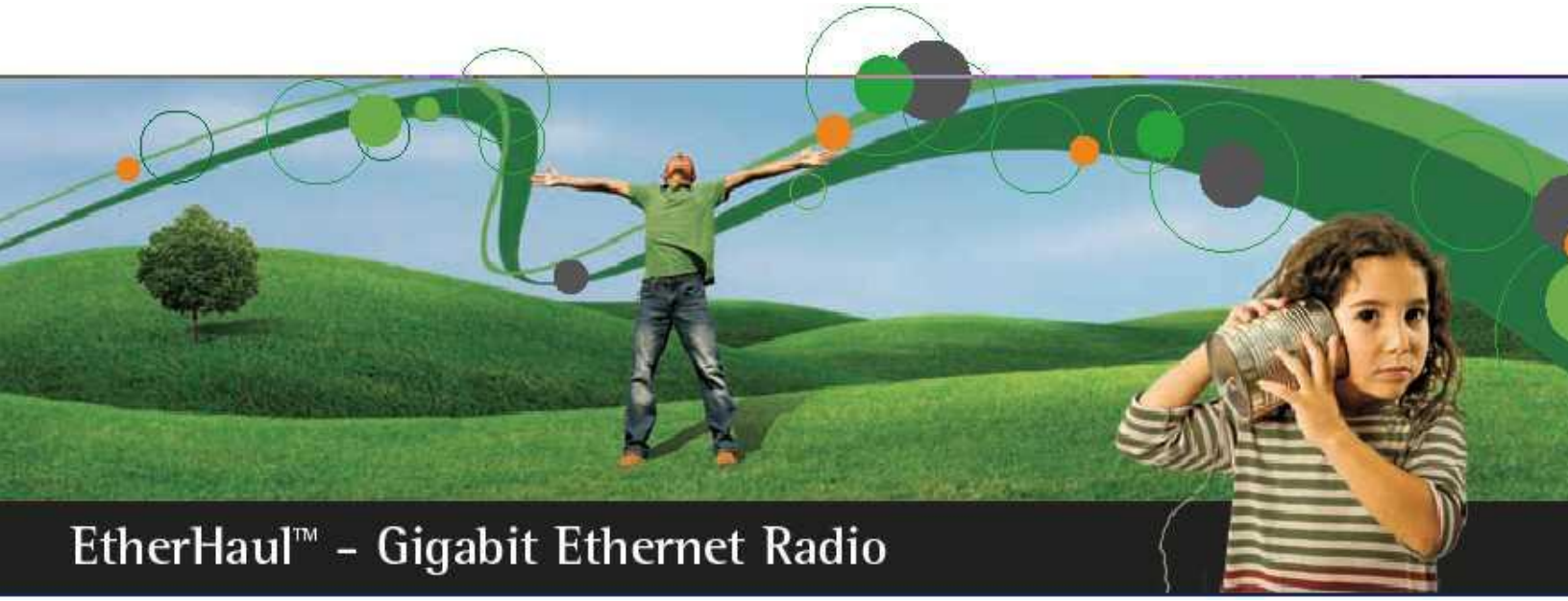


Siklu

EtherHaul 1200™

Gigabit Ethernet Wireless Solution

Installation and User Manual

EH-INST-02, Issue 3.0

June 2012

Trademarks

Siklu, the Siklu logo, and EtherHaul are all trademarks of Siklu Communication Ltd.

All other product names and trademarks mentioned in this document are trademarks or registered trademarks of their respective companies.

Copyrights

Disclaimers

The information contained in this document is subject to change without notice.

Siklu assumes no responsibility for any errors that may appear. Siklu makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein.

This document was originally written in English. Please refer to the English language version for a full and accurate description of all products and services described herein.

Safety and Regulatory Notices

The following are mandatory notices for installation and operation of EtherHaul 1200™ 70GHz Wireless Backhaul Link. Indications appearing here are required by the designated government and regulatory agencies for purposes of safety and compliance.

General

Do not install or operate this System in the presence of flammable gases or fumes. Operating any electrical instrument in such an environment is a safety hazard.

European Commission

This product has been designed to comply with CE markings in accordance with the requirements of European Directive 1995/5/EC.

This product has been designed to comply with the requirements of European Directives.

This equipment must be permanently earthed for protection and functional purposes. To make a protective earth connection, use the grounding point located on the System ODU using a minimum amount of 16AWG grounding cable or according to local electrical code.

This apparatus is intended to be accessible only to authorized personnel. Failure to prevent access by unauthorized personnel will invalidate any approval given to this apparatus.

This product is in full compliance with the following standards:

- RF EN 302 217-3 1.3.1
- EMC EN 301 489-4
- Safety IEC 60950
- Operation EN 300 019-1-4 Class 4.1E
- Storage EN 300 019-1-1 Class 1.2
- Transportation EN 300 019-1-2 Class 2.2

About this Document

This document is the Installation and User Manual for the EtherHaul 1200™ 70GHz Wireless Link.

Audience

This document assumes a working knowledge of wireless backhaul platforms and their operating environments.

This document is intended for use by all persons who are involved in planning, installing, configuring, and using the EtherHaul system.

Conventions

The following conventions are used in this document in order to make locating, reading, and using information easier.

Special Attention

Hint:

Informs you of a helpful optional activity that may be performed at the current operating stage.

Note:

Provides important and useful information.

Caution:

Describes an activity or situation that may or will interrupt normal operation of the EtherHaul system, one of its components, or the network.

Text Conventions

Document References	Italicized text is used to reference sections or chapters in this document. In many cases, references use clickable hypertext links that enable immediate access to referenced objects.
`Command Input`	Monospace text is used to help delineate command line user input or text displayed in a command window.

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction to the EtherHaul™ 1200 System

Siklu's EtherHaul 1200 is a carrier-class, high-capacity E-band radio that dramatically lowers the cost of wireless and Ethernet backhaul. The system is uniquely based on an all-silicon design that results in fewer components, greater reliability, and pricing that is up to 80% less than comparable radio systems. Operating in the uncongested and inexpensive licensed 71-76 GHz E-band, TCO (total cost of ownership) is reduced even further to the lowest in the industry.

The following are just some of the highlights of the EtherHaul 1200 system:

- Operates in the licensed, uncongested, and inexpensive 71-76 GHz E-band
- Carrier-grade Gigabit Ethernet radio
- Revolutionary all-silicon-based design, resulting in the industry's lowest TCO
- Priced at as little as one-fifth the cost of available wireless radio alternatives
- Green design providing for extremely low power consumption, small form factor, and easy installation
- Perfect wireless backhaul solution for mobile operators, business service providers, and enterprises

This chapter provides a brief overview of the EtherHaul 1200 system, its features, and its specifications, including:

- System Applications
- Main Features
- Functional Description
- Licensing
- Management
- Technical Specifications

Figure 1-1 EtherHaul 1200 System

1.1 System Applications

Wireless Backhaul for 2G, 3G, 4G, LTE, and WiMAX Networks

High-capacity Gigabit Ethernet backhaul at the lowest TCO in the industry enables mobile operators to provide data-intensive services profitably and reliably.

- EtherHaul 1200 uses the uncongested and interference-free licensed E-band 71-76 GHz wireless spectrum, enabling fast and efficient frequency and network planning and deployment. As a bonus, licensing registration processes for this band are cheaper, simpler, and quicker.
- With 1 Gbps throughput, the EtherHaul 1200 radio future-proofs the backhaul network to meet the growth in demand for data capacity from 4G, LTE, and WiMAX installations.
- Carrier-class Ethernet provides QoS and OAM with standards-based support for ring, mesh, and multi add-drop topologies, assuring resiliency and high availability.
- EtherHaul 1200's bandwidth-aware QoS mechanism differentiates between multiple services, guaranteeing efficient transport of timing, signaling, voice, video, web surfing, and more.
- Advanced timing over packet handling (SyncE, IEEE 1588) enables migration to packet-based backhaul.

- All-outdoor unit eliminates co-location fees and costs associated with indoor installations, and enables fast deployment at any cell-site.
- Low power consumption delivers 80% energy savings.

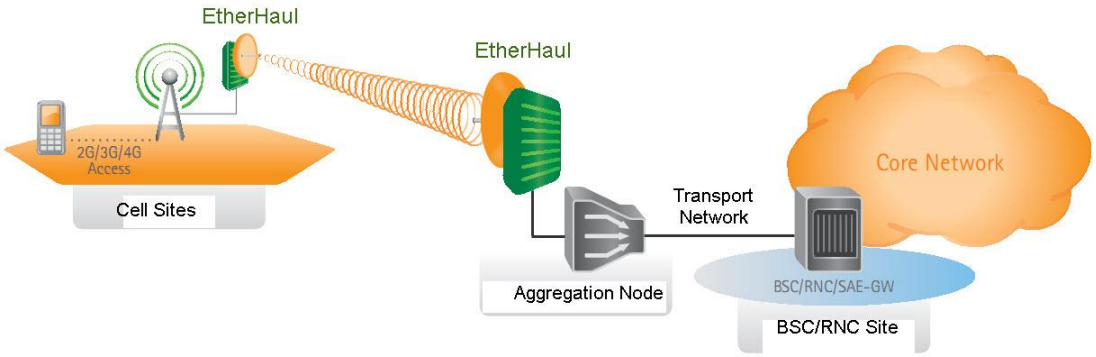


Figure 1-2 Wireless Backhaul for 2G, 3G, 4G, LTE, and WiMAX Networks

Ethernet Wireless Backhaul for Business Services and Enterprise Connectivity

A low cost, high capacity Ethernet wireless solution enables you to rapidly extend your fiber reach beyond your existing fiber footprint or to expand your enterprise network.

- EtherHaul 1200 operates in the licensed E-band 71-76 GHz wireless spectrum, with significantly lower licensing fees and simpler and quicker licensing registration processes, for rapid service deployment.
- 1 Gbps throughput delivers enough capacity to support voice, video and high speed data services.
- EtherHaul 1200's advanced Carrier Ethernet capabilities enable differentiated QoS, maintaining diverse SLAs for multiple services and customers.
- EtherHaul 1200's all-outdoor unit eliminates the need for a dedicated indoor cabinet and enables rapid roll-out with minimal site preparation.
- EtherHaul 1200's zero footprint and flexible installation options enable deployment in any urban, business, or residential environment.
- EtherHaul 1200's low power consumption enables the use of standard PoE supplies, connecting the radio with a single cable for both power and data.

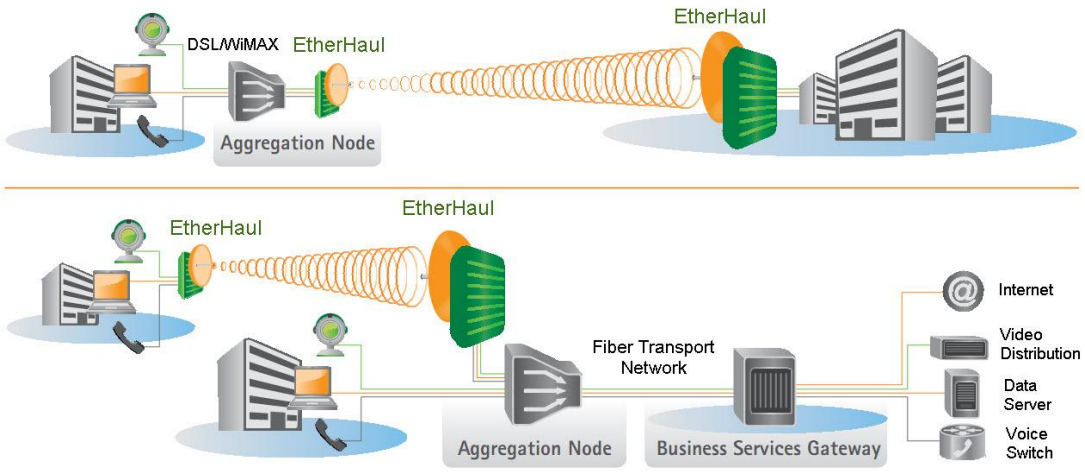


Figure 1-3 Wireless Backhaul for Business Services and Enterprise Connectivity

1.2 Main Features

Siklu's EtherHaul 1200 wireless backhaul radio link operates in the new E-band spectrum, which provides clear technological and economical advantages over the existing lower frequency bands. Taking advantage of the new spectrum, the EtherHaul 1200 enables easy migration to support Gigabit throughput, enabling operators to enhance bandwidth capacity on a "pay as you grow" basis. Supporting point-to-point, daisy-chain, ring, and mesh configurations, the EtherHaul system offers carrier class availability and services.

The following are some of the main features of the EtherHaul 1200 (availability of features depends on platform):

All-Outdoor Packet E-band Radio

- Operates in the licensed 71-76 GHz E-band
- Up to 1 Gbps throughput
- Asymmetric capacity configuration
- High gain narrow beam-width directional antenna
- Low latency

Highest Spectral Efficiency in E-band Spectrum

- 250 MHz, 500 MHz channel bandwidth
- Advanced hitless/errorless Adaptive Bandwidth, Coding and Modulation (ABCM) for a large dynamic range
- Configurable center frequency across the entire band

Carrier Ethernet Inside:

- Integrated Gigabit Ethernet switch
- Advanced bandwidth-aware QoS capabilities
- Advanced service management and OAM
- SyncE and optimized transport of IEEE 1588
- Ring, mesh, and Link Aggregation (1+1, 2+0) for carrier class availability and resiliency
- Standard-based for seamless integration into existing networks and multi-vendor interoperability
- Seamless software upgrades to MPLS, IP, and beyond

Carrier Grade:

- CLI, SNMP, or web-based local and remote management
- Extremely high reliability with high MTBF
- Designed for ultra-low MTTR without the need for antenna realignment

Green Design:

- Zero footprint, all-outdoor, extremely light weight
- Ultra low power consumption
- Standard IEEE 802.3at Power over Ethernet (PoE)

Quick and Easy Installation

- Rapid and flexible deployment
- Precise antenna alignment
- Minimal site preparation

Security

- Advanced AES encryption and security
- Narrow and secure beam-width

1.3 Functional Description

The EtherHaul 1200 system consists of an outdoor unit (radio link unit and antenna).

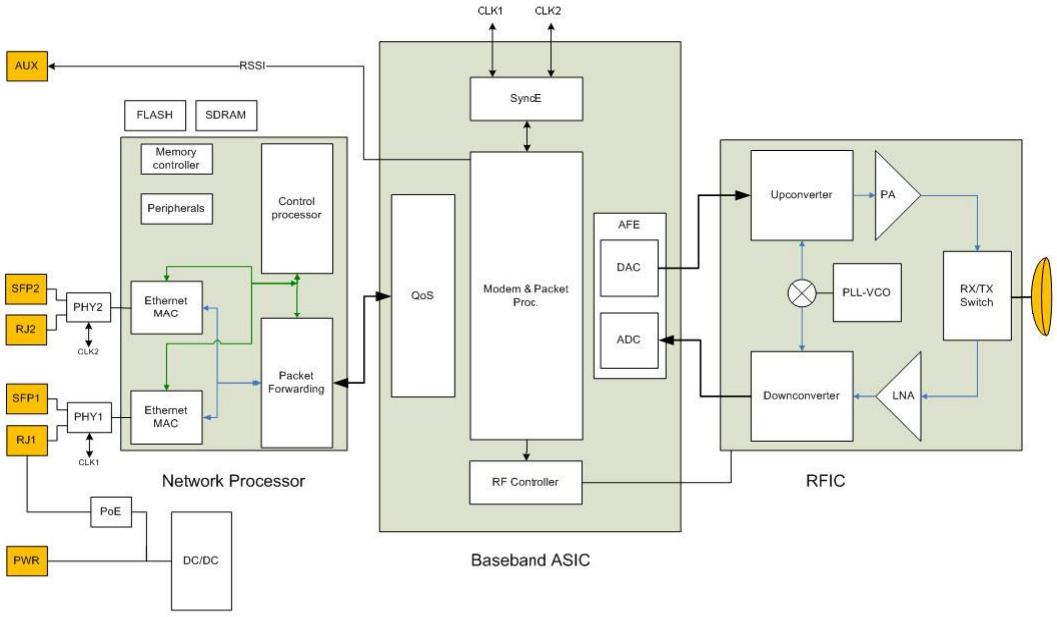


Figure 1-4 EtherHaul 1200 Functional Block Diagram

RFIC – Siklu's integrated Silicon Germanium (SiGe) transceiver operating at 71-76 GHz.

Modem/Baseband ASIC – Siklu's modem/baseband ASIC includes the modem, FEC engines, and Synchronous Ethernet support.

Network Processor – The network interface consists of two integrated 100/1000 Ethernet MAC I/F. The block is suitable for both copper and fiber interfaces by using the external PHY.

The networking engine is the heart of the high speed bridge/router function. The engine receives packets from both Ethernet interfaces and from the modem. It is responsible for proper forwarding between these three ports.

Host processor (integrated with the network processor) – The general purpose host processor controls the system, and the antenna alignment system. The processor is integrated with standard peripherals such as memory controller, communication I/F, WD, GPIO, and motor controller.

Antenna – Siklu's self-designed, innovative antenna is designed for best price-performance ratio.

1.4 Licensing

The EtherHaul 1200 provides for easy migration to support Gigabit throughput, enabling operators to enhance bandwidth capacity on a "pay as you grow" basis as well as adding

features and capabilities according to their networks evolutions. You can order the following EtherHaul 1200 software (capacity steps and feature availability depend on your platform):

- Data rates
- Layer 2 networking capabilities –OAM and Resiliency.
- Synchronization – Synchronous Ethernet (ITU-T G.8261)
- Encryption

Vlan configuration and Provider-Bridge settings capabilities are enabled by default and do not require a license.

The software licenses are serial number dependent.

1.5 Management

You can manage an EtherHaul 1200 system using a Web-Based Element Management System (Web EMS) or a Command Line Interface (CLI). The CLI is compatible with SNMP.

Advanced network features must be managed using the CLI.

The EtherHaul system features a wide range of built-in indicators and diagnostic tools for advanced OAM functionality. The system is designed to enable quick evaluation, identification, and resolution of operating faults. See *EtherHaul Diagnostics* on page 140.

1.6 Technical Specifications

For detailed technical specifications please refer to the datasheet.

2 Installing the EtherHaul 1200

This chapter describes how to install and perform the basic setup for EtherHaul antenna outdoor units (ODUs) in an EtherHaul wireless network, including:

- Preparing the Site
- EtherHaul 1200 Package Contents
- Unpacking the EtherHaul 1200
- Required Tools
- Preparing for Installation
- Mounting the EtherHaul 1200
- Connecting the Cables
- Aligning the Antenna
- Performing Initial System Setup

Note:

The installation and maintenance of the EtherHaul 1200 link should only be done by service personnel who are properly trained and certified to carry out such activities.

2.1 Preparing the Site

Carefully select and prepare each EtherHaul ODU site to make device installation and configuration as simple and trouble-free as possible. During site selection and preparation, always consider the long-term needs of both your network and your applications.

2.1.1 Physical and Environmental Requirements

Each EtherHaul ODU site should adhere to the following requirements:

- There must be a clear, unobstructed line-of-sight between ODU nodes.
- The EtherHaul ODU must be mounted on a fixed, stable, permanent structure. A reinforced steel mounting pole is required, with a diameter measuring from 2-4 inches (5-10 centimeters).

Caution:

Do not mount the EtherHaul device on a structure that is temporary or easily moved. Doing so may result in poor service or equipment damage.

- The EtherHaul ODU must be mounted in a site that is easily accessible to authorized personnel, and only authorized personnel.
- Operating Temperature – -45° ÷ +55°C

- Relative Humidity – 0 to 100%
- Maximum Altitude – 4,500m
- Ingress Protection Rating – IP67

2.1.2 Cabling Requirements

- Ensure that your power connection cable matches the EtherHaul power connector pin-outs. See *Figure 2-3* for the DC power connector pin-out diagram.
- Install the EtherHaul ODU where network connections and optional power cabling are ready for operation and easily accessible.
- All cabling connected to the ODU should be outdoor-grade, with UV protection.
- Use a 2-wire cable (14-18 AWG) to connect the power supply to the ODU.
- Outdoor Cat5e cables terminated with RJ45 connectors should be used. Shielded cables and connectors should be used.
- In order to protect indoor equipment, surge protection circuits must be installed on all copper cables (DC and Ethernet) on their entrance to the building.
- Install the EtherHaul ODU in a location where proper electrical outdoor grounding is readily available. Typically, the grounding connection is attached directly to the mounting pole. If not already present, then suitable structure-to-earth grounding connections must be created before installation. Ground the ODU using a minimum quantity of 16AWG grounding cable or according to local electrical code.

Note:

Improper electrical grounding can result in excessive electromagnetic interference or electrical discharge.

Siklu will not be held responsible for any malfunction or damage in the event that the ODU is not properly grounded.

2.2 EtherHaul 1200 Package Contents

An EtherHaul 1200 link consists of two ODUs and two mounting assemblies.

The EtherHaul 1200 package includes the following components:

Package	Description	Quantity
EtherHaul 1200 ODU		
	EtherHaul 1200 ODU (including antenna and radome)	1
	Connecting Cable All-Weather Shells	3

Package	Description	Quantity
	Unit Grounding Cable (90 cm)	1
	DC Cable Terminal Block Connector	1
EtherHaul 1200 Mounting Assembly		
	EtherHaul 1200 Mounting Assembly	1

You must examine all EtherHaul package contents carefully upon arrival. If a component is missing or damaged, contact your EtherHaul distributor before attempting to install the equipment.

2.3 Unpacking the EtherHaul 1200

When you unpack the components of the EtherHaul 1200, it is important to use care so as to avoid damaging or scratching the antenna radome:

- Do not touch the radome when unpacking the ODU.
- Do not rest the ODU face down or touch the radome. It is crucial to prevent contact between the radome and other objects.

