- One EIA-232 Console management port with DE-9 female connector
- One 10/100BASE-TX Ethemet management port with UTP connector
- One User Port (for service data) with both SFP and UTP connectors
- One Network Port (for service data) with both SFP and UTP connectors
- One Multi-Purpose Port (service data and/or proprietary traffic) with both SFP and UTP connectors

Five 9145E base unit powering options:
1) Single AC Power
2) Redundant AC Power
3) Single DC Power
4) Redundant DC Power
5) Redundant AC and DC mix

**User Port, Network Port and Multi-Purpose Port Interfaces**

These ports provide both a fixed UTP and an SFP connector. The UTP port is an IEEE 802.3 compliant for 10BASE-T, 100BASE-TX and 1000BASE-T. To assist with diagnosing customer location problems, the UTP port supports cable diagnostics, verifying integrity of the copper connection to the customer equipment. SFPs are available in a variety of multimode, single mode, CWDM and single fiber BIDI interfaces. The SFP port is MSA compliant, supporting support Digital Diagnostics, including transmit and receive optical signal levels.

**Console Management Interface**

The console port of the 9145E is used for serial communication between the 9145E and a VT100 terminal or emulator. It uses a EIA-232 compliant port terminated on a DE-9 female connector, with a DCE pin-out so that it may be directly connected to a terminal through a null modem cable.

**Ethernet 10/100BASE-TX Management Interface (OOB)**

The Ethernet 10/100BASE-TX Management port (also known as OOB Management Port) is used for out-of-band management of the 9145E and is terminated on a RJ 45 UTP connector.

The 10/100BASE-TX Management Interface supports the following modes of operation:

- Autonegotiation
- 10BASE-T Half-Duplex
- 10BASE-T Full-Duplex
- 100BASE-TX Half-Duplex
- 100BASE-TX Full-Duplex

The 10/100BASE-TX Management Interface supports auto-MDI/MDIX in order to sense TX and RX pairs and automatically cross-over its interface.
SERVICE LEVEL AGREEMENT (SLA) MANAGEMENT

Canoga Perkins’ Performance Collection System (PCS) effectively performs and collects network performance assurance statistics across IP based networks and their associated services including video, voice, storage and data applications. These features are essential for any Carrier or Internet Service Provider (ISP) in order to support Service Level Assurance (SLA) contracts. Enterprise or private networks may also choose to utilize these features to monitor the performance of their network.

What is SLA?
SLA stands for Service Level Agreement. It is basically an agreement or contract between a service provider and its customer. The supplier agrees to provide a specific level of service of which if the level of service is not met, then penalties are applied. Typically this implies a percentage of money to be credited for the billing cycle.

What is CoS?
CoS, or Class of Service, is a method of identifying and prioritizing communication packets for the purpose of supporting applications and users, based on their data, priority and timing requirements. Applications consist of voice, video or data, and users may be management, engineers, accounting or other levels of employees with varying requirements. Bandwidth management, performance management, provisioning, fault management, jitter and latency control, etc. are all major components or building blocks used to setup the strategy that a service provider follows in order to fulfill their SLA contractual obligations.

Canoga Perkins’ ability to monitor network performance up to the “last mile” without the need for additional equipment requirements provides a key advantage in determining the overall performance of the network. See Figure 2. Key performance parameters that can be monitored include:

- Packets Sent
- Round Trip Packets
- Dropped Packets
- Out of Order Packets
- Data Delivery %
- Minimum, Maximum, Average and Total Round Trip Latency
- Local to Remote Minimum, Maximum, Average and Total Jitter
- Remote to Local Minimum, Maximum, Average and Total Jitter

Performance Measurement Model Furthermore, the ability to define performance metrics and capture the number of packets that belong within each metric, helps to determine the overall effectiveness and quality for each CoS provided. These performance metrics which are later referred to as Latency
and Jitter Buckets, are configurable for each CoS in each NID in the network. These metrics along with other packet parameters such as priority, size, number of packets per seconds, etc. are used to define what Canoga has named as a “Profile”. The purpose of a “Profile” is to mimic the end-user’s transfer of data between NIDs for the purpose of ensuring that the overall quality of a CoS has been met as described and defined within a SLA.

Canoga Perkins supports SLA through the use of its Network Performance Assurance (NPA) and Performance Collection System (PCS) components. Additional support for Enterprise and Carrier Class Northbound Interface (NBI) for provisioning, accounting, etc. support systems can be added as a custom option. Figure 3 shows the relationship between the various SLA components.

PERFORMANCE MEASURING

The Network Interface Device (NID) level Performance Measuring (PM) application conducts latency, jitter, and packet loss tests one or more multiple destinations on a scheduled basis and stores the results data for subsequent submittal to an analysis or business system.