2.4 Required Tools

Ensure that you have the following tools with you when performing an EtherHaul installation:

- Standard handheld digital voltage meter (DVM) with probes
- Standard open-end wrench, 13 millimeter
- Philips screwdriver (medium size head for grounding connection)
- 8mm Allen key for ODU installation with 2ft antenna
- Cable ties (for securing network and optional power cables)
- Cutter
- Cable labeling

2.5 Preparing for Installation

- EtherHaul units must be installed in pairs, working with two technicians. One technician must be located at each node, in order to align and calibrate each antenna ODU with its remote node pair for best performance.
- The expected receive signal strength for each antenna ODU (read from the DVM) must be calculated prior to installation, based on the network link budget.

Calculating the expected RSSI:

$$\mathbf{RSSI = P_{tx} + G_{ant1} – LFS – Att_{atm} + Gant2}$$

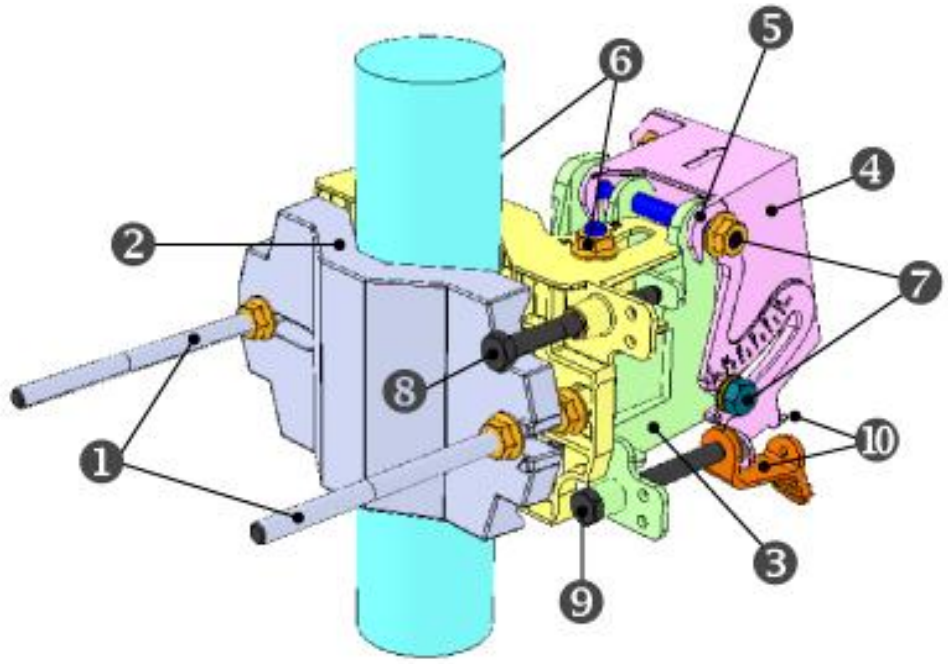
Where:

- P_{tx} – ODU's Tx Power (typically +5dBm)
- Gant1 – Gain of antenna 1 (in dBi)
- Gant2 – Gain of antenna 2 (in dBi)
- LFS – Loss of Free Space = 92.45+20*Log (D_{Km}*F_{GH}z)+
  - D - Link distance in Km
  - F – Frequency in GHz)
- Att_{atm} – Attenuation due to Atmospheric gases (~0.5dB/Km)= 0.5* D_{Km}

2.6 Mounting the EtherHaul 1200

Note: These instructions are for mounting a system with a one-foot antenna. For instructions on mounting the EtherHaul 1200 with a two-foot antenna, refer to **Appendix A: Install the ODU with Two Foot Antenna**.

Figure 2-1 shows the components of the EtherHaul 1200 Mounting Assembly.



1. Unit Mounting Screws and Bolts
2. Back Mounting Bracket
3. Front Mounting Bracket
4. Quick Release Plate (Attached to ODU)
5. Quick Release Hooks
6. Azimuth Adjustment Lock Bolts
7. Elevation Adjustment Lock Bolts
8. Azimuth Fine Adjustment Screw (± 8°)
9. Elevation Fine Adjustment Screw (± 16°)
10. Elevation Screw Tension Band and Pin

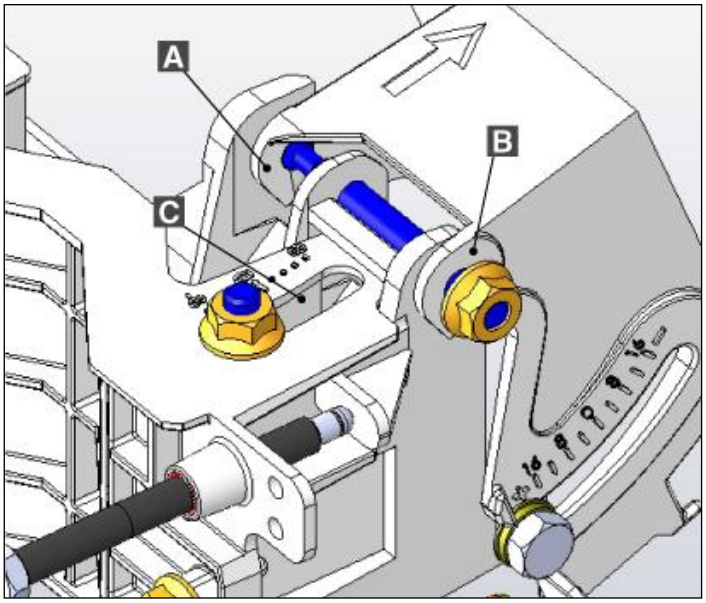
Figure 2-1 EtherHaul 1200 Mounting Assembly Components

1. Prior to mounting, unpack the mounting kit package and attach the two Unit Mounting Screws (❶) to the Front Mounting Bracket (❸), securing them with Mounting Bolts.
2. Assemble the Back (❷) Mounting Bracket to the Front (❸) Mounting Bracket using one bolt and separate them by about 120 degrees so that the Assembly can to be attached to the mounting pole.
3. Place the Assembly on the mounting pole and rotate the Front and Back Mounting Brackets to close the Assembly on the pole. Replace the Unit Mounting Bolt that was removed.

4. Ensure that both Front and Back Mounting Brackets are attached evenly to the pole, and are completely level.
5. Use the 13mm open wrench to tighten the nuts on both Unit Mounting Bolts. Temporarily tighten the Unit Mounting Bolts at this stage to keep the unit from moving freely.
6. By default, the ODU is delivered with the Quick Release Plate (❹) securely attached in a vertical polarization. If necessary, change the ODU polarization to match the orientation of the remote ODU by removing the Quick Release Plate, changing its orientation, and reattaching. For ease of reference, the markings "V" (vertical) and "H" (horizontal) are engraved on the back side of the ODU.
7. Examine the position scales of both the Azimuth Adjustment Lock Bolts (❻) and the Elevation Adjustment Lock Bolts (❼), found on the Front Mounting Bracket, and ensure that they are positioned at 0 degrees (in the middle of the scale).
8. Position the Quick Release Hooks (❺) onto the top Elevation Adjustment Lock Bolt (❼) and carefully set the ODU in place on the Front Mounting Bracket and slide it firmly inwards.

Hint:

Mount the ODU by attaching the Interior Quick Release Hook (A) in place **before** attaching the Exterior Hook (B). The Interior Hook is the one located farthest from the tightening nut, as shown below.

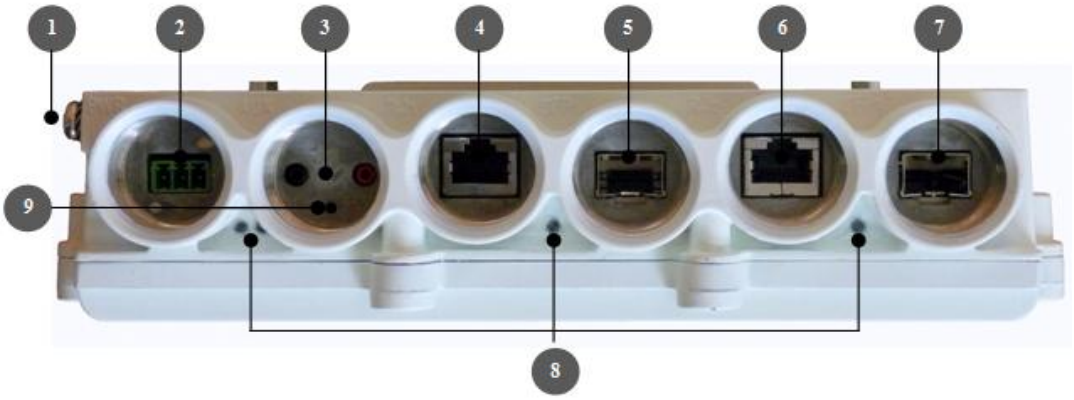


A. Interior Quick Release Hook **B**. Exterior Quick Release Hook **C**. Elevation Position Slot

9. **Unlock** the Azimuth Adjustment Lock Bolts (❻) and the Elevation Adjustment Lock Bolts (❼).
10. Stretch the Elevation Screw Tension Band (❿) slightly and connect it to its mating Tension Pin, located on the Quick Release Plate.

2.7 Connecting the Cables

Figure 2-2 shows the ODU interfaces. There are two Ethernet interfaces, Eth1 and Eth2. For each of these interfaces, you can choose between an optical (Fiber Cable SFP) and electrical (Ethernet Cable RJ45) physical interface. A power over Ethernet (PoE) connection can only be made via the first Ethernet RJ45 interface (RJ1).



1. Electrical Ground Outlet (GND)
2. Power Connector Interface (PWR)
3. DVM Probe Interface (AUX)
4. Ethernet Cable RJ45 Interface (RJ1)
5. Fiber Cable SFP Interface (SFP1)
6. Ethernet Cable RJ45 Interface (RJ2)
7. Fiber Cable SFP Interface (SFP2)
8. System LEDs
9, Reset Button (press for more than 5 seconds to restore factory defaults)

Figure 2-2 EtherHaul 1200 Connection Panel Details

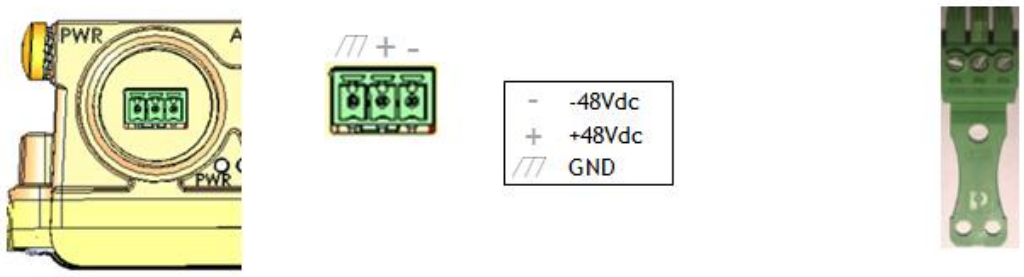


Figure 2-3 EtherHaul 1200 DC Power Connector Pin-Out Diagram

2.7.1 Grounding the EtherHaul 1200

The location of the Electrical Ground Outlet on the ODU is shown in *Figure 2-2*.

1. Connect one end of the Grounding Cable to the Ground Outlet on the left side of the ODU using the Grounding Cable Lug.
2. Tighten the lug securely in place.
3. Connect the opposite end of the Grounding Cable to the earth connection, typically located on the mounting pole. If the earth connection is out of reach of the Grounding Cable, install an alternative cable.

Figure 2-4 ODU with Grounding Cable Connected

2.7.2 Power Supply Notes

- The DC power input range of the ODU is 21 ÷ 57 VDC.
- The DC supply should be limited to 2 Ampere to avoid surges and possible damage to the ODU. For that, limited power supply or circuit breaker should be used (fast-blow fuse). The circuit-breaker is the disconnecting device, and should be readily accessible.
- When connecting the ODU to a MAINS DC distribution system, 2 Ampere circuit breaker should be used to enable the central DC system to isolate the ODU in an emergency case.
- One poly circuit breaker should be used and should be connected on the live voltage: (+) or (-). The other poly should be grounded.

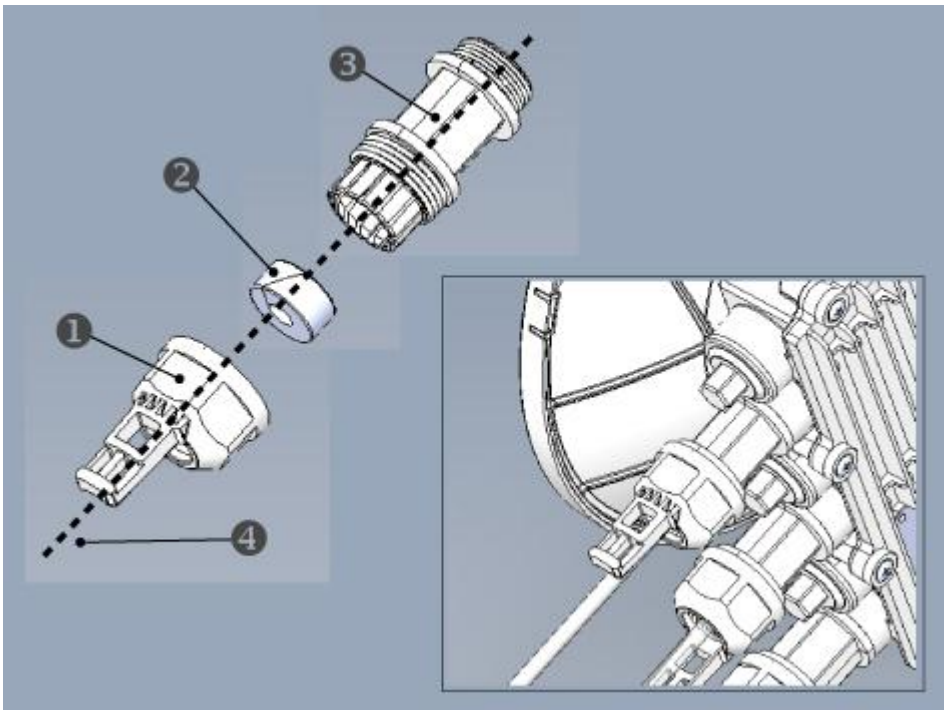
- The circuit breaker should be connected to the (+) or (-) live voltage.
- The DC input is floating, so either (+) or (-) can be connected to the GND on the power supply side. For the sake of consistency with other systems, Siklu recommends that you connect the (+) to the GND.
- Use a 2-wire cable (14-18 AWG) to connect the power supply to the ODU. On the ODU DC terminal, connect only the (+) and (-) wires. Do not connect to the ODU's GND input.

Caution:

Disconnect all power cables before service!

2.7.3 Preparing the Cables

Before inserting a cable connector into the ODU, you must first enclose the cable connector in a protective All-Weather Shell. 3 sets of All-Weather Shells are provided with the ODU for the ODU interfaces. The protective All-Weather Shell assembly is shown in *Figure 2-5.*



1. Cable Inlet Portion
2. Rubber Gasket Insert
3. Connector Outlet Portion
4. Ethernet Cable

Figure 2-5 All-Weather Connecting Cable Shell Assembly

3 sets of Rubber Gasket Insert are provided for different cable diameters:

- 4.2mm inner diameter – for cable diameter 3.5-4.9mm
- 5.8mm inner diameter – for cable diameter 5.0-6.7mm
- 7.9mm inner diameter – for cable diameter 6.8-9.0mm

1. For each ODU cable connection, perform the following procedure:
   a. Disassemble a protective shell by unscrewing its parts and carefully removing the Rubber Gasket Insert (❷) from the Cable Inlet Portion (❶) of the shell.
   b. Thread the cable connector through the Cable Inlet Portion (❶)of the shell, through the Rubber Gasket Insert (❷) and through the Connector Outlet Portion (❸) as shown in *Figure 2-5*.
   c. Connect the cable connector to the ODU interface.
   d. Screw the Connector Outlet Portion (❸) to the ODU firmly by hand (do not use tools).
   e. Insert the Rubber Gasket Insert snugly into the Connector Outlet Portion (❸) of the shell.
   f. Screw the Cable Inlet Portion (❶) to the Connector Outlet Portion (❸)firmly by hand (do not use tools).

2.7.4 Removing Connectors from the EtherHaul ODU

Caution:

To avoid accidental damage to the connector, always use the following order to remove cable connections from the ODU (refer to *Figure 2-5*).

1. Unscrew the Cable Inlet Portion (❶) of the All-Weather Shell first to release the gasket seal and remove tension from the cable connector.
2. Unscrew the Connector Outlet Portion (❸) of the All-Weather Shell from its ODU port.
3. Remove the cable connector from its port.

2.7.5 Connecting the Power

1. Carefully screw the Connector Outlet Portion (❸) of the All-Weather Shell into the PWR port or alternatively, if a PoE connection is being used, the RJ1 port. Tighten the Connector Outlet Portion securely by hand. **Do not use a wrench**.
2. Insert the power or PoE data connector into the port. The PWR LED color indicator will turn red for one second, then blinking green. This indicates that the ODU is powered on.
3. Screw the Cable Inlet Portion (❶) of the All-Weather Shell onto the secured Connector Outlet Portion, taking care not to twist the connecting cable. Tighten

the Cable Inlet Portion securely by hand. The Rubber Gasket Insert (❷) will tighten to create a moisture-proof seal. **Do not use a wrench**.

4. Secure the power supply cable into place using a cable tie. Ensure that there is sufficient play in the cabling to allow movement of the ODU during final alignment.
5. Wait for the EtherHaul ODU to boot up (about two minutes). When the ODU is fully rebooted, the PWR LED color indicator will turn green (during power-up the PWR LED will blink green) and the RF LED color indicator will turn off, indicating that the link is down.

2.7.6 Connecting Other Interfaces

For each network connection, perform the following steps:

1. Carefully screw the Connector Outlet Portion (❸) of the All-Weather Shell into the appropriate port. Tighten the Connector Outlet Portion securely by hand. **Do not use a wrench**.
2. Insert the RJ45 or SFP connector into the port.
3. Screw the Cable Inlet Portion (❶) of the All-Weather Shell onto the secured top portion, taking care not to twist the connecting cable.
4. Tighten the bottom portion securely by hand. The Rubber Gasket Insert (❷) will tighten to create a moisture-proof seal. **Do not use a wrench**.
5. Secure the network connection cable into place using a cable tie. Ensure that there is sufficient play in the cabling to allow movement of the ODU during final alignment.

2.8 Aligning the Antenna

The ODU antenna must be aligned on both local and remote ODUs. You must first perform coarse alignment on each ODU, followed by fine alignment. Accurate alignment of the ODU is critical for achieving the strongest possible receive signal.

In order to perform antenna alignment, the ODU must be in Alignment Mode.

The ODU has three modes of operation:

- **Alignment** – Carrier Wave transmission. Used for antenna alignment.
- **Adaptive** – Operational mode used with Adaptive Bandwidth, Code, and Modulation.
- **Static** –Operational mode used with a fixed modulation profile.

ODUs are shipped from the factory in Adaptive Mode.

2.8.1 Setting the ODU to Alignment Mode

Switch the EtherHaul ODUs to Alignment Mode by inserting the DVM probes into the DVM Probes at the AUX Interface. Following this action, the RF LED color indicator will turn orange, indicating the ODU is in Alignment mode.

The ODU will remain in Alignment Mode even if the DVM probes are ejected, until the ODU is rebooted.

2.8.2 Performing the Alignment

Note:

These instructions are for aligning a one-foot antenna. For instructions on aligning a two-foot antenna, refer to **Appendix A: Install the ODU with Two Foot Antenna.**

These instructions refer to Figure 2-6 EtherHaul 1200 Mounting Assembly Components

1. Verify that the ODU is in Alignment Mode. Refer to *Aligning the Antenna* on page 31.

Coarse Alignment (Azimuth Only)

2. Loosen the Unit Mounting Bolts (❶) slightly in order to allow the ODU some freedom of movement.
3. Perform a coarse ODU alignment using a line-of-sight visual check with the remote EtherHaul ODU. Lock the Unit Mounting Bolts (❶) using the 13mm open wrench.
4. Repeat Steps 1 to 3 above on the remote ODU.

Fine Alignment

Note:

When aligning an antenna, the antenna in the remote node must remain completely stationary. Fine alignment is performed first on the local antenna, and only afterwards on the remote antenna.

The optimum alignment may require several adjustment iterations between the local and remote antennas.

5. Connect the DVM to the ODU by inserting both red and black probes into their appropriate positions in the AUX port (*Figure 2-2)*.

   Throughout the alignment procedure, you must compare the actual receive signal strength indication (RSSI) to the expected RSSI that was calculated during network link budget preparation (refer to *Preparing for Installation* on page 23).

   Read the receive level (RSSI) using the DVM. The voltage reading will be between 0 to 1V, indicating the RSSI in dBms. For example, a DVM reading of 0.45 V is equivalent to -45 dBm.

6. Align the fine azimuth axis. Use the hexagonal wrench to adjust the Azimuth Fine Adjustment Screw (❽). Be sure to sweep the complete range of the azimuth in order to determine the maximum received signal strength position.

   When the optimum axis is achieved, tighten both Azimuth Adjustment Lock Bolts (❻).

7. Align the fine elevation axis. Use the hexagonal wrench to adjust the Elevation Fine Adjustment Screw (❾). Be sure to sweep the complete range of the elevation in order to determine the maximum received signal strength position.

   When the optimum axis is achieved, tighten both Elevation Adjustment Lock Bolts (❼).

8. Perform Steps 6 and 7 for the remote ODU.
9. Repeat Steps 6 and 7 for the local ODU.
10. Use the DVM to verify maximum received signal strength on both local and remote ODUs. For best performance, measured RSSI should be within ±4 dB of the calculated value.
11. Once the optimum position has been achieved for the ODU pair, tighten the azimuth adjustment lock bolts (❻) on one ODU, being very careful not to move the ODU when tightening.
12. Tightening the azimuth adjustment lock bolts will tilt the ODU, so realign the elevation again for optimum position.
13. Once the optimum position has been achieved for the ODU pair, tighten the elevation adjustment lock bolts (❼) on the ODU, being very careful not to move the ODU when tightening.
14. Repeat steps 11 through 13 for the second ODU.
15. Use the DVM to verify that the received signal strength has not changed on either the local or the remote ODU after final tightening of the brackets.

Antenna alignment is now complete.

Figure 2-7 shows the EtherHaul 1200 after it has been completely installed.

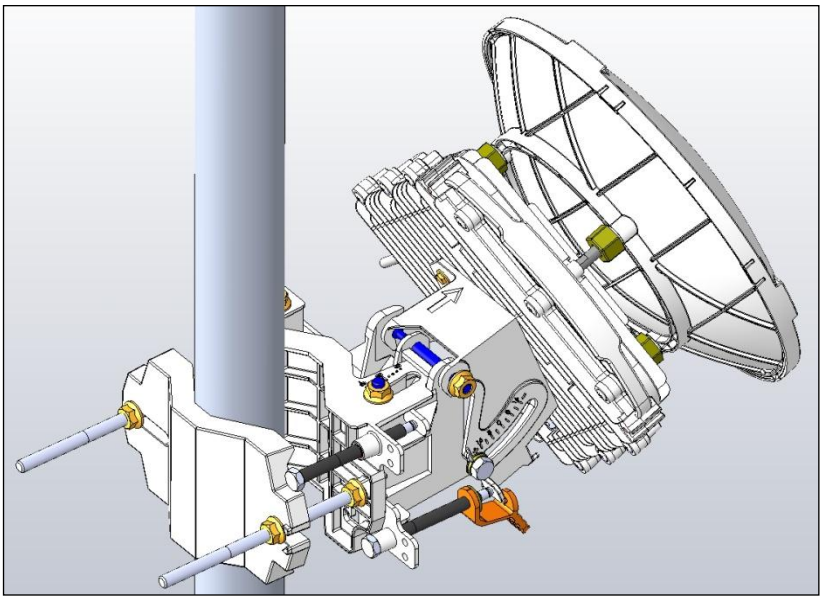


Figure 2-7 Installed EtherHaul 1200 Unit

2.9 Performing Initial System Setup

Note:

The instructions in this section refer to *Figure 2-1*.

1. Disconnect the DVM from the ODU by removing the probes from the AUX port (*Figure 2-2)*.
2. Reboot both ODUs by gently pressing the ODU Reset Button (❽). This returns the ODU to **Adaptive Mode.** Following this action, and after the ODU has finished rebooting, the RF LED color indicator on both ODUs will turn **green,** indicating that the radio link is Up.
3. Carefully reinsert and tighten using the 13mm open wrench the AUX port protective seal.

The EtherHaul 1200 link can now pass traffic and management between the ports and over the radio link.

Further configuration can be performed using the Web EMS or the CLI.

Note:

To perform configuration and monitoring, you must connect your laptop or PC to one of the two Ethernet ports on the ODU.

3 Performing Basic Configuration Using the Web EMS

This chapter explains how to perform basic configuration tasks using the Web EMS.

- For instructions how to configure a link using the CLI, refer to *Performing Basic Configuration using the CLI* on page 47.
- For instructions on performing advanced configuration, such as network configuration, synchronization, OAM, and other advanced configuration tasks, refer to *Performing Advanced Configuration* on page 77.

This chapter includes the following topics:

- Connecting to the ODU Using the Web EMS
- Saving Configuration Changes and Resetting the System Using the Web EMS
- Quick Configuration
- Configuring and Displaying Basic System Information Using the Web EMS
- Configuring System IP Addresses Using the Web EMS
- Configuring Radio Parameters Using the Web EMS
- Viewing Modulation Profiles Using the Web EMS
- Configuring Ethernet Interfaces Using the Web EMS
- Configuring SNMP Settings
- Default VLAN Setting

Note:

Before you perform basic configuration on the ODU, you must ensure that the ODU is set to either Adaptive or Static mode. The RF LED color indicator on a network-ready ODU **green**. Refer to Step 2 in *Performing Initial System Setup,* on page 34.

3.1 Connecting to the ODU Using the Web EMS

1. Launch an Internet browser and enter the ODU's IP address in the address bar. The default IP address is https://192.168.0.1.
2. Wait for the Java Applet to load and enter the username and password (admin, admin). The Web EMS Main screen is displayed:

Figure 3-1 Web EMS Main Screen

3.2 Saving Configuration Changes and Resetting the System Using the Web EMS

Whenever you make changes to the ODU configuration using the Web EMS, you must click **Save Configuration** on the Web EMS Main screen in order to save the configuration changes to the startup configuration. If you do not save the configuration, the changes will be lost the next time the system resets.

To reset the system, click **Reset System** on the Web EMS Main screen.

3.3 Quick Configuration

It is recommended to use the Quick Configuration screen to configure the basic ODU parameters. To display the Quick Configuration screen, click **Quick Configuration** on the toolbar on the left.

You can also click specific topics on the toolbar on the left to display and configure more extensive system parameters.

3.4 Configuring and Displaying Basic System Information Using the Web EMS

You can view and configure basic system information in the System Information section of the Quick Configuration screen.

Figure 3-2 Web EMS Quick Configuration Screen – System Information Section

The following are the basic system parameters:

- Name
- Date
- Time

When you are finished, click **Apply**.

To view and configure more extensive system information, click **System** on the Web EMS Main screen. The System screen is displayed.

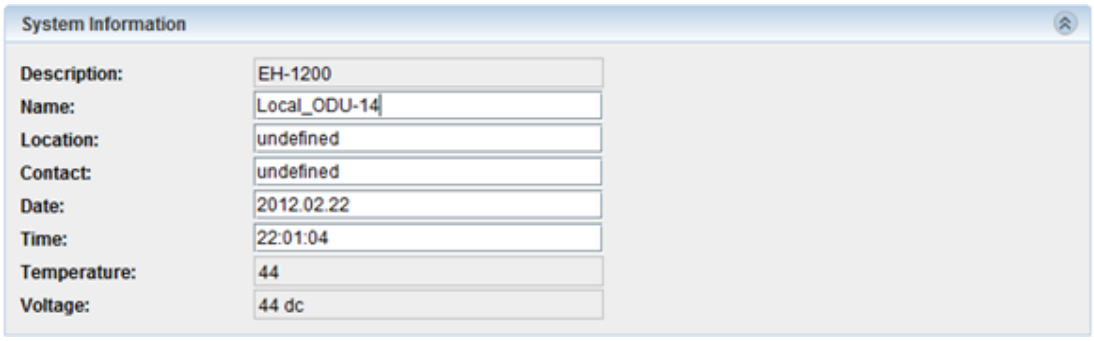


Figure 3-3 System Screen – System Information Section

The System Information section of the System screen includes the following system parameters:

- Description
- Name
- Location
- Contact
- Date
- Time
- Temperature
- Voltage (and indication about power source: DC or PoE)

3.5 Configuring System IP Addresses Using the Web EMS

You can change and add system IP addresses in the IP section of the Quick Configuration screen, or by clicking **System** on the Web EMS Main screen and clicking the IP section of the System screen.

The EtherHaul ODU supports up to four IP addresses that can be on different subnets and associated with different VLANs. You can assign a static route to each IP address. Default IP-Gateway is defined as a static route.

By default, one IP address is defined (IP #1):

- IP Address – 192.168.0.1
- IP Prefix Length - 24 (equivalent to Mask 255.255.255.0)
- VLAN – 0 (not defined, meaning the IP is not associated with specific VLAN)

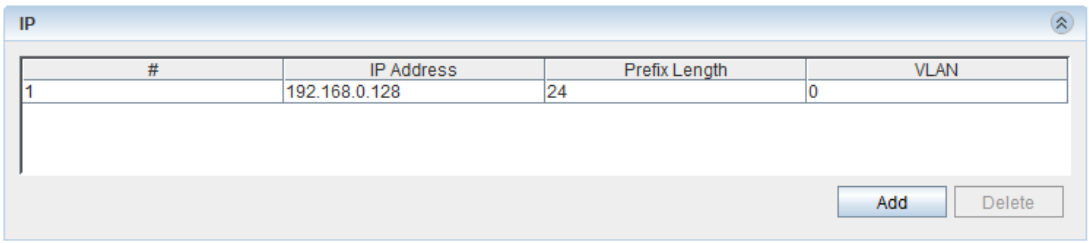


Figure 3-4 IP Section of Quick Configuration and System Screen

To add or change an IP address:

1. Click **Add**. The Add IP window opens.

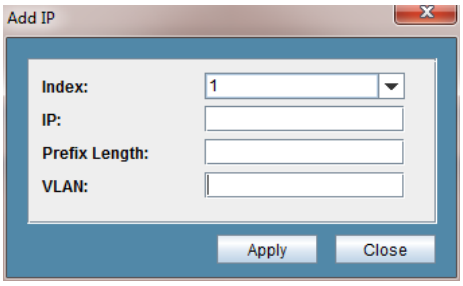


Figure 3-5 Add IP Window

2. In the **Index** field, select the index of the IP you want to add or change. Select Index #1 if a single IP is used and you wish to change it.

Note: If you change the default IP address, your connection to the ODU will be lost. To re-establish a connection, launch an Internet browser and connect using the new IP address.

3. Click **Apply**.

Note: By default, no static route or default gateway is defined.

Creating and modifying the IP Route (and Default Gateway) is performed using the Route section of the Quick Configuration screen or the System screen.

To add or change a Route:

1. Click **Add**. The Add Route window opens.

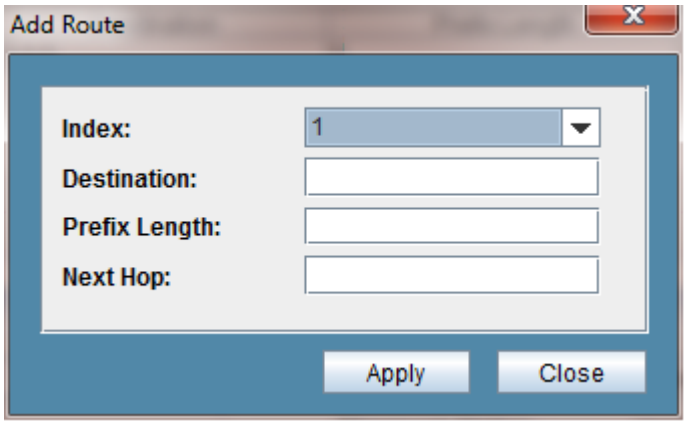


Figure 3-6 Add Route Window

2. In the Index field, select the index of the IP for which you want to add or change a route. Select Index #1 if you are using a single IP and you want to change its route.

idx	number 1 to 10
dest	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74).
prefix-len	ip prefix – a number from 0 to 32
next-hop	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74). All IP addresses in the table must be different.

3. Click **Apply**.

The following example shows a single IP configuration with a default gateway:

ODU with IP 192.168.0.17, mask 255.255.255.0 and default gateway 192.168.0.254.

ODU config – IP screen:

- Index – 1
- IP Address – 192.168.0.17
- Prefix Lenght – 24
- VLAN – 0

ODU config – Route screen:

- Index – 1
- Destination – 0.0.0.0
- Prefix Length – 0
- Next Hop – 192.168.0.254

3.6 Configuring Radio Parameters Using the Web EMS

You can configure basic radio parameters in the Radio section of the Quick Configuration screen.

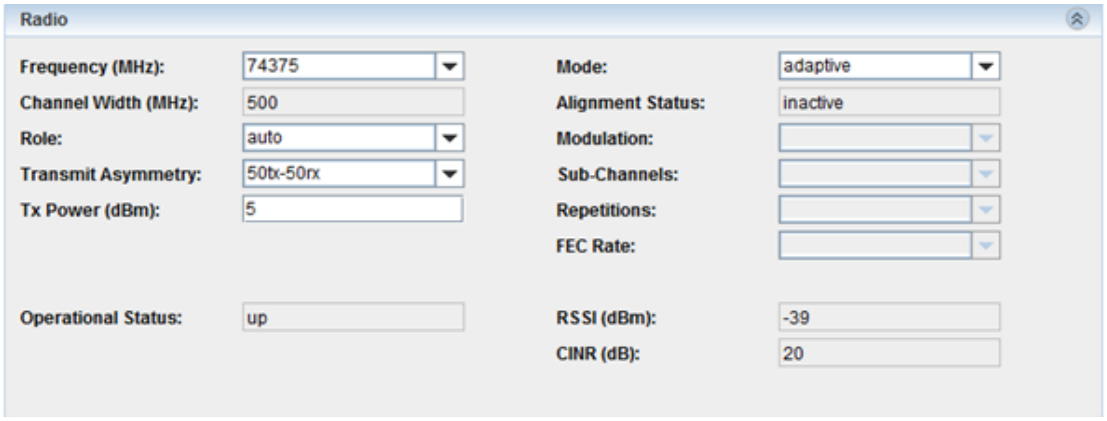


Figure 3-7 Web EMS Quick Configuration Screen – Radio Section

You can also configure the radio parameters by clicking **Radio** on the Web EMS Main screen and going to the Radio section of the Radio screen. The Radio screen displays several additional fields.

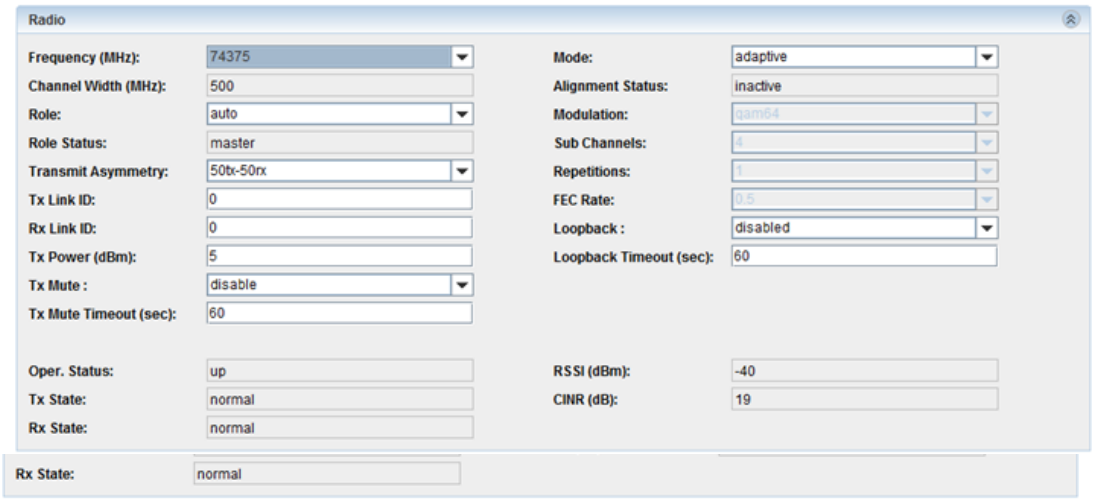


Figure 3-8 Web EMS System Screen – Radio Section

- **Frequency (MHz)** – Select a frequency channel. The default values is 74375.
- **Channel Width (MHz)** – 250MHz or 500MHz. Default value is **500**.
- **Role** – Determines whether the ODU functions as a master or slave. In a link, one side must be set to **Master** and the other side must be set to **Slave** (required for link synchronization)**.** Default value is **Auto,** meaning the role will be set automatically by the link**.** You can check the current set role in the **Role Status** field.

Manually setting the Role is necessary only for asymmetric configurations.

- **Transmit Asymmetry** – Default value is symmetric configuration: 50% for Tx and Rx (**50tx-50rx**). For an asymmetric configuration (75%/25% or 90%/10%), you will have to manually configure the Role and set the Master unit to **75tx-25rx (or 90tx-10rx)** and the Slave unit to **25tx-75rx (or 10tx-90rx)**. Default value is **50tx-50rx**.
- **Mode** – Select one of the following operation modes:
  - **Alignment** – Carrier Wave transmission. Used for antenna alignment.
  - **Adaptive** – Adaptive Bandwidth, Code, and Modulation.
  - **Static** – Fixed modulation profile. If you select **Static**, you must select from a list of pre-configured modulation profiles in the **Modulation** field.

Default value is **Adaptive**.

- **Modulation** – qpsk, 16QAM, or 64QAM.
- **Sub Channels** – From 1 to 4 (occupied bandwidth. For Channel Width 250MHz: 62.5-250MHz, For Channel Width 500MHz: 125-500MHz)
- **Repetitions** – 1,2 or 4
- **FEC Rate** – 0.5

When using the system in Static mode, you must select from a pre-defined list of modulation profiles. In Adaptive mode, the ODU will switch among the modulation profiles from this list.

To check the available modulation profiles, refer to *Viewing Modulation Profiles Using the Web EMS* on page *43*.

- **Tx and Rx Link ID** –You can set unique Link IDs for links installed on the same site to avoid locking on the wrong transmitter.
- **Operational Status** – Displays the radio link status (Up or Down).
- **Tx and Rx State** –Displays the Tx and Rx chains status.
- **RSSI (dBm)** – Displays the Receiver Signal Strength Indicator.
- **CINR (dB)** – Displays the Carrier to Interference + Noise ratio, which indicates the radio link's signal quality. In normal conditions, CINR≥17 indicates a good signal quality.
- **Tx Power (dBm)** –ODU's transmit power (+5 to -35dBm).
- **Tx Mute** – set to **Enable** to mute the transmitter
- **Tx mute Timeout (seconds)** – number of seconds for Tx mute enabled
- Loopback – ODU RF loopback. Select the modulation the ODU will be set to in loopback mode.

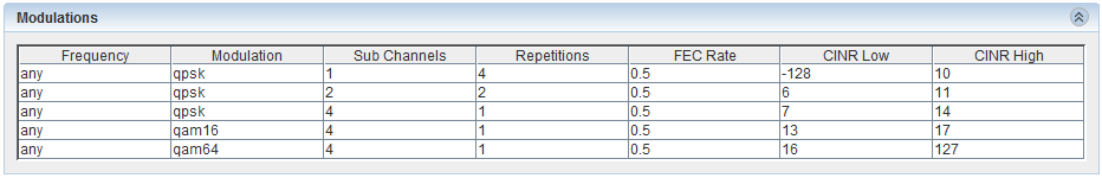
- Loopeback Timeout (seconds) – number of seconds the ODU will be in RF loopback

When you are finished, click **Apply**.

3.7 Viewing Modulation Profiles Using the Web EMS

To view the available modulation profiles, click **Radio** on the Web EMS Main screen and click the Modulations section of the Radio screen.

Note that different modulation tables may apply according to the frequency channel used.



Frequency	Modulation	Sub Channels	Repetitions	FEC Rate	CINR Low	CINR High
any	qpsk	1	4	0.5	-128	10
any	qpsk	2	2	0.5	6	11
any	qpsk	4	1	0.5	7	14
any	qam16	4	1	0.5	13	17
any	qam64	4	1	0.5	16	127

Figure 3-9 WEB EMS Radio Screen – Modulations Section

- **CINR Low** – Lower threshold for stepping down in modulation profile (Adaptive Mode).
- **CINR High** – Upper threshold for stepping up in modulation profile (Adaptive Mode).

3.8 Configuring Ethernet Interfaces Using the Web EMS

The EtherHaul system includes four Ethernet interfaces:

- **Host** – Management interface
- **Eth0** – Radio interface
- **Eth1** – ODU interface, port 1
- **Eth2** – ODU interface, port 2

You can configure Ethernet port parameters in the Port sections of the Quick Configuration screen. Some EtherHaul Ethernet port parameters are preset and cannot be modified. This section lists and describes those parameters that can be modified.

Figure 3-10 Web EMS Quick Configuration Screen – Port Section (Eth1)

You can also configure Ethernet port parameters by clicking the icon of the interface you want to configure on the EMS Web Main screen (*Figure 3-11*). The Interface screen (*Figure 3-12*) contains several additional fields.