An ICMP Ping Test Packet is sent by the Near (Local) NID. The test packet contains test control information and fields for time stamps. Four time stamp fields are contained in the payload of the Test Packet. The Time Stamps include Originating Departure Time, Destination Arrival Time, Destination Departure Time and Originating Arrival Time. In 2009, Canoga Perkins implementation of RFC-2544 Performance Testing is planned as an alternate Performance Testing technique. This article describes the current testing technique.
The Time Stamps are inserted by the Field Programmable Gate Array (FPGA) contained in the NID. Time Stamping by the FPGA eliminates variable processing times associated with the Management Processor’s IP Stack and reflects the true time it took for the Test Packet to transverse the network.

The Time Stamps allow Round Trip Latency and Jitter parameters to be calculated and reported. Control information tracks the packets and their sequence and accounts for Lost Packets and Out of Sequence Packets.

Ping type Test Packets were selected for use in the NID with SLA Support Option due to their virtually universal compatibility with non-Canoga Perkins IP devices that may become added to the testing.

Round Trip Latency is the time it takes a packet to get through the network, less processor time at the destination. Round Trip Latency = (Origination Departure-Origination Arrival) – (Destination Departure-Destination Arrival).

Jitter is the difference between originating packet intervals and arriving intervals. The four Time Stamps also allow Jitter to be measured independently in each direction (origin-destination, destination-origin).

Figure 4 below illustrates the use of two NIDs to measure EVC performance at the customer premises.

**Test Parameters**

There are several parameters in the NID with SLA Support Option that describe test packet contents, addressing and prioritization, test duration and results classification.

The parameters are:

- Circuit ID / EVC ID – User definable text
- Destination MAC and IP Address
- VLAN ID
- Class of Service - 802.3p P-Bit
- IP DSCP Value
- Packet Rate - Packets Per Second, 1 to 100 PPS, Packets are released at a consistent rate \( \sqrt{PPS} \)
- Test Duration in Seconds - 0 to 16,384 seconds, 0=continuous test
- Packet Return Timeout in Seconds
- Packet Time to Live in Seconds
• Packet Length in Bytes
  o Minimum Packet Length (86 to 1517 bytes)
  o Maximum Packet Length (86 to 1518 bytes)
    ▪ Test begins with minimum length; each successive test packet sent increments packet length by one byte until maximum length is reached. Packet length is then reset to minimum value and cycle begins again. For fixed length packets, minimum and maximum values are set equal.

• Latency Buckets (Milliseconds, 10 Buckets)
  ▪ Latency Buckets tally the number of packets with round trip latency falling in each bucket’s range. Buckets 1-9 are set by entering maximum time value for the bucket. Minimum time value is previous bucket maximum value plus 1. Bucket 1 minimum time is 0. Bucket 10 maximum value is set to the Packet Return Timeout value.

• Jitter Measurement Offset (1 to 20 packets)
  ▪ Jitter is measured packet to packet. Offset is the number of packets between measuring packets. If set to 4, the jitter is measured between packets 1&5, 2&6, 3&7… For adjacent packet measurements, set Offset to 1.

• Jitter Buckets (Milliseconds, 9 Near-Far Buckets, 9 Far-near Buckets)
  ▪ Buckets 1-9 are set by entering positive or negative time value for the bucket. Minimum time value is previous bucket maximum value plus 1. Bucket 1 minimum time is 0. Bucket 5 maximum value is set to the Packet Return Timeout value. Both Local-Remoter and Remote-Local Buckets are set to the same values. Will allow negative and positive values with the middle bucket 0.

Test Results
A number of Network Parameters are characterized by the test, latency, inter-frame jitter, lost frame rate and packet sequencing problems. Through the sending and receiving of Test Packets, the following parameters are reported and recorded.

• Round Trip Latency – Minimum, Maximum, Average, Buckets (number of packets in each Bucket)
• Jitter – Originating-Destination, Destination-Originating - Minimum, Maximum, Average, Buckets
• Number of Round Trip Packets
• Number of Lost Packets
• Number of Out-of-Sequence Packets

Key functions of the NID Network Performance Assessment application are the Buckets for Latency and Jitter results, multiple Test Profiles, and an Address List. The Address List and Test Profiles work together to allow the NID to autonomously perform Network Performance Assessment tests to multiple destinations and store results.

The Address List contains information describing the Destination device and Test Profile to run. The Address List supports 100 entries (destinations/virtual circuits). Multiple entries of a single Circuit ID are permissible. Testing of all entries of the List are executed as described by the List’s Testing Rate setting which is done in minutes.
The Address List has a single parameter that is set at the NID, Test Interval. The Test Interval describes often the NID cycles through the Address List performing Network Performance Assurance Tests. It is in minutes and based on the time of the last NID Boot-up. Minimum value is based on the Address List size and each Test Duration Time. The NID will not allow a Testing Rate shorter than reasonable to get through the list. Each Entry in the list is tested sequentially until the list is completed, then waits for the next start time.