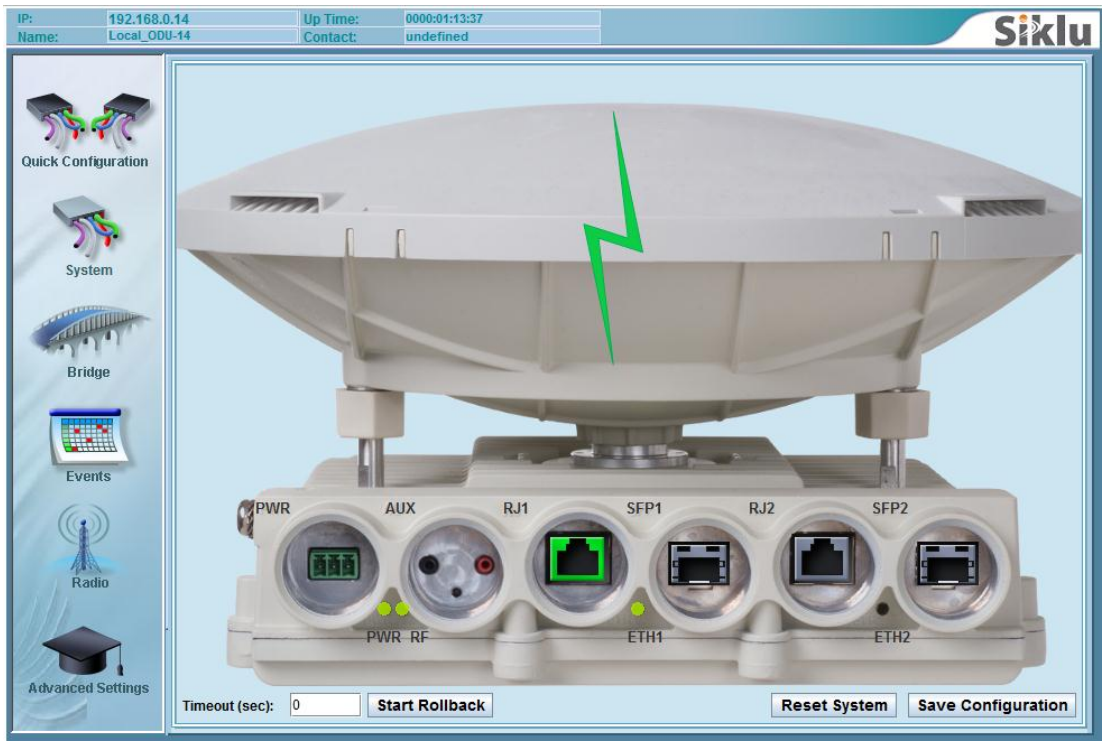


Figure 3-11 Interface Icons on Web EMS Main Screen

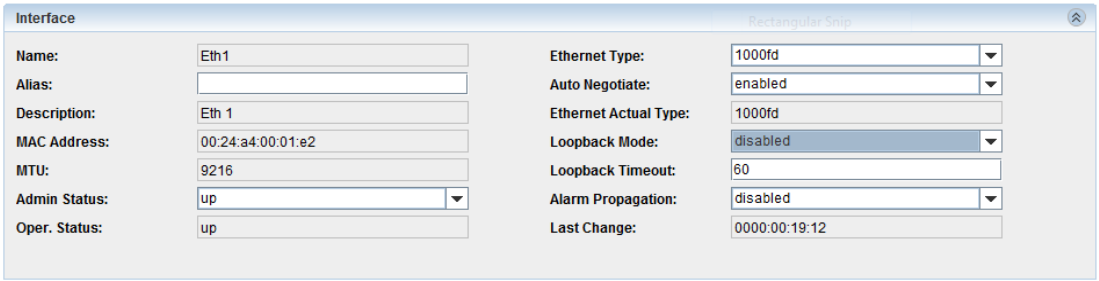


Figure 3-12 Interface Screen

- **Admin Status** – Determines whether the port is enabled (**up**) or disabled (**down**). Default value is **up**.
- **Oper. Status** – Displays the operational status of the port - **up** or **down**.
- **Auto Negotiation** – Determines whether or not auto-negotiation is enabled (**enabled**) or disabled (**disabled**). Default value is **enabled**.

- **Ethernet Type** – When Auto Negotiation is disabled, select the port's speed manually in this field (10/100/1000, HF/FD). When using the SFP physical port, set this field to **1000xfd**. Default value is **1000fd** (Electrical RJ45, 1000 Full-Duplex).
- **Ethernet Actual Type** – Displays the port's actual speed/duplex (after negotiation).

Note:

Auto-negotiation and Ethernet Speed/Duplex (in case Auto-neg disabled) must be identical on the ODU port and the end-equipment port.

- **Loopback Mode** – Interface screen only. Options are: Disabled, Internal, Internal-mac-scap, External, External-mac-swap.
- **Loopback Timeout** – Interface screen only. The loopback timeout (in seconds).
- **Alarm Propagation** – Interface screen only. Used to define system behavior in case of Eth or Radio link failure (port shutdown):
  - "Backward" – Eth port down in case radio link down or Eth port down at the remote.
  - "Forward"= notification is sent to the remotein case Eth port link down.
  - "Both Directions"= Eth port down in case of both radio or Eth link down.

When you are finished, click **Apply**.

3.9 Configuring SNMP Settings

You can configure the SNMP V2 managers trap destination in the SNMP section of the System screen.

SNMP V3 attributes may be configured via CLI only. Refer to Managing SNMP on page 129.

You can define up to five managers, with the following settings:

- **Destination IP Address**
- **UDP Port Number**
- **Read Community (security key)**

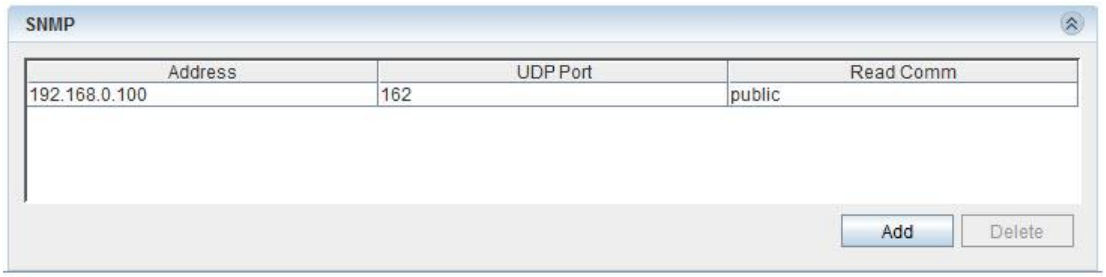


Figure 3-13 Web EMS System Screen – SNMP Section

To add or change managers, click **Add**.

When you are finished, click **Apply**.

Note:

These settings are applicable for SNMPv2.

SNMPv3 settings are available for configuration using the CLI.

3.10 Default VLAN Setting

EtherHaul's Undefined VLAN feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the EtherHaul system.

For VLAN configuration options, including the ability to define or block specific VLANs, , refer to *Configuring VLANs* on page 63.

4 Performing Basic Configuration using the CLI

This chapter explains how to perform basic configuration tasks using the CLI.

- For instructions how to configure a link using the Web EMS, refer to *Performing Basic Configuration Using the Web EMS* on page 35.
- For instructions on performing advanced configuration, such as network configuration, synchronization, OAM, and other advanced configuration tasks refer to *Performing Advanced Configuration* on page 77.

This chapter includes the following topics:

- Establishing a CLI Session with the ODU
- Saving Configuration Changes and Resetting the System Using the CLI
- Configuring and Displaying Basic System Information Using the CLI
- Configuring System IP Addresses Using the CLI
- Configuring Radio Parameters Using the CLI
- Configuring Ethernet Interfaces Using the CLI
- Default VLAN Setting

Note:

Before you perform basic configuration on the ODU, you must ensure that the ODU is set to either Adaptive or Static mode. The RF LED color indicator on a network-ready ODU is **green**. Refer to Step 2 in *Performing Initial System Setup*, on page 34.

4.1 Establishing a CLI Session with the ODU

1. Run a standard SSH client. You can use a common, open source SSH client program, such as PuTTY, available for download from the web.
2. Enter the ODU's **default** IP address: **`192.168.0.1`** (the default Mask is 255.255.255.0) and open the connection.
3. Login as user **`admin`**.
4. Enter the password **`admin`**.

When a successful connection is established, the ODU responds as follows:

```
login as: admin
EH-1200, S/N: F026500012, Ver:  3.0.0 6311
admin@192.168.0.15's password:
```

4.2 Saving Configuration Changes and Resetting the System Using the CLI

Whenever you make changes to the ODU configuration, you must save the configuration changes to the startup configuration. If you do not save the configuration, the changes will be lost the next time the system is reset. Use the following command to save configuration changes to the startup configuration:

```
Local_Site> copy running-configuration startup-configuration
```

To reset the system, use the **reset system** command. You must reset the system whenever you exit Alignment mode.

```
Local_Site> reset system
```

4.3 Configuring and Displaying Basic System Information Using the CLI

Use the **set system name** command to set the ODU's name. Once you set the ODU's name, a prompt appears with the name you just set, the date, and the time.

```
Default> set system name Local_Site
Local_Site>
```

To set system date & time, use the following command:

```
Local_Site> set system date 2011.01.18 time 15:08:00
```

Use the **show system** command to display basic information about the ODU.

```
Local_Site>show system

system description          : EH-1200
system snmpid               : 1.3.6.1.4.1.31926
system uptime               : 0000:00:05:10
system contact              : undefined
system name                 : Local_Site
system location             : undefined
system voltage              : 55 dc
system temperature          : 39
system date                 : 2011.01.18
system time                 : 15:08:06
system cli-timeout          : 15
```

4.4 Configuring System IP Addresses Using the CLI

The EtherHaul ODU supports up to four IP addresses that can be on different subnets and associated with different VLANs. You can assign a static route to each IP address. The Default IP-Gateway is defined as a static route.

By default, one IP address is defined (IP #1):

- IP Address – 192.168.0.1
- IP network Prefix – 24 (Mask 255.255.255.0)
- VLAN – 0 (not defined)

By default, no route is defined.

Use the **`set ip`** command to change or add an IP address. The command must be followed by the index number of the IP address you want to add or change. Use the index number 1 to change the default IP address. For example:

```
set ip <ip-index>  ip-addr <value> [prefix-len <value>] [vlan
<value>]
    <ip-index>              : integer 1..4
```

```
Local_Site>set ip 1 ip-addr 192.168.0.11 prefix-len 24
```

If the IP entry does not already exist, the **`set ip`** command creates it and assigns the attributes specified. If the interface address or the default router address is not explicitly specified, the entry is created with the default value that has been defined for the VLAN.

If the IP entry already exists, the **`set ip`** command replaces the attributes that are currently defined for the entry with the values specified in the command.

Up to four IP addresses can be specified on the command line.

A **`set ip`** command fails if the route specified is not within the subnet that has been defined by mask.

Note: If you change the default IP address, your connection to the ODU will be lost. To re-establish a connection, launch an Internet browser and connect using the new IP address.

To display all of the currently configured IP addresses and their attributes, use the **`show ip`** command:

For example:

```
Local_Site>show ip

ip 1 ip-addr                : 192.168.0.11
ip 1 prefix-len             : 24
ip 1 vlan                   : 0
```

To delete IP entries, use the **clear ip** command:

clear ip <index>

To create and modify an IP Route and Default Gateway, use the **set route** command:

set route <idx> [dest <ip-address>] [prefix-len 0..32] [next-hop <ip-address>]

idx	number 1 to 10
dest	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74).
next-hop	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example, 10.0.15.74). All IP addresses in the table must be different.
prefix-len	ip prefix – a number from 0 to 32

By default, no route is defined.

To set a static route, use the following command:

Local_Site>set route 1 dest 192.168.0.64 prefix-len 30 next-hop 192.168.0.66

To set a single default gateway, use the following command. When single IP is used and a Static route is not used, you may configure a default IP gateway. In such case, use 0.0.0.0 as the destination network with **prefix-len 0**.

set route 1 dest 0.0.0.0 prefix-len 0 next-hop 192.168.0.254

To display all of the currently configured routes and their attributes, use the **show route** command:

```
Local_Site>show route
ip 1 dest       : 0.0.0.0
ip 1 prefix-len: 0
ip 1 next-hop   : 192.168.0.254
```

4.5 Configuring Radio Parameters Using the CLI

This section lists and describes the CLI commands you need to configure and display radio parameters.

Use the **set rf** command, followed by the name of the parameter you want to configure, to configure the ODU's radio parameters:

For example:

```
Local_Site>set rf frequency 75375
Local_Site>set rf role slave
Local_Site>set rf mode adaptive
```

4.5.1 Displaying Radio Parameters and Status Using the CLI

Use the **show rf** command to display the ODU's current radio status and parameter settings.

```
Local_Site>show rf
rf operational           : up
rf tx-state              : normal
rf rx-state              : normal
rf cinr                  : 19
rf rssi                  : -43
rf channel-width         : 500
rf frequency             : 74375
rf role                  : auto
rf role-status           : master
rf mode                  : adaptive qam64 4 1 0.5
rf alignment-status      : inactive
rf lowest-modulation     : qpsk 1 4 0.5
rf tx-asymmetry          : 50tx-50rx
rf rx-link-id            : 0
rf tx-link-id            : 0
rf temperature           : 52
rf loopback-timeout      : 60
rf loopback              : disabled
rf tx-power              : 5
```

Table 11-3 on page 179 lists and describes the configurable RF attributes. *Table 11-5* on page 180 lists and describes the read-only RF attributes.

4.5.2 Configuring the Radio Parameters Using the CLI

Set rf
[frequency {71375 | 71875 | 72375 | 72875 | 73375 | 73875 | 74375 | 74875 | 75375}]

[role {master | slave | auto}]

[f tx-mute {disable | enable}]

[tx-mute-timeout <integer 0..86400>]

[mode {static <modulation> <subchannels> <repetitions> <fec-rate> - (from list of modulations) | alignment | adaptive}]

[lowest-modulation {<modulation> <subchannels> <repetitions> <fec-rate> - (from list of modulations)}]

[tx-asymmetry for master use 50tx-50rx, 75tx-25rx, 90tx-10rx
for slave use 50tx-50rx, 25tx-75rx, 10tx-90rx}]

[tx-link-id <integer 0..127>]

[rx-link-id <integer 0..127>]

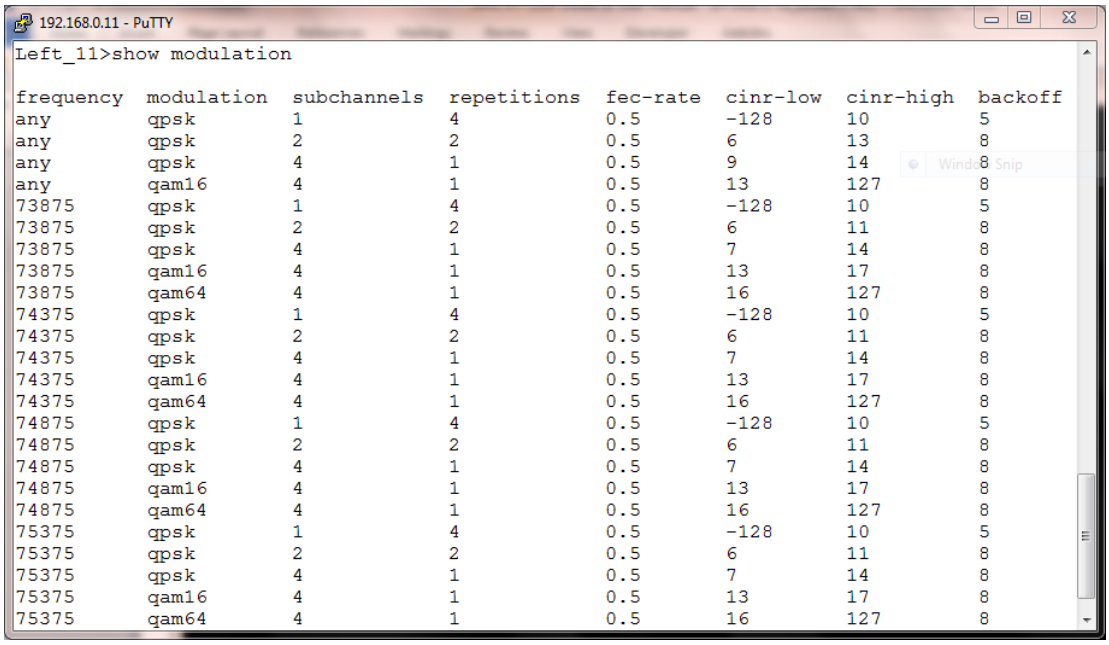
[loopback {internal-mac-swap <modulation> <subchannels> <repetitions> <fec-rate> - (from list of modulations) | disabled}]

[loopback-timeout <integer 0..86400>]

[tx-power <integer -35..5>]

4.5.3 Viewing Modulation Profiles Using the CLI

Use the **`show modulation`** command to display available supported modulation profiles and their parameters.



- **CINR Low** – Lower threshold for stepping down in modulation profile (Adaptive Mode).
- **CINR High** – Upper threshold for stepping up in modulation profile (Adaptive Mode).
- **Backoff** – internal setting controlling the OFDM Tx power backoff.

Note that different modulation tables may apply according to the frequency channel used.

Note:

Modulation parameters are optimized configuration and should not be altered by the user

4.6 Configuring Ethernet Interfaces Using the CLI

The EtherHaul system has four Ethernet interfaces:

- **Host** – Management interface
- **Eth0** – Radio interface
- **Eth1** – ODU interface, port 1
- **Eth2** – ODU interface, port 2

You can change the default values of the ODU interfaces, and display the port status of a specific interface.

Note:

The Eth object is always followed by one or more name strings that correspond to ports or devices to be acted upon.

In the commands below, this string is represented as **<eth-list>**.

For more details on this convention, refer to *Designating Named Objects* on page 158.

4.6.1 Configuring Interface Parameters

Use the **set eth** command, followed by the name of the interface (Eth1 or Eth2) to change the default values of an Ethernet interface.

```
set  eth <eth-list>
     [admin up | down]
     [alias <string>]
     [eth-type <eth-type-set>]
     [auto-neg {enabled | disabled}]
     [loopback-mode { disabled | external | internal}]
     [loopback-timeout <integer>]
     [alarm-propagation {disabled | backward | forward | both
     directions}
```

For example, use the following command to set Ethernet port 1 to SFP mode:

```
set eth eth1 eth-type 1000xfd
```

Table 11-18 on page 198 lists and describes the configurable Ethernet interface attributes.

4.6.2 Displaying Interface Status

Use the **show eth** command, followed by the name of the interface, to display the Ethernet port status for a specific interface.

```
show  eth [{<eth-list> | all}
      [{info | description | mtu | mac-addr | admin | operational
      | last-change | name | alias | eth-type | eth-act-type
```

```
      | auto-neg | loopback-mode | loopback-timeout | statistics
      | alarm-propagation}]]
```

The following is an example of an Ethernet interface status display.

```
Local_Site> show eth eth1

eth eth1 description           : Siklu
eth eth1 mtu                   : 9216
eth eth1 mac-addr              : 00:24:a4:00:06:d2
eth eth1 admin                 : up
eth eth1 operational           : up
eth eth1 last-change           : 0000:00:12:11
eth eth1 name                  : Eth1
eth eth1 alias                 :
eth eth1 eth-type              : 1000fd
eth eth1 eth-act-type          : 1000fd
eth eth1 auto-neg              : enabled
eth eth1 loopback-mode         : disabled
eth eth1 loopback-timeout      : 60
eth eth1 alarm-propagation     : disabled
```

Table 11-18 on page 198 lists and describes the configurable Ethernet interface attributes. *Table 11-19* on page 201 lists and describes the read-only Ethernet interface attributes.

4.7 Default VLAN Setting

EtherHaul's Undefined VLAN feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the EtherHaul system.

For VLAN configuration options, including the ability to define or block specific VLANs, refer to *Configuring VLANs* on page 63.

5 Commissioning and Acceptance Procedure

This chapter presents the recommended commissioning and acceptance procedure to be performed following the installation of each EtherHaul ODU.

The commissioning and acceptance procedure verifies the correct installation and the proper, safe, and robust operation of the EtherHaul RF link.

This chapter includes the following topics:

- Installation Verification and Testing
- EtherHaul Commissioning and Acceptance Form

5.1 Installation Verification and Testing

Inspect the following components and confirm their adherence to requirements that are detailed in the accompanying checklist (*EtherHaul Commissioning and Acceptance Form* on page 57).

Hint:

Make copies of the *EtherHaul Commissioning and Acceptance Form* on page 57 and use it as a comprehensive guide to RF link commissioning and acceptance.

5.1.1 Physical Installation Verification

This inspection verifies the physical installation of the ODU, in accordance with *For detailed technical specifications* please refer to the datasheet.

Installing the EtherHaul 1200 on page 20.

- Pole mount installation
- ODU installation
- Connectors' sealing
- Cables installation
- Grounding

5.1.2 RF Link Test

This inspection verifies the RF link status, in accordance with *Performing Basic Configuration Using the Web EMS* on page 35 and *Performing Basic Configuration using the CLI* on page 47.

- RF LED is green

- Management/CLI indication: “RF Operational – Up”
- Receive Signal Strength Indication (RSSI) achieved in Alignment Mode is within +/-5dB of the expected value
- Carrier to Interference + Noise Ratio (CINR) is 16 or higher
- Link configuration (modulation, mode) is in accordance with plan requirements

5.1.3 Link Errors Test

This inspection verifies error-free operation of the radio link.

- No errors/loss on the RF Statistics counters (show rf statistics)

5.1.4 Ethernet Services Test

This inspection verifies correct Ethernet services flow and error-free operation.

- Connect PCs on both ends of the link and use software-based utilities to test for packet-loss
- If available, connect a packet analyzer to the GbE port and verify that no packets are lost

5.1.5 Management Verification

This inspection verifies proper management of the link.