Each entry in the Address List contains the following parameters:

- Circuit ID /EVC ID (User definable text)
- Destination IP Address
- VLAN ID
- Test Profile ID

Eight Test Profiles are provided in the NID and are available for definition. A Test Profile describes test parameters, control information and Class of Service attributes.

- Profile Name
- Class of Service
- Packet Rate
- Packet Timeout
- Packet Time to Live
- Jitter Measurement Offset
- DF Value
- User Text
- IP DSCP Value
- Test Duration
- Packet Length - Minimum Packet Length, Maximum Packet Length
- Latency Statistics Bucket Values, 5 Buckets
- Jitter Statistics Bucket Values, 9 Buckets

SERVICE AVAILABILITY MONITORING

Service Availability Monitoring (SAM) is unique, it was developed by Canoga Perkins in 2006 and entered service in 2007. It performs connectivity tests and reports availability on each EVC connection. For connections where both the local and remote sides have implemented this SA method, one way availability is reported. For connections where only the local side has SA implemented, round trip availability is reported.

To collect metrics on the availability of a network connection small test packets are sent at regular time intervals called the Sample Period (see Figure 1). The test packets are organized into groups to determine the service availability. The shorter time period is called delta t (Dt) which consists of a small number of samples and a computation is completed for each Dt providing a Frame Loss Ratio (FLR). The longer time period is called Service Availability Window consisting of several Dt periods and determines the state of that connection by comparing each Dt value to a pair of thresholds and the state prior to the Service Availability Window.

![Service Availability Window Diagram](image)

The SA option conducts conduct continuous testing on up to 150 connections simultaneously. For equipment compatible with Canoga Perkins SAM option, availability data is maintained on a one way basis (local ->remote and remote->local). For other remote devices, the availability data is on a round trip basis. Test packets are sent at the specified interval for each enabled connection. The return of each packet will be matched with the
packets sent or wait the specified timeout period before declaring that packet lost. Packet payload contains EVC and packet sequence identifier information that aids in matching the returned packets to those sent. The remote 9145E adds additional information for one-way direction availability.

Modified Ping packets are sent to each remote to be monitored and await its return up to the timeout period. For networks where both ends of the virtual connection have 9145Es that support SA, separate availability data is maintained for each direction (Local to Remote (LR) and Remote to Local (RL)). For remote 9145Es that do not have SA, or other vendor equipment the availability determination is for Round Trip.

Availability results are logged and distributed to the Performance Collection System (PCS) application of CanogaView SEM periodically and whenever there is change of Availability State. The PCS stores and uploads Availability Results to an analysis or business system.

**9145E ARCHITECTURE TRAFFIC POLICING AND FILTERING DESCRIPTION**

**CoS Queuing**
The 9145E Architecture is able to queue both service frames and management frames using Weighted Fair Queuing (WFQ) scheme for service frames and eight CoS queues.

Management frames are classified and queued into one of two management queues. A high-priority management queue is reserved for Performance Measuring (PM) and Service Availability Monitoring (SAM) traffic, while a low-priority management queue is used for all other types of traffic. The low-priority queue is rate limited so that there is always sufficient bandwidth to the manager for PM and SAM traffic (and any other type of mission critical management traffic).
Figure 5 shows the functional blocks for the classification and queuing mechanisms for both the data and management plane.

Note that Classification, Early Detection (ED) and Queuing can be disabled. In this mode, both Service Frames and Management Frames (including PM and SAM frames) will not be classified on the data plane and will be subject to latency and jitter induced by a single FIFO buffer. In this case, the management frames would still be classified into two management queues (see Management Classifier & Queues heading below) to ensure PM and SAM frames are not discarded at the Manager.

**Pre-Queue Egress Demultiplexer**

When the Pre-Queue Egress Demultiplexer receives a frame, it checks to see whether the frame is a service frame or a frame destined for the manager (i.e., management frame). If the frame is a service frame, the Egress Demultiplexer forwards it to the Egress Multiplexer. If the frame is a management frame, the frame is inspected to see if it is an PM frame. If the management frame is an PM frame, it is also forwarded to the Egress Multiplexer, as the frame is required to pass through the Egress Queues. If the management frame is not an PM frame, it is forwarded to the Management Classifier.

**Egress Multiplexer**

The Egress Multiplexer functional block multiplexes frames forwarded by the Pre-Queue Egress Demultiplexer and by the Router to the Egress Classifier.
Statistics
There is a set of four statistics counters for each of the Early Detection (ED) Drop Profiles in the set. The four statistics counters are:

- TotalPacketsClassifiedToTheQueue: The number of packets that the Classifier classified to a particular queue.
- TotalPacketsSubjectToEDDropProfile: The number of packets subject to a particular ED Drop Profile.
- TotalPacketsQueued: The total number of packets queued after being subject to the ED function.
- TotalPacketsDropped: The total number of packets dropped after being subject to the ED function.

Ingress/Egress Queues
The initial release implements three Ingress/Egress Queues and one LLQ as shown in Figure 1. Release schedule for Q2 2008 increases this to eight queues. Each of the queues are enabled/disabled and size configured independently. The LLQ is configurable between 16 KB and 256 KB with the three remaining CoS queues between 16 KB and 8 MB.

Ingress/Egress Scheduler
The scheduler decides when to select packets for transmission from each of the queues. Queue 3, Queue 2 and Queue 1 can be configured independently to have packets selected for transmission using a Strict Priority or Weighted Fair Queuing (WFQ) scheduling scheme. The LLQ always has packets selected for transmission based on Strict Priority.

Strict Priority means that a queue of a particular priority is not serviced until the queue of higher priority is empty. Consider the example where Queue 3, 2 and 1 are all configured for Strict Priority scheduling. The LLQ is always scheduled by Strict Priority (i.e., it is not configurable). By default, the LLQ is the queue with highest priority, followed by Queue 3, then Queue 2 and finally Queue 1 (this increases to eight queues in the Q2 2008 Release). In this example, packets in the LLQ would be selected for transmission until the LLQ is empty. Only when the LLQ is empty would the scheduler select packets from Queue 3 to transmit. Similarly, packets from Queue 2 would not be selected for transmission until both Queue 3 and the LLQ are empty.

Consider another example where Queues are configured for WFQ scheduling. Strict Priority is always used to schedule the transmission of frames from the LLQ. When the LLQ is empty, the Egress Scheduler uses a WFQ algorithm to schedule the frames in the three Egress Queues for transmission. The weighting of each queue is configurable to a value of 1 to 1000.

For example, the output data rate (ODR) of an ETH flow $i$ with weight $w_i$ when all $N$ ETH flows are active is approximately:

$$ ODR = R \times w_i / (w_1 + w_2 + \ldots + w_N) $$

where $R$ is the link rate.

Obviously, this is a crude estimate that does not take into consideration that the LLQ is scheduled under strict priority. Hence, the OBW is always somewhat less than calculated when LLQ traffic is nominally small, but can drop to 0 Mbps when LLQ traffic approaches line rate.
Post-Queue Egress Demultiplexer

When the Post-Queue Egress Demultiplexer receives a frame, it is inspected to see if the frame is an PM frame. PM frames are forwarded to the Timestamp block. All other frames are forwarded to the User Port TX for transmission.

Management Classifier & Queues

The Management Classifier classifies frames into two queues: a high-priority queue and a low-priority queue. The high-priority queue is reserved for PM and SAM frames only, while the low-priority queue serves frames from all other protocols (SNMP, TELNET, SysLog, etc.). The low-priority queue is rate limited as to always allow PM and SAM frames sufficient bandwidth to the Manager. For the initial release, the size of these queues and the rate limit bandwidth on the low-priority queue are fixed and not configurable by the user.

Management Scheduler

The Management Scheduler is used to rate limit the low-priority management queue so that PM and SAM frames always have sufficient bandwidth to the manager.

Router

The Router is used to route frames from the Manager to the appropriate functional block. For example:

An PM Test Frame transmitted by the Manager would be routed to the Timestamp module before being queued to the Ingress Multiplexer. To obtain accurate Delay and Jitter measurements, the PM Test Frames travels through the same queues as Service Frames and are classified and queued at the ingress in the same manner as Service Frames.

If the link connecting the 9145E User Port to the CE employs 802.3ah OAM, the OAM PDUs transmitted by the Manager are not subjected to the traffic class queues, but are routed to a Low-Latency Queue (LLQ) before being transmitted by the Egress Scheduler.

Pre-Queue Ingress Demultiplexer

When the Pre-Queue Ingress Demultiplexer receives a frame, it checks to see if the frame is a service frame or a frame destined for the manager (i.e., management frame). If the frame is a service frame, the Ingress Demultiplexer forwards it to the Ingress Multiplexer. If the frame is a management frame, the frame is forwarded to the Management Classifier.

Ingress Multiplexer

The Ingress Multiplexer functional block multiplexes frames forwarded by the Pre-Queue Ingress Demultiplexer and by the Router to the Ingress Classifier.

Management Interface and Sample Menus

Canoga Perkins utilizes an easy to use menu driven Craft management interface instead of a cryptic Command Line Interface (CLI). Our customer have found the menu oriented interface reduces training and operator error. It also reduces the amount of reference material the Network Operations and Field personnel need since specific command structure need not to be remembered.