- Verify correct management/CLI connection to both local and remote ODUs
- Verify management access from remote NMS stations

5.1.6 Recording ODU Configuration

Perform the following steps after the EtherHaul ODU is commissioned and accepted:

- Copy the Running Configuration (currently active) to Startup Configuration
- Save the configuration file for future records and backup

5.2 EtherHaul Commissioning and Acceptance Form

EtherHaul™ Commissioning and Acceptance Form		
Customer Details		
Customer		
Project/link name		
Physical Installation Verification	Local Site	Remote Site
Site name &address		
Mount type	☐ Roof-top ☐ Mast/Tower	☐ Roof-top ☐ Mast/Tower
ODU mount above ground	meters	meters
Clear line-of-sight	☐ Yes ☐ No	☐ Yes ☐ No
ODU safely mounted using Siklu's bracket correctly installed	☐ Yes ☐ No	☐ Yes ☐ No
Pole diameter between 2-4"	☐ Yes ☐ No	☐ Yes ☐ No
Bracket's mounting bolts securely tightened	☐ Yes ☐ No	☐ Yes ☐ No
ODU grounding	☐ Yes ☐ No	☐ Yes ☐ No
Cables/Fibers Connections (mark all cables connected)	☐ Eth1 Cat5 ☐ Eth1 Fiber ☐ Eth2 Cat5 ☐ Eth2 Fiber ☐ DC	☐ Eth1 Cat5 ☐ Eth1 Fiber ☐ Eth2 Cat5 ☐ Eth2 Fiber ☐ DC
Overall Cables/Fibers length	meters	meters
Cables/Fibers securely routed and fixed properly using cable ties	☐ Yes ☐ No	☐ Yes ☐ No
Cables/Fibers are properly weatherproofed using the appropriate glands	☐ Yes ☐ No	☐ Yes ☐ No

ODU DC source	☐PoE ☐External DC	☐PoE ☐External DC
PoE model and manufacturer		
Measured DC power (or CLI/Web reading)	Volts DC	Volts DC
RF Link Parameters		
ODU Model		
ODU P/N		
ODU S/N		
ODU running SW version		
Tx/Rx Frequency	MHz	MHz
Channel-Width	☐250MHz ☐500MHz	☐250MHz ☐500MHz
Role	☐Auto ☐Master ☐Slave	☐Auto ☐Master ☐Slave
Tx/Rx Link ID	0 (not used)	0 (not used)
Modulation/Mode Mode: modulation/sub-channel/repetitions/FEC	☐Adaptive _____ ☐Static _____	☐Adaptive _____ ☐Static _____
UL/DL Configuration	☐Symmetric ☐Asymmetric (ratio)_____%	☐Symmetric ☐Asymmetric (ratio)_____%
ODU Polarization	☐V ☐H	☐V ☐H
Link distance	meters	
RF Link Tests		
Expected RSSI	dBm	dBm
Measured RSSI	dBm	dBm
Measured CINR	dB	dB

Green “RF” led	☐ Yes ☐ No	☐ Yes ☐ No
RF operational status Up	☐ Yes ☐ No	☐ Yes ☐ No
RF Statistics error counters clear	☐ Yes ☐ No	☐ Yes ☐ No
Ethernet Services Tests		
Packet-Loss test ☐Packet Analyzer ☐SW-based	☐No Packet-Loss Test duration _____	☐No Packet-Loss Test duration _____
Eth Statistics dropped-packets counters clear	☐ Yes ☐ No	☐ Yes ☐ No
Management		
IP address/Mask		
IP Mask		
Default IP Gateway		
In-band management enabled	☐ Yes ☐ No VLAN ID _____	☐ Yes ☐ No VLAN ID _____
Management of local and remote	☐ Yes ☐ No	☐ Yes ☐ No
NMS used	☐ Web/CLI ☐ SikluView ☐ Other _____	☐ Web/CLI ☐ SikluView ☐ Other _____
NMS management access	☐ OK ☐ NOK ☐ N/A	☐ OK ☐ NOK ☐ N/A
Traps received in NMS	☐ OK ☐ NOK ☐ N/A	☐ OK ☐ NOK ☐ N/A
Final Configuration Verification		
Copy running config to startup	☐ Done	☐ Done
Clear all statistics and logs	☐ Done	☐ Done
Configuration file saved and stored	☐ Done	☐ Done
Additional Info / Remarks		

I&C Details	
I&C Date	
Installation team	
Commissioning team	

6 EtherHaul Networking Configuration

This chapter presents the EtherHaul bridge management model and describes the initial procedures for configuring the EtherHaul network, including:

- Provider Bridge
- EtherHaul Bridging Model
- Configuring VLANs
- Configuring Bridge Ports
- Configuring Provider Bridge and Advanced VLAN Settings

6.1 Provider Bridge

The IEEE 802.1ad Provider Bridge, commonly known as QinQ or Provider Bridge, extends the IEEE 802.1Q standard by providing for a second stack of VLANs in a bridged network. The general purpose of Provider Bridge is to enable frames from multiple customers to be forwarded (or tunneled) through another topology (provider network) using service VLANs or S-VLANs. The provider bridge, which may consist of multiple devices in the service provider domain, looks like a simple bridge port to the customer's traffic and maintains the customer's VLANs.

Customer VLANs (referred to as C-VLANs by the IEEE 802.1ad specification) are not used to make any forwarding decisions inside the provider network where customer frames get assigned to service VLANs (S-VLANs). Inside the provider cloud, frames are forwarded based on the S-VLAN tag only, while the C-VLAN tag remains shielded during data transmission. The S-VLAN tag is removed when the frame exits the provider network, restoring the original customer frame.

The EtherHaul 1200 incorporates a fully functional integrated Provider Bridge (IEEE 802.1ad).

6.2 EtherHaul Bridging Model

The Siklu implementation of Provider Bridge is a network of up to five virtual bridges connected in a “cross-like” fashion as shown in *Figure 6-1*.

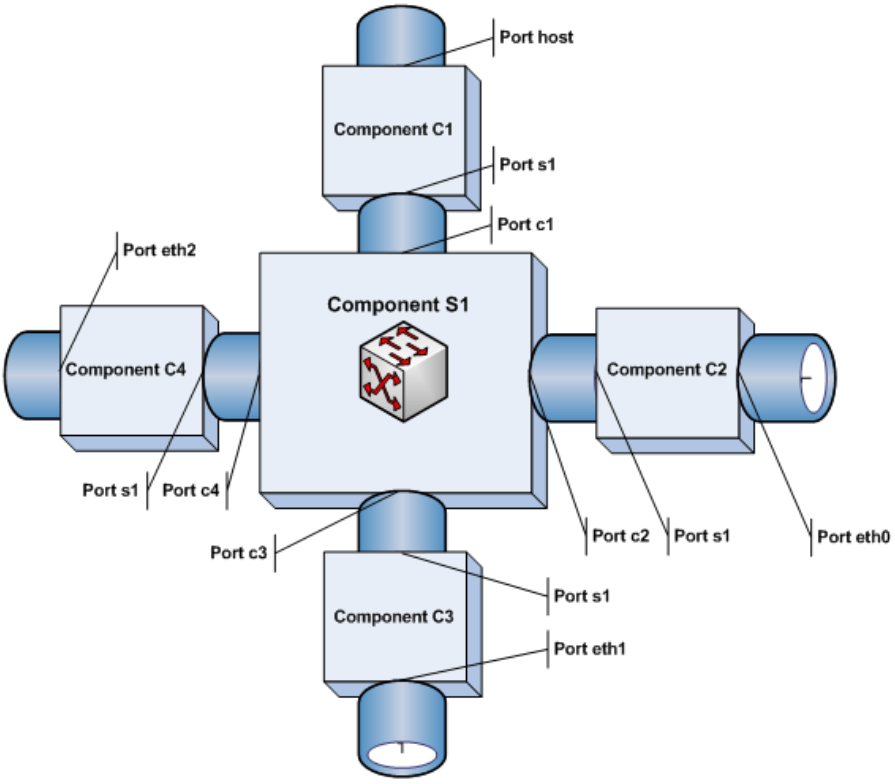


Figure 6-1 Provider Bridge Architecture

Figure 6-2 shows the generic model of the EtherHaul bridge.

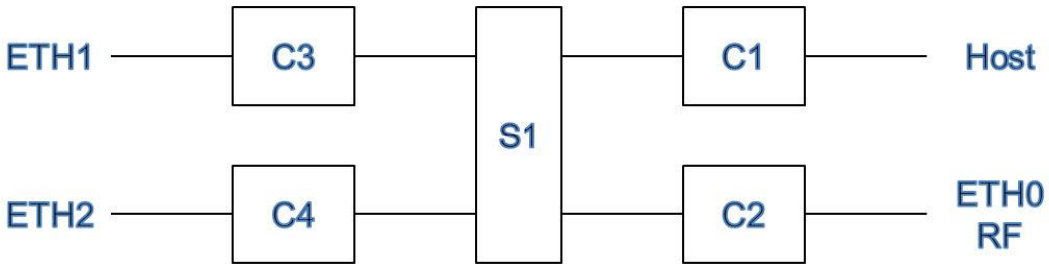


Figure 6-2 Generic Model of the EtherHaul Bridge

Each component acts as a virtual bridge. A component can have both external and internal ports. An external port name is identical to its interface name. For example, the C-component 1 (C1) external port name is ETH2. An internal port uses the name of its peer component as shown in *Figure 6-2*. For example, when C-component 1 (C1) is connected to the S component, the corresponding internal port is S1 .

You can change the default bridge configuration to suit your network by removing or adding the desired bridge components. All components are created, managed, and removed using the CLI or Web EMS.

6.3 Configuring VLANs

This section lists the default VLAN and Port settings, and provides instructions how to modify these settings.

By default, the EtherHaul system is set to Transparent Bridge (Undefined VLAN) mode. The Transparent Bridge feature enables transparent forwarding of both tagged and untagged traffic by default. No configuration or license is necessary for this feature, which gives you the flexibility to change your VLANs with no additional configuration necessary in the EtherHaul system.

In addition to the default Transparent Bridge feature, you can choose to create VLANs, as well as block specific VLANs.

6.3.1 Transparent Bridge Mode

EtherHaul's default setting is Transparent Bridge (Undefined VLAN). In this configuration, both tagged and untagged traffic is forwarded transparently. No VLAN configuration is required for Undefined VLAN. This feature gives you the flexibility to change your VLANs with no configuration necessary on the part of the EtherHaul system.

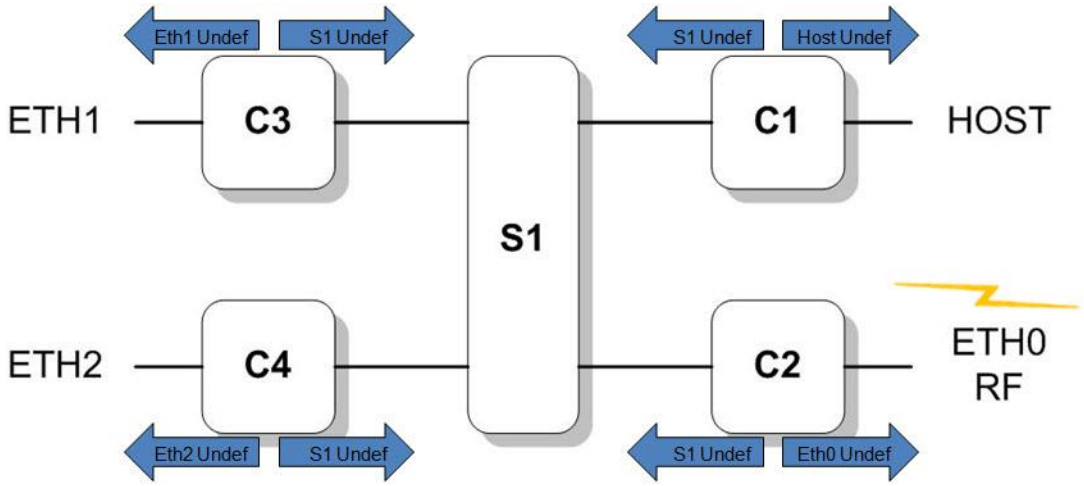


Figure 6-3 Undefined VLAN Implementation

In Transparent VLAN mode, you can use the Eth1 or the Eth2 port for all data and management traffic, included both tagged and untagged data (*Figure 6-4*). Alternatively, you can use one of the ports for management, and the other port for data, including both tagged and untagged data (*Figure 6-5*).

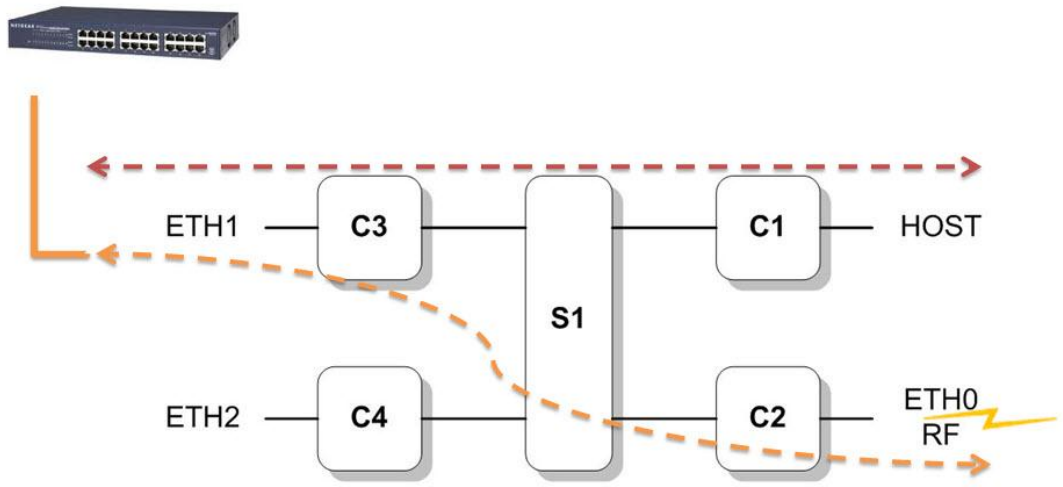


Figure 6-4 Transparent Bridge Mode – All Traffic Through Eth1

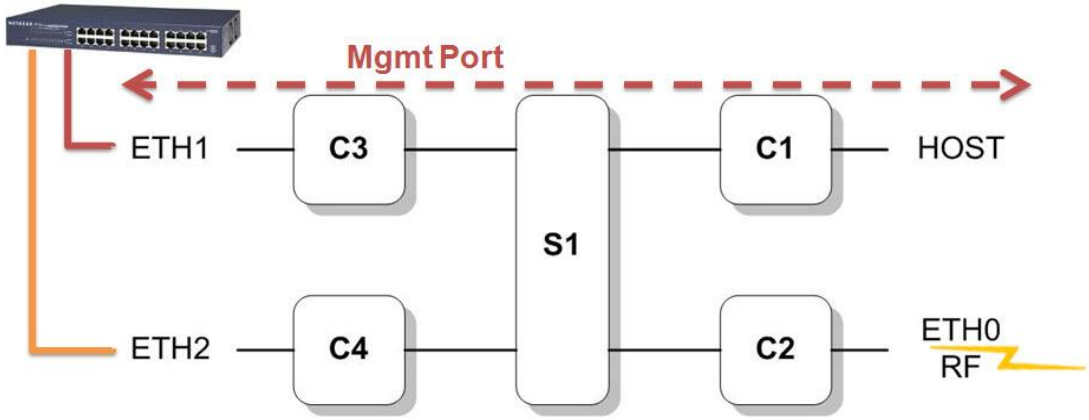


Figure 6-5 Transparent Bridge Mode Using Eth1 for Management and Eth2 for Data

```
default>show vlan
component-id  vid    fdb-id    egress         untagged       history
s1            1      1         c1,c2,c3,c4    c1,c2,c3,c4    disable
s1            undef  1         c1,c2,c3,c4    none           disable
c1            1      1         host,s1        host           disable
c1            undef  1         host,s1        none           disable
c2            1      1         eth0,s1        eth0           disable
c2            undef  1         eth0,s1        none           disable
c3            1      1         eth1,s1        eth1           disable
c3            undef  1         eth1,s1        none           disable
c4            1      1         eth2,s1        eth2           disable
c4            undef  1         eth2,s1        none           disable
default>
```

6.3.2 Configuring VLANs Using the Web EMS

To configure VLANs using the Web EMS:

1. In the Web EMS Main screen, click **Bridge**. The Bridge screen is displayed.
2. Click the VLANs section of the Bridge screen.

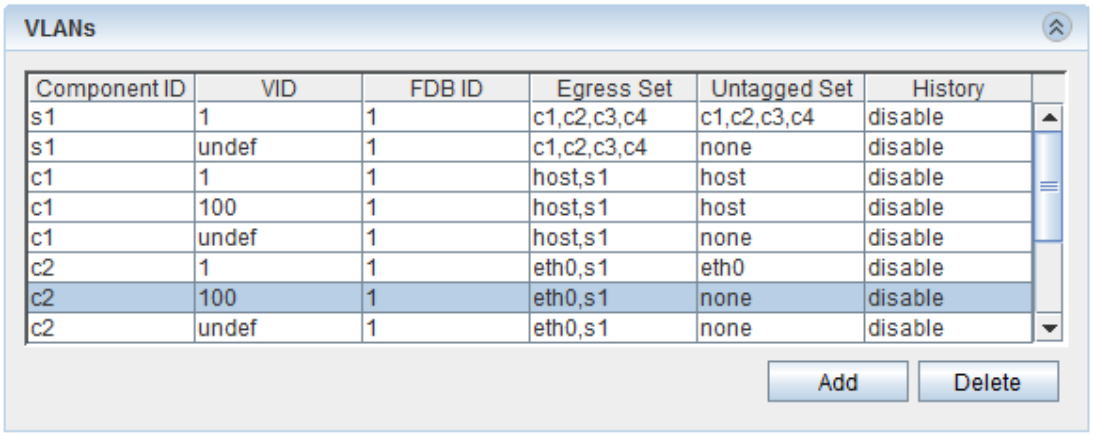


Figure 6-6 Web EMS Bridge Screen – VLANs Section

3. Click **Add**. The Add VLAN window is displayed.

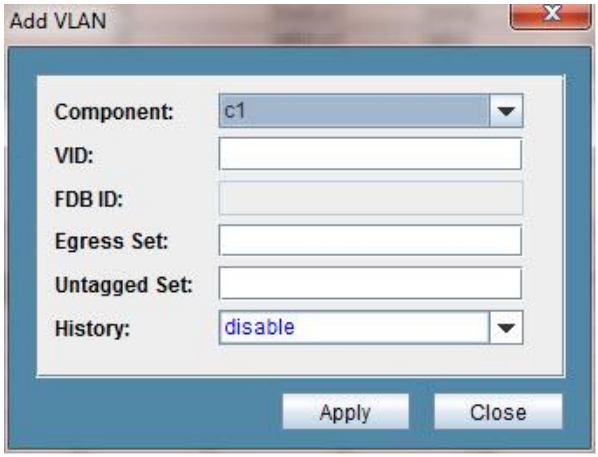


Figure 6-7 Add VLAN Window

4. Configure the following VLAN attributes for the required components:
   - **VID** – C-VLAN Identifier. This can be any number from 1 to 4094, which identifies a particular C-VLAN, or the special value “undef”, which identifies configuration relevant for all VLANs that are not explicitly defined in the VLAN Table. To edit an existing VLAN, enter the VID of the VLAN you want to edit.
   - **FDB ID** – Enter 1. For S-VLANs in Provider Bridge configuration, up to 64 FDBs are available for different S-VLANs.

- **Egress Set** – A frame which belongs to a VLAN identified by *vid* can enter the bridge through any port but can only leave through the ports that are included in the egress set (Host – management, Eth0 – radio, Eth1 – ODU port 1, Eth2 – ODU port 2).
- **Untagged Set** – A subset of the egress set. If a port is a member of the untagged set and a frame leaves the bridge through this port, the C-Tag is removed (untagged) To leave the VLAN tagged when transmitted on all ports in the egress set, enter **none**.
- **History** – If you want the ODU to collect statistics for this VLAN, select **enable**. Otherwise, select **disable**.

5. Click **Apply** to close the Add VLAN window.
6. Click **Apply** to implement the changes and close the Bridge screen.

6.3.3 Configuring VLANs Using the CLI

6.3.3.1 Creating and Modifying VLANs

VLAN definitions are stored in a table containing static configuration information for each VLAN that is configured in the device by local or network management. All VLAN Table entries are permanent and are restored when the device is reset.

Use the following syntax to create or modify a VLAN:

```
set  vlan <comp-id-list> <vid-list>
     [fdb-id <fdb-id>]
     [egress <bridge-port-list>]
     [untagged <bridge-port-list>]
```

6.3.3.2 Blocking Specific VLANs

You can block specific VLANs from entering the EtherHaul system by using the **`set vlan`** command and setting the **`egress`** attribute to **`none`**.

The following example blocks VLAN 333 traffic from entering the EtherHaul system:

```
default>set vlan c3 333 egress none untagged none
Set done: vlan c3 333
default>set vlan c4 333 egress none untagged none
Set done: vlan c4 333
default>set vlan c2 333 egress none untagged none
Set done: vlan c2 333

default>show vlan
component-id  vid    fdb-id     egress        untagged      history
s1            1      1          c1,c2,c3,c4   c1,c2,c3,c4   disable
s1            undef  1          c1,c2,c3,c4   none          disable
c1            1      1          host,s1       host          disable
c1            undef  1          host,s1       none          disable
c2            1      1          eth0,s1       eth0          disable
c2            333    1          none          none          disable
c2            undef  1          eth0,s1       none          disable
c3            1      1          eth1,s1       eth1          disable
c3            333    1          none          none          disable
c3            undef  1          eth1,s1       none          disable
c4            1      1          eth2,s1       eth2          disable
c4            333    1          none          none          disable
c4            undef  1          eth2,s1       none          disable
default>
```

6.3.3.3 Deleting VLANs

Use the **`clear vlan`** command to delete VLANs and clear their associated statistics.

Use the following syntax:

```
clear   vlan {<comp-id-list> | all} {<vid-list> | all}
        [statistics]
```

- Before deleting a **C-VLAN**, verify that it is not being used as a key to the C-VLAN Registration Table (*Table 11-29*). Do not delete the C-VLAN if such an entry exists.
- Before deleting an **S-VLAN**, verify that:
  - The S-VLAN is not being used as the key in the PEP Virtual Port Table (*Table 11-30*) and S-VID Translation Table (*Table 11-31*).
  - The S-VLAN is not being used as Relay S-VID in the S-VID Translation Table (*Table 11-31*).
  - The S-VLAN is not defined in any entry of the C-VLAN Registration Table (*Table 11-29*).