Following pages contain example screen shots of the 9145E.
9145E Sample Management Screens

9145E Main Screen

Canoga Perkins Corporation
20600 Prairie Street, Chatsworth, CA 91311

9145E System Configuration Selection Screen

Canoga Perkins Corporation
20600 Prairie Street, Chatsworth, CA 91311
9145E Hardware Configuration Screen

```
Canoga Perkins Corp.  Ethernet Network Interface Device  07-Jul-2008
Model 9145E-101-0-0 V02.01 F53  15:45:13

HARDWARE INFORMATION
-------------------------
NID Model Number         9145E-101-0-0
NID Hardware Rev.         A3
NID Serial Number         20070505144

SFP Information
User Port  Network Port
Model Number       SFP Not Present  SFP Not Present
Wavelength         N/A                N/A
Connector Type     N/A                N/A
Data Rate          N/A                N/A
Maximum Link Length N/A                N/A
Maximum Loss Budget N/A                N/A

Power Supply         AC 120/240

Press ESC to return to previous screen
```

9145E Performance Management Screen

```
Canoga Perkins Corp.  Ethernet Network Interface Device  07-Jul-2008
Model 9145E-101-0-0 V02.01 F53  15:46:12

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

1) To IP Addr  0.0.0.0  5) DF Bit  Clear
2) From IP Addr Auto Selection  6) DSCP Code (0 - 63)  0
3) Test VLAN  0  7) Test Packet Priority (0 - 7)  0
4) Test Packets per sec  1

B) Test Duration min:sec (0=forever)  0
9) Min Test Payload Size (40 - 9954)  40
10) Max Test Payload Size (40 - 9954)  40
11) Test Packet Timeout sec (1 - 10)  3
12) Start/Stop Test

Select [1-12]:
```

Canoga Perkins Corporation  September 2008
20600 Prairie Street, Chatsworth, CA 91311
Page 16
9145E CFM VLAN Loopback Statistics Screen

<table>
<thead>
<tr>
<th>User Port</th>
<th>Net Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBM Transmitted: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBM Received: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBM Mismatched: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBR Transmitted: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBR Received: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBR Out Of Sequence: 0</td>
<td>0</td>
</tr>
<tr>
<td>LBR Unexpected: 0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

9145E Port Status Screen

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

Select [1-4]:

* USR & NET ARE DOWN *
9145E Link and SFP Status Screen

Canoga Perkins Corp. | Ethernet Network Interface Device | 07-Jul-2008
Model 9145E-101-0-0 V02.01 F53 | 15:50:01

User Port | Link Down
Network Port | Link Down
MGMT UTP Port | Link Up

SFP Status:
- User SFP Rx Power: N/A
- User SFP Tx Power: N/A
- Network SFP Rx Power: N/A
- Network SFP Tx Power: N/A

Press ESC to return to previous screen

9145E VLAN Tagging Rules Screen

Canoga Perkins Corp. | Ethernet Network Interface Device | 07-Jul-2008
Model 9145E-101-0-0 V02.01 F53 | 15:51:18

Select [1-9]:

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

Select [1-9]:

Messages:
9145E 802.1AH OAM Configuration Screen

<table>
<thead>
<tr>
<th>Canoga Perkins Corp.</th>
<th>Ethernet Network Interface Device</th>
<th>07-Jul-2008</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model 9145E-101-0-0 V02.01 F53</td>
<td>OAM CONTROL</td>
<td>15:35:56</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Operational Status</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td></td>
<td>Link Fault</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Max PDU Size</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1518</td>
<td></td>
<td>1518</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Revision</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Functions Supported</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback</td>
<td></td>
<td>Link Events</td>
</tr>
<tr>
<td>Link Events</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Loopback Status</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Loopback</td>
<td></td>
<td>No Loopback</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OAM Remote Link Fault</th>
<th>User Port</th>
<th>Network Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

1) OAM Admin State Disabled Yes
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]:

9145E Alarms and Traps

- Master Trap Control (activates/deactivates sending of all traps)
- User Port Link Traps
- Network Port Link Traps
- Remote Fault Received Traps
- Link Loss Forwarding Traps
- Cold Start Traps
- Authentication Traps
- Diagnostic Traps
- Configuration Traps
- Fan/Power/Temperature Traps
- SFP Traps
- Management Port Alarms
- Link Loss Forwarding
- Remote Fault Forwarding
- Fan Status (Redundant Fans)
- Power Supply Status and Voltage
- Unit Temperature
VLAN STACKING IMPLEMENTATION

The 9145E Architecture supports VLAN Stacking (a.k.a “Q-in-Q” or “double-tagging”). The 9145E is configurable to:

a) Remove the outmost tag from a tagged packet.
b) Add a specific tag to all untagged packets it receives.
c) Add a specific tag to all tagged packets it receives.
d) Add a specific tag to all tagged packets it receives with p-bits equal to the p-bits of the tagged packets received.

Note: the use of the word “tag” above refers only to C-Tags compliant with IEEE 802.1ad.