VLAN IDs 1 and Undef are default VLANs and cannot be deleted (but can be blocked).

6.3.3.4 Displaying VLAN Details

Use the **show vlan** command to display VLANs and their details.

Use the following syntax:

```
 show vlan [{all | <component-id>}
      [{all | <vids>}
      [{info | statistics | fdb-id | egress | untagged}]]]]
show  vlan
      [{all | <vids>}
      [{info | statistics | fdb-id | egress | untagged}]]]]
```

6.3.3.5 VLAN Table Attributes

Table 11-28 on page 210 lists and describes the attributes in the VLAN Table.

6.3.3.6 Displaying VLAN Common Properties

To display the ODU's VLAN configuration, use the following command:

```
show  vlan-common [{<comp-id-list> | all}
      [{ info | version | max-vid | max-num | curr-num}]]
```

This command displays general information about VLAN bridges that are active in the network. *Table 11-27* on page 209 lists and describes the VLAN Common attributes.

6.4 Configuring Bridge Ports

6.4.1 Configuring Bridge Ports Using the Web EMS

To configure ports using the Web EMS:

1. In the Web EMS Main screen, click **Bridge**. The Bridge screen is displayed.
2. Click the Bridge Ports section of the Bridge Ports screen.

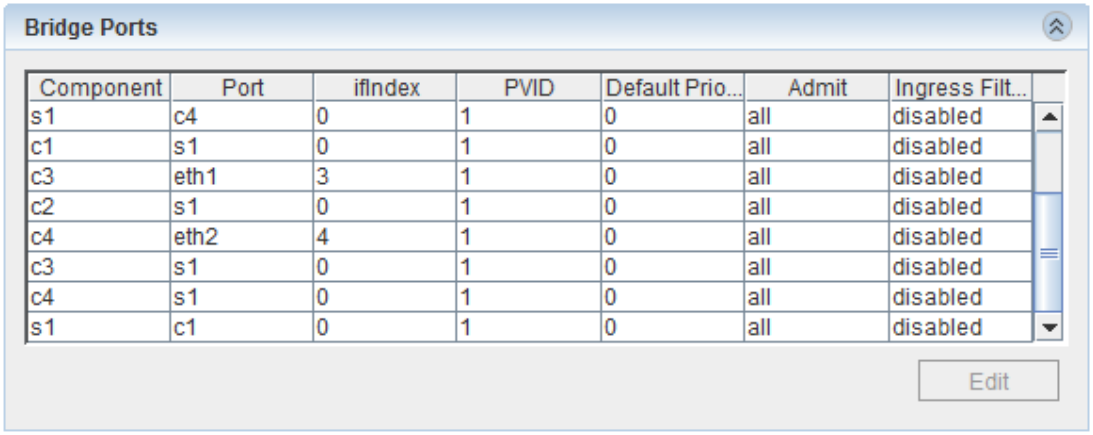


Figure 6-8 Web EMS Bridge Screen – Bridge Ports Section

3. To edit a port and change its PVID, click **Edit**. The Change Port window is displayed.

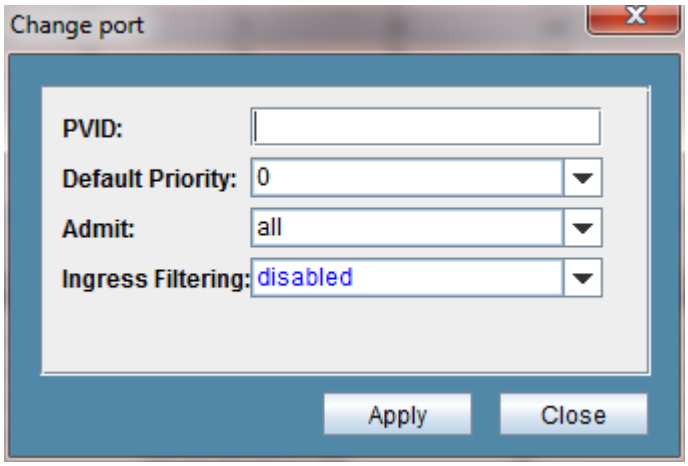


Figure 6-9 Change Port Window

4. In the **Port** field, select the port you want to edit.

5. Configure the following Port attributes:

pvid — A *vid* which will be assigned to an untagged frame or a priority-tagged frame, but VID is set to 0 indicating that the frame does not belong to any VLAN and only PCP field is relevant), which enters to the bridge through this port. The special value “undef” cannot be used as PVID. By default it is set to 1.

prio — The value which will be assigned to PCP field if an untagged frame arrives through this port. For priority-tagged frames this field is irrelevant. By default it is set to 0.

admit — This attribute controls what kinds of frames are allowed into the bridge. If set to *untagged* then only untagged or priority tagged frames may enter. If set to *tagged* then only tagged frames (i.e., those with VID different from zero) may enter. If set to *all*, all kinds of frames may enter. By default it is set to *all*.

filter — By default the VLAN configuration is essentially asymmetrical. Frames with any VIDs may enter through any port but leave only though a port which is a member in the egress set assigned to a particular VLAN. By setting *filter* to *enabled* symmetry is introduced – in this case a frame can enter through a particular port only if it can leave through this port as well. By default the attribute is set to *disabled*.

6. Click **Apply** to close the Change Port window.
7. Click **Apply** to implement the changes and close the Bridge screen.

6.4.2 Configuring Bridge Ports Using the CLI

Note:

The Bridge object is always followed by one or more name strings that correspond to ports or devices to be acted upon.

In the commands below, this string is represented as **<comp-id-list>**.

For more details on this convention, see *Designating Named Objects* on page 158.

Use the following command to assign the bridge device:

```
set   bridge <comp-id-list>
```

Use the following command to display bridge parameters:

```
show  bridge {[<comp-id-list> | all}
      [{info | mac-addr | num-ports}]]
```

Use the following command to reset all bridge attributes:

```
clear bridge {<comp-id-list> | all}
```

Table 11-22 on page 205 lists and describes the bridge attributes.

6.4.3 Configuring the Bridging Port

The bridging port provides access to port-wide definitions from the bridge. When using the **bridge-port** commands, you can specify any combination of components and ports. However, only certain combinations will produce a result.

In the current product version, the following usage restrictions exist:

- Component *c1* is strictly associated with the Ports *host* and *s1*
- Component *c2* is strictly associated with the Ports *eth0* and *s1*
- Component *c3* is strictly associated with the Ports *eth1* and *s1*
- Component *c4* is strictly associated with the Ports *eth2* and *s1*
- The Ports associated with the Component *s1* are dependent on the *c* components that currently exist. For example, if the components *c1* and *c4* already exist, then the Component *s1* is associated with the Ports *eth0, eth1, c1* and *c4*.

The validity of a specified combination should be tested before command execution.

You can use the **set bridge-port** command to assign the bridging port parameters.

```
set   bridge-port <comp-id-list> <bridge-port-list>
      [pvid <vlan>]
      [prio {0..7}]
      [admin untagged | tagged | all]
      [filter enabled | disabled]
```

You can use the **show bridge-port** command to display the bridging port attributes.

```
show  bridge-port [[{<comp-id-list> | all}] {<bridge-port-list> |
all}
      [{ info | mac-addr | num-ports | interface | pvid | prio
      | admin | filter | gvrp | vlan-restricted | last-pdu-origin
      | statistics}]]
```

Table 11-23 on page 205 lists and describes the bridging port attributes.

6.5 Configuring Provider Bridge and Advanced VLAN Settings

6.5.1 Configuring PEP Virtual Ports

PEP Virtual Ports are used to configure ingress port filtering. PEP table entries define traffic flows from the provider network to the customer edge port. The table is indexed by Component ID and S-VID. You can specify the default C-VID value and default user priority in the PEP table.

Use the following command to create and modify PEP Virtual Port elements:

```
set  pep-vp <c-comp-id-list> s1 <vid-list>
     [cpvid <vid>]
     [prio 0..7]
     [admit all | tagged | untagged]
     [filter enabled | disabled]
```

If the PEP Virtual Port entry does not already exist, the **set pep-vp** command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the PEP Virtual Port entry already exists, then the **set pep-vp** command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution:

- The **set pep-vp** command is valid only for those bridge ports which are S-component ports.
- The **set pep-vp** command fails if the port specified belongs to an S-component and not a C-component.
- The **set pep-vp** command also fails if the S-VID specified is not yet defined in the VLAN table.

Use the following command to display PEP Virtual Port entries:

```
show  pep-vp [{<c-comp-id-list> | all}
      [{all | <bridge-port-list>}
      [{all | <s-vid>}
      [{info | cpvid | prio | admit | filter}]]]].
```

Use the following command to delete PEP Virtual Port entries:

```
clear pep-vp {<c-comp-id-list> | all} {s1 | all} {<vid-list>
      | all}
```

Table 11-30 on page 212 lists and displays the PEP Virtual Port table attributes.

6.5.2 S-VID Translation Table

The S-VID Translation table is used to maintain bi-directional mapping between a Local S-VID (used in data and protocol frames transmitted and received through a CNP or PNP) and a Relay S-VID (used by the filtering and forwarding process).

Each VID Translation Table definition contains Component, Port, Local S-VID values and the Relay S-VID values for each specified S-VID. If no entry exists in this table for a specified Component, Port and Local S-VID, then a substitute value is taken from the Relay S-VID that is specified in a frame received on a Local S-VID Port.

All S-VID Translation table entries are permanent and are restored when the device is reset.

Use the following command to create and modify S-VID Translation table entries:

```
set svid-xlat s1 <ext-bridge-port-list> <vid> relay-svid <vid>
```

If the entry does not already exist, the **`set svid-xlat`** command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the **`set svid-xlat`** command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution of the **`set svid-xlat`** command:

- The command is valid only for bridge ports that are S-component ports.
- The **`set svid-xlat`** command fails if the port specified belongs to a C-component and not a S-component.
- The **`set svid-xlat`** command also fails if the S-VID specified is not yet defined in the VLAN table.

Use the following command to delete S-VID Translation table entries and clear their associated statistics:

```
clear svid-xlat {s1 | all} {<ext-bridge-port-list> | all} {<vid-
list> | all}
```

Use the following command to display S-VID Translation table entries:

```
show  svid-xlat [{s1 | all}
      [{<ext-bridge-port-list> | all}
      [{<vid-list> | all}
      [info]]]]
```

Table 11-31 on page 213 lists and displays the S-VID Translation table attributes.

6.5.3 C-VLAN Registration Table

An element of the C-VID registration table is accessed by PB C-VLAN component, Customer Edge Port bridge port number, and C-VID. Each element contains the mapping between a C-VID and the S-VID which carries the service and Booleans for handling untagged frames at the PEP and CEP.

Use the following command to create and modify C-VLAN Registration table entries:

```
set  cvlan-reg <c-comp-id-list> <ext-bridge-port-list> <vid-list>
     [svlan <vid>]
     [untag-cep yes | no]
     [untag-pep yes | no]
```

If the entry does not already exist, the **set cvlan-reg** command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the **set cvlan-reg** command replaces the attributes that are currently defined for the entry with those specified in the command.

Note the following conditions for execution of the **set cvlan-reg** command:

- The **set cvlan-reg** command is valid only for bridge ports that are external C-component ports: host, eth0, eth1 and eth2.
- The **set cvlan-reg** command fails if the port specified belongs to a S-component and not a C-component.
- The **set cvlan-reg** command also fails if the C-VID specified is not yet defined in the VLAN table.

Use the following command to display C-VLAN Registration table entries:

```
show  cvlan-reg [{<c-comp-id-list> | all}
      [{<ext-bridge-port-list> | all}
      [{<vid-list> | all} [{info | svlan | untag-cep
      | untag-pep}]]]]
```

Use the following command to delete C-VLAN Registration table entries:

```
clear cvlan-reg {<c-comp-id-list> | all} {<ext-bridge-port-list>
      | all} {<vid-list> | all}
```

Table 11-29 on page 211 lists and describes the C-VLAN Registration table attributes.

6.5.4 VLAN-to-SNMP ifTable

Whenever a VLAN is associated with Component c1, an entry in the SNMP ifTable is automatically created for that VLAN. When the VLAN is deleted, the corresponding ifTable entry is also deleted.

6.5.5 SNMP ifTable Attributes

Table 11-32 on page 214 lists and describes the attributes in the SNMP ifTable.

6.5.6 Forwarding Data Base (FDB)

The Forwarding Data Base (FDB) enables access to general parameters of the FDB Address table, which specifies configuration and control information for each Filtering Database currently operating on the device. Entries in the FDB Address table appear automatically when VLANs are assigned FDB IDs in the VLAN Table (*Table 11-28*). For more information about the FDB Address table, refer to *FDB Address Table* on page 75.

The system maintains 64 permanent instances of the FDB object.

Use the following command to create and modify FDB entries:

```
set fdb s1 <fdb-id-list> [aging <aging-time>]
```

Use the following command to display FDB entries:

```
show fdb   [s1
           [<fdb-id-list>
           [{aging | full-table-counter | num-of-dynamic}]]]
```

Table 11-33 on page 216 lists and describes the FDB attributes.

6.5.7 FDB Address Table

The FDB Address table contains information about unicast entries for which the device has forwarding and/or filtering information. This information is used by the transparent bridging function when determining how to propagate a received frame.

Entries in the FDB Address Table appear automatically when VLANs are assigned FDB IDs in the VLAN Table (*Table 11-28*).

Use the following command to create and modify entries in the FDB Address table:

```
set fdb-table s1 <fdb-id-list> <mac-addr> port <bridge-port>
```

If the FDB Address table entry does not already exist, the **`set fdb-table`** command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the entry already exists, then the **`set fdb-table`** command replaces the attributes that are currently defined for the entry with those specified in the command.

Note that the **set fdb-table** command fails if its port already exists in the FDB with **self** as the assigned status.

Use the following command to display FDB Address table entries:

```
show fdb-table
     [{s1 | all}
     [{<fdb-id-list> | all}
     [{<mac-addr> | all}
     [{info | port | status}]]]
```

Use the following command to delete FDB Address table entries and clear their associated statistics:

```
clear fdb-table {s1 | all} {<fdb-id-list> | all} {<mac-addr>
     | all}
```

Note that the **delete fdb-table** command fails if its port exists in the FDB with **self** as the assigned status.

Table 11-34 on page 217 lists and describes the FDB Address table attributes.

7 Performing Advanced Configuration

7.1 Configuring Quality-of-Service

Quality of Service (QoS) mechanisms enable service providers to offer different classes of service for different types of traffic or customers. QoS mechanisms are especially important in wireless links with adaptive capabilities, because changing link conditions may require the system to drop some traffic according to a predetermined priority and scheduling scheme.

EtherHaul has 8 priority queues per interface.

Queues are accessed by Strict Priority or Weighted Fair Queuing (WFQ) and Shaper mechanisms. QoS functions:

- Classifier (COS & EVC)
- Metering (CIR/EIR/CBS/EBS)
- Ingress QOS Marking (Green/Yellow/Red)
- Scheduler (Strict Priority/WFQ/ SP+Shaper /WFQ+Shaper)

7.1.1 QoS Classification

The EtherHaul 1200 QoS Engine classifies the incoming packets by port, VID, PCP, and/or DSCP (as defined by the IEEE 802.1 Q/p and RFC-2475 standards), or alternatively MPLS EXP bit and maps them onto {EVC, CoS} pairs.

The classification fields of VID, PCP and DSCP/MPLS-Exp represent the CoS that determine the egress queue.

Classification based on EVC forwards the packets through the meter and marker.

7.1.1.1 Classifier-Cos Settings

Use the following command to configure classifier-cos:

set classifier-cos <classifier-id: 1..248> [interface <host|eth0|eth1|eth2>] [precedence <1..8>] [vid < list 0..4094>] [pcp < list 0..7>] [ip-cos <{{dscp-cos | mpls-exp} <list of 0..7>}|dont-care>] [cos <0..7>]

The default system configuration is priority based on Vlan pBits (PCP) on all interfaces:

classifier-cos configuring
set classifier-cos 1 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 0 ip-cos dont-care cos 0
set classifier-cos 2 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 1 ip-cos dont-care cos 1
set classifier-cos 3 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 2 ip-cos dont-care cos 2

set classifier-cos 4 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 3 ip-cos dont-care cos 3
set classifier-cos 5 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 4 ip-cos dont-care cos 4
set classifier-cos 6 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 5 ip-cos dont-care cos 5
set classifier-cos 7 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 6 ip-cos dont-care cos 6
set classifier-cos 8 interface host,eth0,eth1,eth2 precedence 1 vid 0-4094 pcp 7 ip-cos dont-care cos 7

Classifier-Cos settings example for management priority (for traffic from ports: Host, Eth2):

```
set classifier-cos 1 interface host precedence 1 vid 0-4094 pcp 0-7 ip-cos dont-care cos 7
set classifier-cos 2 interface eth2 precedence 1 vid 0-4094 pcp 0-7 ip-cos dont-care cos 7
```

Classifier-Cos settings example for priority based on PCP (pBits) on Eth1, Eth0 with management priority (for traffic from ports: Host, Eth2):

```
# classifier-cos configuring
set classifier-cos 1 interface host,eth2 precedence 1 vid 0-4094 pcp 0-7 ip-cos dont-care cos 7

set classifier-cos 2 interface eth0,eth1 precedence 1 vid 0-4094 pcp 0 ip-cos dont-care cos 0
set classifier-cos 3 interface eth0,eth1 precedence 1 vid 0-4094 pcp 1 ip-cos dont-care cos 1
set classifier-cos 4 interface eth0,eth1 precedence 1 vid 0-4094 pcp 2 ip-cos dont-care cos 2
set classifier-cos 5 interface eth0,eth1 precedence 1 vid 0-4094 pcp 3 ip-cos dont-care cos 3
set classifier-cos 6 interface eth0,eth1 precedence 1 vid 0-4094 pcp 4 ip-cos dont-care cos 4
set classifier-cos 7 interface eth0,eth1 precedence 1 vid 0-4094 pcp 5 ip-cos dont-care cos 5
set classifier-cos 8 interface eth0,eth1 precedence 1 vid 0-4094 pcp 6 ip-cos dont-care cos 6
set classifier-cos 9 interface eth0,eth1 precedence 1 vid 0-4094 pcp 7 ip-cos dont-care cos 7
```

7.1.1.1.1 Classifier-EVC Settings

Use the following command to configure classifier-evc:
set classifier-evc <classifier-id: 1..248> [interface <host|eth0|eth1|eth2>] [precedence <1..8>] [vid < list 0..4094>] [pcp < list 0..7>] [ip-cos <{{dscp-cos | mpls-exp} <list of 0..7>}|dont-care>] [evc <1..31>]

Classifier-EVC settings for priority based on PCP (pBits) on Eth0 and Eth1:

```
# classifier-evc configuring
set classifier-evc 1 interface eth0 precedence 1 vid 0-4094 pcp 0
ip-cos dont-care evc 1
set classifier-evc 2 interface eth0 precedence 1 vid 0-4094 pcp 1
ip-cos dont-care evc 2
set classifier-evc 3 interface eth0 precedence 1 vid 0-4094 pcp 2
ip-cos dont-care evc 3
set classifier-evc 4 interface eth0 precedence 1 vid 0-4094 pcp 3
ip-cos dont-care evc 4
set classifier-evc 5 interface eth0 precedence 1 vid 0-4094 pcp 4
ip-cos dont-care evc 5
set classifier-evc 6 interface eth0 precedence 1 vid 0-4094 pcp 5
ip-cos dont-care evc 6
set classifier-evc 7 interface eth0 precedence 1 vid 0-4094 pcp 6
ip-cos dont-care evc 7
set classifier-evc 8 interface eth0 precedence 1 vid 0-4094 pcp 7
ip-cos dont-care evc 8
```

7.1.2 Metering and Coloring

7.1.2.1 Configuring Meter

This is an optional mechanism (only for use in cases in which classifier-evc is configured) to control and limit the traffic (committed rate and peak rate).

If a meter was defined for the classifier, the packet is internally colored (Green or Yellow) or dropped (Red) based on the following:

- CIR -Committed Information Rate [Mbps]. Represents the amount of credit the meter should receive each time interval.
- EIR – Excess Information Rate [Mbps]. Exceeding limitations of credits for each time interval.
- CBS - Committed Burst Size [bytes].
- EBS - Excess Burst Size [bytes].

Color-aware mode is supported for ingress S-VLAN packets only (based on MEF definitions).

Use the following command to configure a meter:

```
set meter <meter-id: 1..248>  [cir <0..1000>] [cbs <1522..50000>]
[eir <0..1000>] [ebs <1522..100000>] [color-mode < aware|blind>]
```

The following is an example of configuring a meter with 5Mbps CIR and 15Mbps EIR:

```
# meter configuring
set meter 1 cir 5 cbs 9600 eir 15 ebs 100000 color-mode blind
```

7.1.2.2 Binding Classifier and Meter

Use the following command to bind specific configured classifier-evc to CoS (queue) and Meter:

```
set ingress-qos <evc-id:1..31> <cos-id:0..7>  [meter <id: 0..248>]
[marking <enable|disable>]
```

The following is an example of binding the meter (configured above) to an evc and cos:

```
# ingress-qos configuring
set ingress-qos 5 5 meter 1 marking enable
```

7.1.3 QoS Scheduling

The EtherHaul 1200 QoS mechanism operates according to the following scheduling mechanisms:

- **Strict Priority** - Lower priority packets are served only if all higher priority queues are empty.
- **Weighted Fair Queuing (WFQ)** – Weights can be assigned to the radio queues, assuring fairness between the queues.
- **Shaper** – Sets the CIR (Committed Information Rate, i.e., the maximum rate) of the queues, with Strict Priority or WFQ

The default scheduling mode is Strict Priority.

When configuring the egress-cos, color-drop blind or aware can be configured.

7.1.3.1 Weighted Fair Queue (WFQ)

Weighted Fair Queuing (WFQ) can be used to provide different rates to different flows while maintaining fairness in order to avoid starvation. WFQ is a data packet scheduling technique that provides different scheduling priorities to statistically multiplexed data flows.

If the link data rate is R, weights of N data flows are W1,W2,…,Wn, the i'th data flow will achieve an average data rate of:

R*Wi / (W1 + W2 + … + Wn)

WFQ explicitly considers data queue, and by regulating the weights dynamically, WFQ can be utilized to control the QoS.

WFQ can only be configured for ETH0 queues 1 through 5. The highest queues, 6 and 7, are Strict Priority queues, and the lowest queue (0) is best effort.

Table 7-1 provides an example of WFQ.

Table 7-1 Weighted Fair Queue Example

Radio Rate	**320**	**Mbps**		
		# Queue	Weight	Expected Rate
Stream rate =	60	SP CoS 7	NA	60
Stream rate =	60	SP CoS 6	NA	60
Stream rate =	60	WFQ CoS 5	8	76.2
Stream rate =	60	WFQ CoS 4	6	57.1
Stream rate =	60	WFQ CoS 3	4	38.1
Stream rate =	60	WFQ CoS 2	2	19.0
Stream rate =	60	WFQ CoS 1	1	9.5
Stream rate =	60	BE CoS 0	0	0
Total =	**480**			

In this example, the introduced load exceeds the radio link rate (480>320 Mbps). The two highest queues (Strict Priority 6 and 7) take precedence over WFQ queues. The remaining bandwidth (320-60-60=200 Mbps) is split among the weighted queues (1 - 5).

The lowest queue (Best Effort 0) gets no bandwidth.

The following is an example of WFQ configuration:

```
# Scheduler mode configuration
set scheduler mode wfq
# egress-qos configuring
set egress-qos eth0 1  color-drop blind weight 1 cir 0
set egress-qos eth0 2  color-drop blind weight 2 cir 0
set egress-qos eth0 3  color-drop blind weight 4 cir 0
set egress-qos eth0 4  color-drop blind weight 6 cir 0
set egress-qos eth0 5  color-drop blind weight 8 cir 0
```

7.1.3.2 Shaper

Shaper is used to control traffic flows in order to optimize or guarantee performance and improve latency by limiting the maximum bandwidth of certain flows to maintain fairness and to assure SLA.

You must set the Committed Information Rate to a value between 1-1000 Mbps.

Table 7-2 provides an example of Shaper.

Table 7-2 Shaper Example

Radio Rate	320	Mbps		
		# Queue	CIR	Expected Rate
Stream rate =	60	SP CoS 7	NA	60
Stream rate =	60	SP CoS 6	NA	60
Stream rate =	60	CIR CoS 5	50	50
Stream rate =	45	CIR CoS 4	40	40
Stream rate =	15	CIR CoS 3	10	10
Stream rate =	20	CIR CoS 2	20	20
Stream rate =	40	CIR CoS 1	30	30
Stream rate =	70	BE CoS 0	0	50
Total =	370			320

The following is an example of Shaper (Strict Priority) configuration.

```
# scheduler configuring
set scheduler mode priority-shaper

# egress-qos configuring
set egress-qos eth0 1  color-drop blind weight 1 cir 10
set egress-qos eth0 2  color-drop blind weight 2 cir 20
set egress-qos eth0 3  color-drop blind weight 4 cir 30
set egress-qos eth0 4  color-drop blind weight 6 cir 40
set egress-qos eth0 5  color-drop blind weight 8 cir 50
```

7.1.3.3 Egress Queues

There are eight egress queues, one queue per CoS. Eight queues on the interfaces (Eth0, Eth1, and Eth2) are served by four queues on the radio (RF).

WFQ and Shaper can only be configured for queues 1 through 5.

7.2 Configuring CFM (Connectivity Fault Management)

This section explains how to configure CFM, and includes the following topics:

- CFM Overview
- Working with Maintenance Domains
- Working with Maintenance Associations
- Working with Component Maintenance Associations
- Working with Maintenance End Points
- Working with CCM Messages
- Working with Peer MEPs
- Working with the Peer MEP Database
- Working with Linktrace Messages
- Sample CFM Configuration

7.2.1 CFM Overview

Connectivity Fault Management (CFM) is an Ethernet layer operation, administration, and management (OAM) protocol designed to monitor and troubleshoot networks. CFM enables you to detect, verify, and isolate connectivity failures in virtual bridged local area networks.

A Maintenance Domain (MD) is a part of a network that is controlled by a single operator and used to support the connectivity between service access points. There are eight hierarchical Maintenance Domain Levels (MD Level). Each CFM layer supports OAM capabilities independently, with the customer at the highest level, the provider in the middle, and the operator at the lowest level.

CFM is designed to be transparent to the customer data transported by the network and to provide maximum fault coverage. These capabilities are used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment.

CFM entities support an individual service instance as Maintenance Association End Points (MEPs) are configured to create a Maintenance Association (MA). The MA monitors connectivity provided by that instance through the Maintenance Domain. Maintenance Association Intermediate Points (MIPs) are the intermediate points in a specific MA or MD.

The major features of CFM are fault detection, path discovery, fault verification, fault isolation, and fault recovery.

7.2.1.1 Fault Detection

A Continuity Check protocol detects both connectivity failures and unintended connectivity between service instances (heartbeat). Each MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA, and tracks the CCMs received from the other MEPs.

7.2.1.2 Path Discovery

The path is determined by the linktrace (L2 Trace Route). Linktrace messages (LTM) are multicast from the originating MEP to the target MAC (MIP or MEP)/MEP ID. Linktrace replies (LTR) are unicast from the target (or MIPs on route) to the originating MEP.

7.2.1.3 Fault Verification and Isolation

A Loopback protocol performs fault verification, typically after fault detection. An MEP can be ordered to transmit a unicast Loopback Message (LBM) to an MEP or MIP in the MA. The receiving MP responds by transforming the LBM into a unicast Loopback Reply (LBR) sent back to the originating MEP.

7.2.1.4 Fault Notification and Recovery

When an MEP detects a connectivity fault in its in its MA (CCM is not received or an invalid CCM is received), it sends an SNMP trap and enters a log entry. The network administrator responds to a fault notification to categorizing, isolating, and resolving the connectivity fault. For information on troubleshooting procedures, refer to *EtherHaul Diagnostics* on page 140.

7.2.2 Working with Maintenance Domains

A Maintenance Domain (MD) is a part of a network that is controlled by a single operator and used to support the connectivity between service access points. Each of the eight hierarchical Maintenance Domain Levels (MD Level) supports OAM capabilities independently.

Use the following command to set an MD. Note that the **`name`** attribute must be unique in the system.

```
set   cfm-md <md-idx> [format <md-name-format>] [name <md-name>]
[level <md level>] [mhf-creation <mhf creation>] [mhfid-permission
<mhf permission>]
```

For example, the following command sets the customer domain at level 2.

```
set cfm-md 2 name string Customer level 2
```

Use the following command to display a particular MD or all MDs.

```
show cfm-md {<md-idx-list> | all} {format | name | level |  mhf-
creation | mhfid-permission | info}
```

Use the following command to clear a particular MD or all MDs:

```
clear cfm-md {<md-idx-list> | all}
```

For example, the following command clears all the MDs in the system.

```
clear cfm-md all
```

Table 11-9 on page 183 lists and describes the MD attributes.

7.2.3 Working with Maintenance Associations

A Maintenance Association (MA) is used to monitor connectivity in relation to a specific service instance. All CFM entities that support that service instance are configured as MEPs, with the same Maintenance Association Identifier (MAID) and MD Level.

Use the following command to set an MA. Note that the **ma-name** attribute is mandatory, and must be unique in the system.

set cfm-ma <md-idx> <ma-idx> [format <ma-name-format>] [name <ma-name>] [interval <ccm-interval>]

Use the following command to display a particular MA or all MAs:

show cfm-ma {<md-idx-list> | all} {<ma-idx-list> | all} {name | component | interval | info}

Use the following command to clear a particular MA or all MAs:

```
clear cfm-ma {<md-idx-list> | all} {<ma-idx-list> | all}
```

Table 11-10 on page 184 lists and describes the MA attributes.

7.2.4 Working with Component Maintenance Associations

Use the following command to set a Component MA:

```
set cfm-ma-comp <comp-id> <md-idx> <ma-idx> [vlan <vid>] [mhf-creation <mhf-creation>] [mhfid-permission <mhf-permission>]
```

Use the following command to display a particular Component MA or all Component MAs:

```
show cfm-ma-comp {<comp-id-list | all} {<md-idx-list> | all} {<ma-idx-list> | all} {vlan | mhf-creation | mhfid-permission | info}
```

Use the following command to clear a particular Component MA or all Component MAs:

```
clear cfm-ma-comp {<comp-id-list | all} {<md-idx-list> | all} {<ma-idx-list> | all}
```

Table 11-11 on page 184 lists and describes the Component MA attributes.

7.2.5 Working with Maintenance End Points (MEPS)

A Maintenance End Point (MEP) is a point, on the perimeter of a domain, which sends and receives CFM frames through the domain.

Use the following command to set an MEP:

set cfm-mep <md-idx> <ma-idx> <mepid> [interface <ext-bridge-port-list>] [dir {down | up}] [vlan {1..4094}] [admin-state {active | inactive}] [cci {enabled | disabled}] [msg-prio {0..7}] [low-defect <low-defect>] [alarm-time {250..1000}] [reset-time {250..1000}] [lbm-dst-type {mac | mepid}] [lbm-dst-mac <mac addr>] [lbm-dst-mepid <mepid>] [lbm-tx-num {1..1024}] [lbm-tx-data <hex string>] [lbm-tx-prio {0..7}] [lbm-tx-drop {enable | disable}] [ltm-dst-type {mac | mepid}] [ltm-dst-mac <mac addr>] [ltm-dst-mepid <mepid>] [ltm-tx-ttl {0..250}] }] [lbm-tx-status {tx-pending | tx-idle}] [ltm-tx-status {tx-pending | tx-idle}]

Use the following command to display a particular MEP or all MEPs:

show cfm-mep [{<md-idx-list> | all} [{<ma-idx-list> | all} [{<mepid-list> | all}]]] {interface | dir | vlan | admin-state | cci | msg-prio | low-defect | alarm-time | reset-time | lbm-dst-mac | lbm-dst-mepid | lbm-dst-type | lbm-tx-num | lbm-tx-data | lbm-tx-prio | lbm-tx-drop | ltm-dst-mac | ltm-dst-mepid | ltm-dst-type | ltm-tx-ttl | lbm-tx-status | ltm-tx-status | fng-state | mac | high-defect | defects | ccm-seq-errors | ccm-tx | lbm-tx-result | lbm-tx-sn | lbm-next-sn | lbr-in-order | lbr-out-of-order | lbr-tx | ltm-next-sn | ltr-unexpected | ltm-tx-result | ltm-tx-sn | last-error-ccm | last-xcon-ccm | info}

Use the following command to clear a particular MEP or all MEPs:

clear cfm-mep {<md-idx-list> | all} {<ma-idx-list> | all} {<mepid-list> | all}

MEP commands include both configurable and read-only attributes.

Table 11-12 on page 186 lists and describes the configurable MEP attributes. *Table 11-13* on page 190 lists and describes the read-only MEP attributes. You can display these attributes using the **`show cfm-mep`** command.

7.2.6 Working with CCM Messages

An MEP can periodically transmit a multicast Connectivity Check Message (CCM) announcing the identity of the MEP and its MA. The MEP also tracks CCMs received from the other MEPs.

The following information is displayed per CCM message stored:

- Eth Source Address
- VLAN Priority (PCP)
- Drop Eligibility
- VLAN ID
- MD Level
- Version
- RDI
- CCM Interval
- Sequence Number
- Counters: TxFCf, RxFCb, TxFCb
- If present:
- Sender Chassis Subtype and ID
- Management Address Domain
- Management Address
- Port Status -- {blocked | up} (according to IEEE 802.1ag Table 21-10
- Interface Status -- {up | down | testing | unknown | dormant | not-present | lower-layer-down} according to IEEE 802.1ag Table 21-1
- Other TLVs: Type, Data as hexadecimal string

To display this information, use the following commands:

```
show cfm-ccm  [{<md-idx-list> | all} [{<ma-idx-list> | all}
[{<mepid-list> | all}]]] last-error-ccm
```

and

```
show cfm-ccm [{<md-idx-list> | all} [{<ma-idx-list> | all}
[{<mepid-list> | all}]]] last-xcon-ccm
```

Table 11-14 on page 191 lists and describes the CCM message attributes.

7.2.7 Working with Peer MEPs

MEPs connected by the EtherHaul Provider Bridge feature are known as Peer MEPs. Peer MEPs can be used to measure CCM delay and changes in that delay.

Use the following command to create a Peer MEP entry. This command causes automatic creation of entries in the Peer MEP DB for all MEPIDs that have entries in MEP table and this Peer MEP ID.

```
set cfm-peer-mep-create <md-idx-list> <ma-idx-list> <peer-mepid-list>
```

Use the following command to display Peer MEP information:

```
show cfm-peer-mep-create [{<md-idx-list> | all} [{<ma-idx-list> | all}  [{<peer-mepid-list> | all}}]]
```

Use the following command to delete a Peer MEP entry. This command causes automatic deletion of entries in the Peer MEP DB for all MEPIDs that have entries in MEP Table and this Peer MEP ID.

```
clear cfm-peer-mep-create {<md-idx-list> | all} {<ma-idx-list> | all} {<peer-mepid-list> | all}
```

Table 11-15 on page 192 lists and describes the Peer MEP attributes.

7.2.8 Working with the Peer MEP Database

The Peer MEP Database (MEP DB) contains the records of delays and changes in delays reported by Peer MEPs.

Use the following command to display Peer MEP DB information. The information displayed is only for Peer MEPs which have been reported. For those that do not report, this command will display the message “unreachable”.

show cfm-peer-mep-db [{<md-idx-list> | all} [{<ma-idx-list> | all} [{<mepid-list> | all} [{<peer-mepid-list> | all}}]]]

Table 11-16 on page 192 lists and describes the Peer MEP DB attributes.

7.2.9 Working with Linktrace Messages

Linktrace messages are multicast from an originating MEP to a target MAC (MIP or MEP)/MEP ID, to verify the path between the two. Linktrace Reply messages (LTRs) are unicast from the target (or MIPs on route) to the originating MEP. Receipt of an LTR verifies the path.

Arriving LTRs are stored on a per-MEP basis in the LTR database, as shown in *Figure 7-1*.

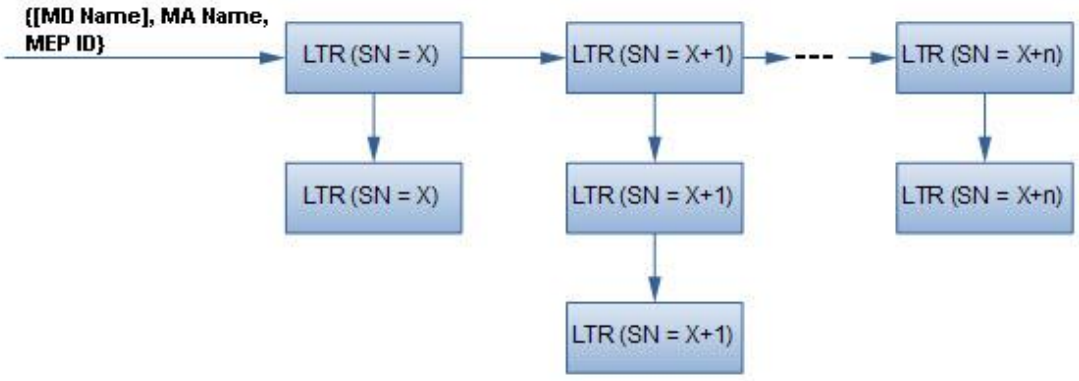


Figure 7-1. Per-MEP LTR Storage Structure

LTRs are stored in ascending sequence number order and LTRs with the same sequence number (i.e., replies to the same LTM) are grouped together.

Since storage is limited, arrival of a new message results in discarding older messages. Entire groups that use the same sequence number are discarded.

Use the following command to display LTR database information:

show cfm ltr-db [{<md-idx-list> | all} [{<ma-idx-list> | all} [{<mepid-list> | all} [{SN-list | all}]]]]

SN stands for the Sequence Number of the LTR message stored. This does not refer to the real sequence number stored in the LTR header, but rather, to the relative SN which is equal to Real SN modulo Maximum Allowed Number of SNs.

For example, if the maximum allowed number of stored LTRs (with different SNs) is 20, then the Real SN = 807 is translated into the Relative SN = 7.

It is possible to specify more than one SN in the command by designating indexed objects. For more information, refer to *Designating Indexed Objects* on page 159.

Table 11-17 on page 195 lists and describes the LTR attributes.

7.2.10 Sample CFM Configuration

This section provides a sample CFM configuration script.

Configuring the Local ODU

The first step in configuring CFM parameters is to enable the OAM license, which is part of the L2 Networking license. Without an enabled OAM license, the necessary CFM commands are not available.

```
set license oam status enable
```

The next step in this configuration is to configure an MD at level 0:

set cfm-md 1 name string Link level 0

The following command creates an MA.

```
set cfm-ma 1 1 name string Link interval 300hz
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector.

```
set cfm-ma-comp c2 1 1 vlan 200
```

The following command creates a Maintenance End Point (MEP).

```
set cfm-mep 1 1 1 interface eth0 dir down cci enabled
```

The following command creates a Peer MEP.

```
set cfm-peer-mep-create 1 1 2
```

The following command creates an MD at level 2.

```
set cfm-md 2 name string Customer level 2
```

The following command creates an MA.

```
set cfm-ma 2 2 name string Customer  interval 1s
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector.

```
set cfm-ma-comp c3 2 2 vlan 200
```

The following command creates a Maintenance End Point (MEP).

```
set cfm-mep 2 2 1 interface eth1 dir up cci enabled
```

The following command creates a Peer MEP.

```
set cfm-peer-mep-create 2 2 2
```

The following command sets the MIP to the lower level.

```
set cfm-ma-comp c3 2 2 vlan 200 mhf-creation explicit
```

To create MIPs on the radio potr (lower level), you must create the Component MA on C3 (Up MEP). If the C3 Component MA is not created on C3, the CFM packets will not enter and pass the through the MIP.

The MHF-Creation value, which determines whether MIPs are created, can be on one of two settings:

- **Default** – Creates MIPs on all ports.
- **Explicit** – Creates MIPS only on ports that have MEPs on their lower level.

Configuring the Remote ODU

The first step in configuring CFM parameters is to enable the OAM license. Without an enabled OAM license, the necessary CFM commands are not available.

```
set license oam status enable
```

The next step in this configuration is to configure an MD at level 0:

```
set cfm-md 1 name string Link level 0
```

The following command creates an MA.

```
set cfm-ma 1 1 name string Link interval 300hz
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector.

```
set cfm-ma-comp c2 1 1 vlan 200
```

The following command creates a Maintenance End Point (MEP).

```
set cfm-mep 1 1 2 interface eth0 dir down cci enabled
```

The following command creates a Peer MEP.

```
set cfm-peer-mep-create 1 1 1
```

The following command creates an MD at level 2.

```
set cfm-md 2 name string Customer level 2
```

The following command creates an MA.

```
set cfm-ma 2 2 name string Customer  interval 1s
```

The following command creates a Component MA and assigns VLAN 200 as its Service Selector.

```
set cfm-ma-comp c3 2 2 vlan 200
```

The following command creates a Maintenance End Point (MEP).

```
set cfm-mep 2 2 2 interface eth1 dir up cci enabled
```

The following command creates a Peer MEP.

```
set cfm-peer-mep-create 2 2 1
```

The following command sets the MIP to the lower level.

```
set cfm-ma-comp c3 2 2 vlan 200 mhf-creation explicit
```

Checking the CCM Status

```
show cfm-peer-mep

cfm-peer-mep 1 1 1 2 state                  : ok
<---ok or failed
cfm-peer-mep 1 1 1 2 failed-ok-time         : 0000:02:22:05
cfm-peer-mep 1 1 1 2 mac                    : 00:24:a4:00:01:e1
cfm-peer-mep 1 1 1 2 rdi                    : off
cfm-peer-mep 1 1 1 2 port-status            : unknown
cfm-peer-mep 1 1 1 2 if-status              : unknown
cfm-peer-mep 1 1 1 2 chassis-id-subtype     : unknown
cfm-peer-mep 1 1 1 2 mng-addr-domain        : unknown

cfm-peer-mep 2 2 1 2 state                  : ok
cfm-peer-mep 2 2 1 2 failed-ok-time         : 0000:02:22:05
```

```
cfm-peer-mep 2 2 1 2 mac                    : 00:24:a4:00:01:e2
cfm-peer-mep 2 2 1 2 rdi                    : off
cfm-peer-mep 2 2 1 2 port-status            : unknown
cfm-peer-mep 2 2 1 2 if-status              : unknown
cfm-peer-mep 2 2 1 2 chassis-id-subtype     : unknown
cfm-peer-mep 2 2 1 2 mng-addr-domain        : unknown
```

Configure the Loopback on the Local ODU

The following set of commands sets up the Loopback on the local ODU. You must set the destination type (mepid or mac) and the destination MEP ID, determine the number of loopback packets to transmit, and enable the Loopback for transmit.

Enter the following commands on the link level:

```
set cfm-mep 1 1 1 lbm-dst-type mepid
set cfm-mep 1 1 1 lbm-dst-mepid 2
set cfm-mep 1 1 1 lbm-tx-num 10
set cfm-mep 1 1 1 lbm-tx-status tx-pending
```

Enter the following commands on the customer level:

```
set cfm-mep 2 2 1 lbm-dst-type mepid
set cfm-mep 2 2 1 lbm-dst-mepid 2
set cfm-mep 2 2 1 lbm-tx-num 10
set cfm-mep 2 2 1 lbm-tx-status tx-pending
```

To view the loopback reply, you must first verify the number for **lbr-in-order**. You can then transmit the loopback packets, using the following command:

```
set cfm-mep 1 1 1 lbm-tx-status tx-pending
```

Re-check the number for **lbr-in-order** to verify that all packets were received.