The Q2 2008 Release adds IEEE 802.1ad compliant S-tags or C-tags. Additional configurations include:

a) Add/Remove a C-Tag to an untagged service interface.
b) Add/Remove an S-Tag to untagged service interface.
c) Add/Remove an S-Tag to a C-Tagged or S-tagged service interface.

S-Tags can be stacked on to tagged interfaces based on the packet’s incoming VID. The appended S-Tag can have user defined PCP and DEI settings.

Performance Measuring and Service Availability Monitoring is supported on both C-VLANs and S-VLANs, and in C-VLANs that are nested within S-VLANs.

The implementation does not restrict the number of tags that can be stacked (limited only by MTU size).
TRAFFIC STATISTICS

Overview

You can view these groups of statistics for Ethernet Packets sent through the 9145:

- **Layer 2 Statistics**
  - Link State
  - Speed/duplex
  - Frames Sent and Rcvd
  - Bytes Sent and Rcvd
  - Undersize (<64)
  - Oversize (>10000)
  - Frames > 1518
  - Frames > 1522

- **Layer 2 Error Statistics**
  - Link State
  - Frames Sent and Rcvd
  - Collisions
  - Alignment Errors
  - Undersize (<64)
  - Oversize (>10000)
  - Fragments
  - CRC Errors
  - Jabber Events
  - Dropped

- **Layer 2 Frame Type Statistics**
  - Link State
  - Frames Sent and Rcvd
  - Rx and Tx Broadcasts
  - Rx and Tx Multicasts
  - VLAN Tagged
  - Pause Frames
  - Rx and Tx Management

- **RMON Group 1 Statistics**
  - Drop Events
  - Octets Rcvd
  - Packets Rcvd
  - Broadcasts Rcvd
  - CRC/Align Errors
  - Undersize
  - Oversize
  - Fragments
  - Jabbers
  - Collisions
  - Packet Sizes 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518

Detail Listing

802.1ag Loopback Statistics
- LBM Transmitted
- LBM Received
- LBM Mismatched
- LBR Transmitted
- LBR Received
- LBR Received Out of Sequence
Layer 2 Port Traffic Statistics
   Bytes Sent
   Bytes Received
   Frames Sent
   Frames Received
   Undersized - <64 bytes
   Oversized - > Configured Max Frame Size
   Frames > 1518
   Frames > 1522
   Time since Last Counter Reset

Layer 2 Port Traffic Errors
   Frames Sent
   Frames Received
   Collisions
   Late Collisions
   Alignment Errors
   Undersized - <64 bytes
   Oversized - > Configured Max Frame Size
   Fragments
   CRC Errors
   Jabber Events
   Dropped Frames
   Time since Last Counter Reset

Layer 2 Port Frame Types Statistics
   Frames Sent
   Frames Received
   Broadcast Frames Received
   Broadcast Frames Sent
   Multicast Frames Received
   Multicast Frames Sent
   VLAN Tagged Frames
   Filtered Frames
   Pause Frames
   Management Frames Received
   Management Frames Sent

Per VLAN Traffic Statistics (Advanced Model Only)
   Bytes Sent
   Bytes Received
   Frames Sent
   Frames Received
   Filtered Frames
   Dropped Frames

RMON Group 1 Statistics (by port)
   Packets Received
   Octets Received
   Broadcast Packets Received
   Multicast Packets Received
   64 Octet Packets Received
65 to 127 Octet Packets Received
128 to 255 Octet Packets Received
256 to 511 Octet Packets Received
512-1023 Octet Packets Received
1024 to 1518 Octet Packets Received
Dropped Events
CRC/Alignment Errors
Undersized Packets - <64 Octets
Oversized Packets - >1518 Octets
Fragments
Jabbers
Collisions

OAM Statistics (by port, sent and received)
  Informational OAMPDUs
  Unique Event Notifications
  Duplicate Event Notifications
  Loopback Control Messages
  Variable Requests
  Variable Responses
  Organization Specific OAMPDUs
  Unsupported OP Codes
  Total OAMPDUs

OAM Link Events Statistics (by port, sent and received)
  Errored Symbol
  Errored Frame
  Dying Gasp Critical Event
  Link Fault
802.3AH OAM

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

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

When 802.3ah OAM Mode is disabled, the 9145E is transparent to 802.3ah OAMPDUs. All incoming OAMPDUs will pass through the 9145E transparently and the 9145E does not generate any OAMPDUs (effectively, the OAM Sublayer will be bypassed and all frames will be forwarded to the superior sublayer).

When a Remote Loopbacks are initiated or invoked from Local 9145E, it generates an event to the system log and generates an equivalent Syslog Message. Likewise, when a Remote Loopback is exited, the 9145E generates an event to the system log and an equivalent Syslog message.

There are three types of Link Events: Critical Link Events, Link Events and Dying Gasp Events.

Critical Link Events are defined as Link Fault, Dying Gasp and Critical Events. The definitions of the specific faults that comprise these events are defined here.

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

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

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

The 9145E supports five loopback modes, four compressive modes activated using Management interfaces (Telnet, local management port, SNMP/CanogaView) and one 802.1ag CFM mode. The Management activated modes loop the data through either the physical layer (PHY) on the User side or the FPGA when looping to the remote user link, or the FPGA when looping to the local user link. CFM Loopback mode is equivalent to the Remote-Remote Mode (figure 9 below).

Local-Local Mode
Local-Local Mode loops data received on the local User Port Rx through the FPGA to the User Port Tx. Data is not sent out the Extension (Network) Port Tx and incoming data on the Extension Port Rx is ignored.

Local-Remote Mode
Local-Remote Mode loops data received on the Extension (Network) Port Rx through the User side PHY to the Extension (Network) Port Tx. Data is not sent out the remote User Port Tx and incoming data on the remote User Port Rx is ignored.

Remote-Local Mode
Remote-Local Mode loops data received on the User Port Rx through the FPGA to the User Port Tx. Data is not sent out the remote Extension (Network) Port Tx and incoming data on the remote Extension (Network) Port Rx is ignored.
Remote-Remote Mode

Remote-Remote Mode loops data received on the Extension (Network) Port Rx through the Local User PHY to the Extension (Network) Port Tx. Data is not sent out the local User Port Tx and incoming data on the local User Port Rx is ignored.

![Remote-Remote Loopback Mode Diagram](image)

Figure 9 - Remote-Remote Loopback Mode

For loopbacks, the 9145E uses a unique MAC address, the Loop Test MAC Address, which is displayed on the Loopback Setup Screen. When in loopback mode, the 9145E filters the incoming packets to identify test packets identified by the MAC address. Loopback frames can be tagged with any VLAN ID. Frames are returned in the same VLAN as received.

The 9145E is configurable to swap the origination and destination MAC Addresses and to Recalculate the looped frame’s CRC. Test packets are returned to the source according to the selected options.

Mounting Options

The 9145E has flexible placement options including desktop/shelf, Wall and Rack mounting. Rubber Feet are including to facilitate desktop and shelf placement. Integral to the 9145E are holes for wall mounting. It can be placed with front panel facing right, left or down. Wall attachment is accomplished using a 2 #10 Screws. 19” and 23” Rack Mounting options include single unit and dual unit in 1RU of rack space.
## SFP Optics Offering

SFP Optics (100 Mbps, 1 Gbps) - 9145E Advanced and Standard Models

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>100 Mbps SFP Optics</strong></td>
<td></td>
</tr>
<tr>
<td>SFP1-1205</td>
<td>100Mbps, 1310nm, MM, 10dB (100BaseFX)</td>
</tr>
<tr>
<td>SFP1-2305</td>
<td>100Mbps, 1310nm 13dB</td>
</tr>
<tr>
<td>SFP1-2605</td>
<td>100Mbps, 1310nm 29dB</td>
</tr>
<tr>
<td>SFP1-3605</td>
<td>100Mbps, 1550nm 29dB</td>
</tr>
<tr>
<td><strong>100 Mbps Single Fiber BiDi SFP Optics</strong></td>
<td></td>
</tr>
<tr>
<td>SFP1-4305</td>
<td>100Mbps, BiDi, 1310nm, 20KM</td>
</tr>
<tr>
<td>SFP1-5305</td>
<td>100Mbps, BiDi, 1550nm, 20KM</td>
</tr>
<tr>
<td>SFP1-4405</td>
<td>100Mbps, BiDi, 1310nm, 40KM</td>
</tr>
<tr>
<td>SFP1-5405</td>
<td>100Mbps, BiDi, 1550nm, 40KM</td>
</tr>
<tr>
<td><strong>Gigabit Ethernet SFP Optics</strong></td>
<td></td>
</tr>
<tr>
<td>SFP1-2225</td>
<td>1000BaseLX, 1310nm, 10dB, 5km</td>
</tr>
<tr>
<td>SFP1-2725</td>
<td>1000BaseEX, 1310nm, 17dB</td>
</tr>
<tr>
<td>SFP1-0045</td>
<td>1.062 to 2.125 Gbps, 850nm, MM, 7dB (1000BaseSX)</td>
</tr>
<tr>
<td>SFP1-0055</td>
<td>1.062 to 2.125 Gbps, 850nm, MM, 7dB (1000BaseSX)</td>
</tr>
<tr>
<td>SFP1-2445</td>
<td>1.062 to 2.125 Gbps, 1310nm, 21dB</td>
</tr>
<tr>
<td>SFP1-3445</td>
<td>1.062 to 2.125 Gbps, 1550nm, 21dB</td>
</tr>
<tr>
<td><strong>Gigabit Single Fiber BiDi SFP Optics</strong></td>
<td></td>
</tr>
<tr>
<td>SFP1-4325</td>
<td>1 Gbps, BiDi, 1310nm, 20KM</td>
</tr>
<tr>
<td>SFP1-5325</td>
<td>1 Gbps, BiDi, 1550nm, 20KM</td>
</tr>
<tr>
<td>SFP1-4425</td>
<td>1 Gbps, BiDi, 1310nm, 40KM</td>
</tr>
<tr>
<td>SFP1-5425</td>
<td>1 Gbps, BiDi, 1550nm, 40KM</td>
</tr>
<tr>
<td><strong>100Mbps to 2.5 Gbps SFP Optics</strong></td>
<td></td>
</tr>
<tr>
<td>SFP1-2155</td>
<td>125 Mbps to 2.5 Gbps, 1310nm, 8dB FP, 22km @ 100Mbps, 5km @ 1.25Gbps, 2.5km @ 2.5Gbps</td>
</tr>
<tr>
<td><strong>CWDM SFP Optics - 100Mbps to 2.5 Gbps</strong></td>
<td></td>
</tr>
<tr>
<td>SFP2-2555</td>
<td>125 Mbps to 2.5 Gbps, 1310nm, 60KM</td>
</tr>
<tr>
<td>SFP2-4765</td>
<td>125 Mbps to 2.5 Gbps, 1470nm, 80KM</td>
</tr>
<tr>
<td>SFP2-4965</td>
<td>125 Mbps to 2.5 Gbps, 1490nm, 80KM</td>
</tr>
<tr>
<td>SFP2-5165</td>
<td>125 Mbps to 2.5 Gbps, 1510nm, 80KM</td>
</tr>
<tr>
<td>SFP2-5365</td>
<td>125 Mbps to 2.5 Gbps, 1530nm, 80KM</td>
</tr>
<tr>
<td>SFP2-5565</td>
<td>125 Mbps to 2.5 Gbps, 1550nm, 80KM</td>
</tr>
<tr>
<td>SFP2-5765</td>
<td>125 Mbps to 2.5 Gbps, 1570nm, 80KM</td>
</tr>
<tr>
<td>SFP2-5965</td>
<td>125 Mbps to 2.5 Gbps, 1590nm, 80KM</td>
</tr>
<tr>
<td>SFP2-6165</td>
<td>125 Mbps to 2.5 Gbps, 1610nm, 80KM</td>
</tr>
</tbody>
</table>
CanogaView SEM Element Manager Architecture

The CanogaView 2.0 Architecture builds on CanogaView 1.0 to provide an environment for the development, distribution, and maintenance of network management applications in a modular fashion to promote quick time to development, greater quality and reduced defects, and greater flexibility for the customer in terms of product updates and installation choices. Along with the architecture changes will be 5 packages developed using this architecture to support the new 9145E product, Layer 2 Statistics Monitoring, Performance Monitoring, Service Availability and a customized interface for supporting provisioning and accounting systems.

The CanogaView 2.0 Core system includes the infrastructure and core system services necessary to support separately available network management device packages and network management vertical applications. The core system infrastructure and system services will be component based to reduce dependencies and allow existing components to be enhanced and new components to be developed without requiring a complete rebuild or testing of the core system.

Based on the customer’s needs in terms of the devices deployed in their networks, network management device package will be available for installation to support those devices. Each device package is independent of any other device package and can be installed or removed at any time. The device packages will be firmware revision aware with separate independent releases of device packages to support specific device firmware releases to ensure that exiting device packages are not compromised in supporting new firmware releases.

CanogaView 2.0 provides necessary trouble shooting features of an element management system for use by carrier level OSS groups. Standards based PM and SA solutions are required for SLA support. Additionally, both PM and SA tests can be performed to aid the OSS groups in troubleshooting network issues.

The CanogaView 2.0 architecture benefits the Customer in multiple ways:

- Provides a multi-vendor standards based SLA, Performance Management and Service Availability Monitoring solution
- Enhanced reliability and scalability realized through the use of the Best Practices and Technology choices and the tried and tested application server platform services in the areas of redundancy and scalability.
- Provides a mechanism to introduce new functionality or improve existing functionality without a complete release of the CanogaView system. This limits or eliminates the qualification and testing required by the customer’s processes at major release points of new systems.
- Provides a customizable solution for the customer by allowing the customer to only install those services and device support packages as required by his deployed network infrastructure. This will reduce complexity and potential failure points and MAY reduce resource requirements of the CanogaView server platform.
- Provides a system monitoring and analysis feature through the performance monitoring packages that can be leveraged by the customer to provide support for Service Level Agreements to his customers.
CanogaView Core

CanogaView Core and Optional Packages