```
show cfm-mep
cfm-mep 1 1 1 interface             : eth0
cfm-mep 1 1 1 dir                   : down
cfm-mep 1 1 1 vlan                  : none
cfm-mep 1 1 1 admin-state           : active
cfm-mep 1 1 1 cci                   : enabled
cfm-mep 1 1 1 msg-prio              : 0
cfm-mep 1 1 1 low-defect            : mac-rem-err-xcon
cfm-mep 1 1 1 alarm-time            : 250
cfm-mep 1 1 1 reset-time            : 1000
cfm-mep 1 1 1 lbm-dst-mac           : 00:00:00:00:00:00
cfm-mep 1 1 1 lbm-dst-mepid         : 2
cfm-mep 1 1 1 lbm-dst-type          : mepid
cfm-mep 1 1 1 lbm-tx-num            : 10
cfm-mep 1 1 1 lbm-tx-data-len       : 0
cfm-mep 1 1 1 lbm-tx-prio           : 0
cfm-mep 1 1 1 lbm-tx-drop           : enable
```

```
cfm-mep 1 1 1 ltm-dst-mac           : 00:00:00:00:00:00
cfm-mep 1 1 1 ltm-dst-mepid         : 1
cfm-mep 1 1 1 ltm-dst-type          : mac
cfm-mep 1 1 1 ltm-tx-ttl            : 64
cfm-mep 1 1 1 lbm-tx-status         : tx-idle
cfm-mep 1 1 1 ltm-tx-status         : tx-idle
cfm-mep 1 1 1 fng-state             : fngReset
cfm-mep 1 1 1 mac                   : 00:24:a4:00:07:59
cfm-mep 1 1 1 high-defect           : none
cfm-mep 1 1 1 defects               :
cfm-mep 1 1 1 ccm-seq-errors        : 0
cfm-mep 1 1 1 ccm-tx                : 656243
cfm-mep 1 1 1 lbm-tx-result         : ok
cfm-mep 1 1 1 lbm-tx-sn             : 19
cfm-mep 1 1 1 lbm-next-sn           : 20
cfm-mep 1 1 1 lbr-in-order          : 20
cfm-mep 1 1 1 lbr-out-of-order      : 0
cfm-mep 1 1 1 lbr-tx                : 0
cfm-mep 1 1 1 ltm-next-sn           : 0
cfm-mep 1 1 1 ltr-unexpected        : 0
cfm-mep 1 1 1 ltm-tx-result         : unknown
cfm-mep 1 1 1 ltm-tx-sn             : 0
cfm-mep 1 1 1 lm                    : disabled
cfm-mep 1 1 1 lm-interval           : 10s
cfm-mep 1 1 1 dm                    : disabled
cfm-mep 1 1 1 dm-interval           : 10s
cfm-mep 1 1 1 ais-generate          : disabled
cfm-mep 1 1 1 ais-period            : 1s
cfm-mep 1 1 1 ais-level             : 7
cfm-mep 1 1 1 ais-suppress          : enabled
cfm-mep 1 1 1 ais-defects           : none

cfm-mep 2 2 1 interface             : eth1
cfm-mep 2 2 1 dir                   : up
cfm-mep 2 2 1 vlan                  : none
cfm-mep 2 2 1 admin-state           : active
cfm-mep 2 2 1 cci                   : enabled
cfm-mep 2 2 1 msg-prio              : 0
cfm-mep 2 2 1 low-defect            : mac-rem-err-xcon
cfm-mep 2 2 1 alarm-time            : 250
cfm-mep 2 2 1 reset-time            : 1000
cfm-mep 2 2 1 lbm-dst-mac           : 00:00:00:00:00:00
cfm-mep 2 2 1 lbm-dst-mepid         : 2
cfm-mep 2 2 1 lbm-dst-type          : mepid
cfm-mep 2 2 1 lbm-tx-num            : 10
cfm-mep 2 2 1 lbm-tx-data-len       : 0
```

```
cfm-mep 2 2 1 lbm-tx-prio           : 0
cfm-mep 2 2 1 lbm-tx-drop           : enable
cfm-mep 2 2 1 ltm-dst-mac           : 00:00:00:00:00:00
cfm-mep 2 2 1 ltm-dst-mepid         : 1
cfm-mep 2 2 1 ltm-dst-type          : mac
cfm-mep 2 2 1 ltm-tx-ttl            : 64
cfm-mep 2 2 1 lbm-tx-status         : tx-idle
cfm-mep 2 2 1 ltm-tx-status         : tx-idle
cfm-mep 2 2 1 fng-state             : fngReset
cfm-mep 2 2 1 mac                   : 00:24:a4:00:07:5a
cfm-mep 2 2 1 high-defect           : none
cfm-mep 2 2 1 defects               :
cfm-mep 2 2 1 ccm-seq-errors        : 2
cfm-mep 2 2 1 ccm-tx                : 1948
cfm-mep 2 2 1 lbm-tx-result         : ok
cfm-mep 2 2 1 lbm-tx-sn             : 9
cfm-mep 2 2 1 lbm-next-sn           : 10
cfm-mep 2 2 1 lbr-in-order          : 10
cfm-mep 2 2 1 lbr-out-of-order      : 0
cfm-mep 2 2 1 lbr-tx                : 0
cfm-mep 2 2 1 ltm-next-sn           : 0
cfm-mep 2 2 1 ltr-unexpected        : 0
cfm-mep 2 2 1 ltm-tx-result         : unknown
cfm-mep 2 2 1 ltm-tx-sn             : 0
cfm-mep 2 2 1 lm                    : disabled
cfm-mep 2 2 1 lm-interval           : 10s
cfm-mep 2 2 1 dm                    : disabled
cfm-mep 2 2 1 dm-interval           : 10s
cfm-mep 2 2 1 ais-generate          : disabled
cfm-mep 2 2 1 ais-period            : 1s
cfm-mep 2 2 1 ais-level             : 7
cfm-mep 2 2 1 ais-suppress          : enabled
cfm-mep 2 2 1 ais-defects           : none
```

Configuring the Link Trace

There are five indices. The first three are the MEP, the fourth is the index number of the LTR packet (each LTR is one packet), and the fifth is the number of replies according to their order of arrival. Where several elements answer, you must check the TTL to identify the trace.

Enter the following on the link level:

```
set cfm-mep 1 1 1 ltm-dst-type mepid
set cfm-mep 1 1 1 ltm-dst-mepid 2
set cfm-mep 1 1 1 ltm-tx-status tx-pending
```

```
show cfm-mep 1 1 1 ltr

cfm-mep 1 1 1 0 0 rx-ttl                 : 63
cfm-mep 1 1 1 0 0 ltr-forward            : unknown
cfm-mep 1 1 1 0 0 relay-action           : hit
cfm-mep 1 1 1 0 0 chassis-id-subtype     : unknown
cfm-mep 1 1 1 0 0 mng-addr-domain        : unknown
cfm-mep 1 1 1 0 0 ingr-action            : ok
cfm-mep 1 1 1 0 0 ingr-mac               : 00:24:a4:00:07:a9
cfm-mep 1 1 1 0 0 ingr-port-id-subtype   : unknown
cfm-mep 1 1 1 0 0 egr-action             : none
cfm-mep 1 1 1 0 0 egr-mac                : 00:00:00:00:00:00
cfm-mep 1 1 1 0 0 egr-port-id-subtype    : unknown
cfm-mep 1 1 1 0 0 trm-mep                : unknown
cfm-mep 1 1 1 0 0 last-egr-id            : 00-00-00-24-a4-00-07-59
cfm-mep 1 1 1 0 0 next-egr-id            : 00-00-00-00-00-00-00-00
```

Enter the following on the customer level:

```
set cfm-mep 2 2 1 ltm-dst-type mepid
set cfm-mep 2 2 1 ltm-dst-mepid 2
set cfm-mep 2 2 1 ltm-tx-status tx-pending

show cfm-mep 2 2 1 ltr

cfm-mep 2 2 1 0 0 rx-ttl                 : 63
cfm-mep 2 2 1 0 0 ltr-forward            : unknown
cfm-mep 2 2 1 0 0 relay-action           : fdb
cfm-mep 2 2 1 0 0 chassis-id-subtype     : unknown
cfm-mep 2 2 1 0 0 mng-addr-domain        : unknown
cfm-mep 2 2 1 0 0 ingr-action            : ok
cfm-mep 2 2 1 0 0 ingr-mac               : 00:24:a4:00:07:59
cfm-mep 2 2 1 0 0 ingr-port-id-subtype   : unknown
cfm-mep 2 2 1 0 0 egr-action             : none
cfm-mep 2 2 1 0 0 egr-mac                : 00:00:00:00:00:00
cfm-mep 2 2 1 0 0 egr-port-id-subtype    : unknown
cfm-mep 2 2 1 0 0 trm-mep                : unknown
cfm-mep 2 2 1 0 0 last-egr-id            : 00-00-00-24-a4-00-07-5a
cfm-mep 2 2 1 0 0 next-egr-id            : 00-00-00-24-a4-00-07-59

cfm-mep 2 2 1 0 1 rx-ttl                 : 62
cfm-mep 2 2 1 0 1 ltr-forward            : unknown
cfm-mep 2 2 1 0 1 relay-action           : fdb
cfm-mep 2 2 1 0 1 chassis-id-subtype     : unknown
cfm-mep 2 2 1 0 1 mng-addr-domain        : unknown
cfm-mep 2 2 1 0 1 ingr-action            : ok
```

```
cfm-mep 2 2 1 0 1 ingr-mac                : 00:24:a4:00:07:a9
cfm-mep 2 2 1 0 1 ingr-port-id-subtype    : unknown
cfm-mep 2 2 1 0 1 egr-action              : none
cfm-mep 2 2 1 0 1 egr-mac                 : 00:00:00:00:00:00
cfm-mep 2 2 1 0 1 egr-port-id-subtype     : unknown
cfm-mep 2 2 1 0 1 trm-mep                 : unknown
cfm-mep 2 2 1 0 1 last-egr-id             : 00-00-00-24-a4-00-07-59
cfm-mep 2 2 1 0 1 next-egr-id             : 00-00-00-24-a4-00-07-aa

cfm-mep 2 2 1 0 2 rx-ttl                  : 61
cfm-mep 2 2 1 0 2 ltr-forward             : unknown
cfm-mep 2 2 1 0 2 relay-action            : hit
cfm-mep 2 2 1 0 2 chassis-id-subtype      : unknown
cfm-mep 2 2 1 0 2 mng-addr-domain         : unknown
cfm-mep 2 2 1 0 2 ingr-action             : ok
cfm-mep 2 2 1 0 2 ingr-mac                : 00:24:a4:00:07:aa
cfm-mep 2 2 1 0 2 ingr-port-id-subtype    : unknown
cfm-mep 2 2 1 0 2 egr-action              : none
cfm-mep 2 2 1 0 2 egr-mac                 : 00:00:00:00:00:00
cfm-mep 2 2 1 0 2 egr-port-id-subtype     : unknown
cfm-mep 2 2 1 0 2 trm-mep                 : unknown
cfm-mep 2 2 1 0 2 last-egr-id             : 00-00-00-24-a4-00-07-aa
cfm-mep 2 2 1 0 2 next-egr-id             : 00-00-00-00-00-00-00-00
```

7.3 Configuring Link OAM

This section explains how to configure Link OAM.

Link OAM, as defined in IEEE802.3ah, is an Ethernet layer operation, administration, and management (OAM) protocol designed to monitor and troubleshoot networks. Link OAM enables you to detect, verify, and isolate connectivity failures in point-to-point connections.

7.3.1 Enabling Link OAM

Link OAM can be enabled on one of the link interfaces (Eth1, Eth2) or the radio interface (Eth0).

To enable Link OAM:

```
set link-oam <eth-list: eth0 | eth1 | eth2>  [admin <value:
Enabled | disabled >]


default>set link-oam eth0 admin enabled
```

To view Link OAM configuration and status:

```
default>show link-oam

link-oam eth0 admin                 : enabled
link-oam eth0 status                : operational
link-oam eth0 mode                  : active
link-oam eth0 pdu-size              : 1518
link-oam eth0 revision              : 0
link-oam eth0 functions             : loopback

link-oam eth1 admin                 : disabled
link-oam eth1 status                : disabled
link-oam eth1 mode                  : active
link-oam eth1 pdu-size              : 1518
link-oam eth1 revision              : 0
link-oam eth1 functions             : loopback

link-oam eth2 admin                 : disabled
link-oam eth2 status                : disabled
link-oam eth2 mode                  : active
link-oam eth2 pdu-size              : 1518
link-oam eth2 revision              : 0
link-oam eth2 functions             : loopback
```

7.3.2 Link OAM Discovery

Once enabled, the Link OAM will perform discovery of the peer Ethernet port.

To view the discovered peer port (MAC address and other settings):

```
default>show link-oam-peer eth0

link-oam-peer eth0 mac-addr              : 00:24:a4:00:1f:b8
link-oam-peer eth0 vendor-oui            : 00-24-a4
link-oam-peer eth0 vendor-info           : 0
link-oam-peer eth0 mode                  : active
link-oam-peer eth0 pdu-size              : 1518
link-oam-peer eth0 revision              : 2
link-oam-peer eth0 functions             : loopback
```

7.3.3 Link OAM Loopback

Link OAM loopback is supported and can be enabled on the Ethernet port. Once enabled, traffic received on the port will be looped back to the port initiated the remote loopback.

To set Link OAM loopback:

```
set link-oam-loopback <eth-list: eth0|eth1|eth2>  [status <value:
init|terminate>] [peer-request <value: ignore|process>]
```

To allow ports to enter loopback state (when receiving remote loopback initiation command) the peer-request status should be set to **process**:

```
default>set link-oam-loopback eth0 peer-request process
```

To initiate loopback on remote port the loopback status should be set to **init**:

```
default>set link-oam-loopback eth0 status init
```

To view loopback settings:

```
default >show link-oam-loopback eth0

link-oam-loopback eth0 status                : remote
link-oam-loopback eth0 peer-request          : process
```

The **status** will change to **remote** on the port that initiated the loopback (i.e., sent the request for loopback) and **local** on the port performing the loopback.

Use reset loopback command to stop the loopback and return to **status: none**;

```
default >reset link-oam-loopback eth0
```

```
default >show link-oam-loopback eth0
link-oam-loopback eth0 status                : none
link-oam-loopback eth0 peer-request          : process
```

7.4 Configuring Synchronous Ethernet (SyncE)

7.4.1 SyncE Overview

The EtherHaul 1200 provides Synchronous Ethernet (SyncE) capabilities, receiving a synchronized Ethernet link and providing a synchronized Ethernet link on the other end of the wireless link within the required masks.

SyncE is a link-by-link distribution scheme that uses the Ethernet physical layer to accurately distribute clock frequency. ITU-T standard G.8261 defines various aspects of SyncE, such as the acceptable limits of jitter and wander as well as the minimum requirements for synchronization of network elements.

With SyncE, the receive clock is extracted from the Ethernet Rx by the clock unit and used for transmission on all interfaces, propagating the clock in the path. Every SyncE Network Element contains an internal clock called the Ethernet Equipment Clock (EEC). The EEC locks on the Rx clock and distributes it for transmission on all interfaces, attenuating jitter and wander, and maintaining clock-in holdover. If the Rx clock fails, the local unit switches to holdover and regenerates the clock accurately until the failure is corrected.

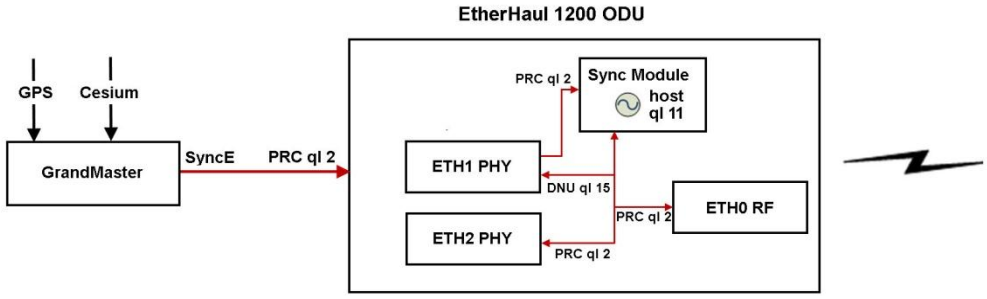


Figure 7-2 SyncE Functional Diagram

Synchronization messages are transported between the SyncE elements using Ethernet Synchronization Message Channel (ESMC). ESMC is similar to SSM (Synchronization Status Message), used in Sonnet/SDH systems. ESMC carries information about the Quality Level (ql) and sync status of the source clock, enabling the EtherHaul 1200 to determine which clock source of use-based on performance and the need to avoid loops. Quality Level is based on the clock's holdover performance.

Quality Levels (ql) names:

No.	Name	No.	Name
0	ql-stu	8	ql-ssu-b
1	ql-prs	9	ql-inv9
2	ql-prc	10	ql-eec2
3	ql-inv3	11	ql-eec1
4	ql-ssu-a	12	ql-smc
5	ql-inv5	13	ql-st3e
6	ql-inv6	14	ql-prov
7	ql-st2	15	ql-dnu

7.4.2 SyncE Configuration

SyncE is a licensed feature that requires a license for operation. Before configuring SyncE, verify that the SyncE license key is available and enable the license. Refer to *Upgrading the License Key* on page 129.

You can set the reference clock (ref-clock) per interface (host|eth0|eth1|eth2) using the following command:

```
set ref-clock <clk-if> [prio 1..255]
```

The **prio** attribute determines the priority of the reference clock source in the event that there is an equal ql among the interfaces. The priority can be any value from 1 to 255, where 1 is the highest priority. One entry, for host, is always present and cannot be deleted. This entry has the fixed priority 255 (the lowest priority). You cannot configure more than one interface with the same priority. If you configure Eth0, you must give it the highest priority.

For example:

```
set ref-clock eth2 5
```

To clear the reference clock settings, use the following command:

```
clear ref-clock {<clk-if-list> | all}
For example:clear ref-clock eth2
```

To display the reference clock settings, use the following command:

```
show ref-clock [{<clk-if-list> | all} [{info | prio}]]
```

For example:

```
Default>show ref-clock
ref-clock host prio                    : 255
ref-clock host status                  : active
ref-clock host ql-actual               : 11
```

```
ref-clock host ql-config              : 11
ref-clock host ql-mode                : disable
ref-clock host ssm-cvid               : none
```

where:

- status – active | backup 1/2/3 | down
- ql-actual – The current ql of the active interface.
- ql-config – 0 to 15. Sets the ql of the interface.
- ql mode – Can be Enabled (enable) or Disabled (disable).
- ssm-cvid – the C-VLAN ssm messages are sent over (default untagged)

When ql-mode is disabled, ESMC messages are ignored and the status is determined by the **`set ql-config`** attribute.

7.4.3 Typical SyncE Scenario

Figure 7-3 illustrates a typical SyncE Scenario in which:

- The local EtherHaul 1200 receives timing information on Eth1 from PRC (ql 2), and distributes it to all interfaces.
- The remote EtherHaul 1200 receives timing information and is locked on PRC, via Eth0 (RF).
- DNU (Do Not use, ql 15) is returned to the source in order to prevent timing loops.

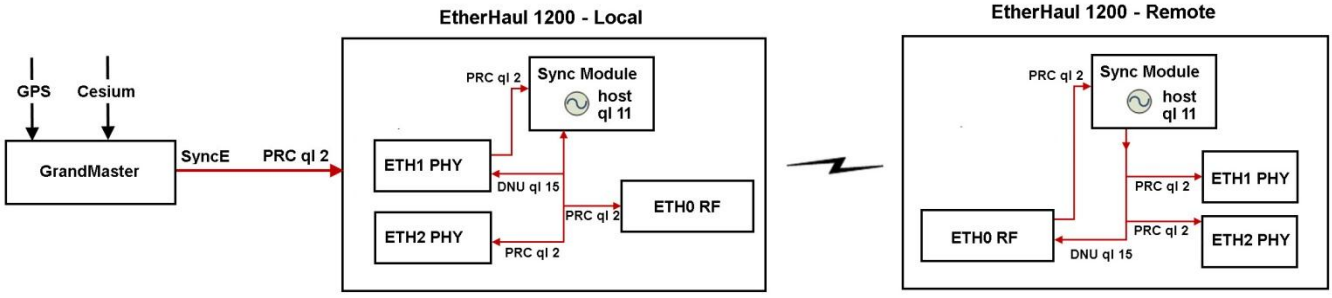


Figure 7-3 Typical SyncE Scenario

The configuration for this scenario is:

Local EtherHaul 1200

```
Default>show ref-clock
ref-clock host prio                   : 255
ref-clock host status                 : backup-1
ref-clock host ql-actual              : 11
```

```
ref-clock host ql-config            : 11
ref-clock host ql-mode              : disable
ref-clock host ssm-cvid             : none
ref-clock eth1 prio                 : 200
ref-clock eth1 status               : active
ref-clock eth1 ql-actual            : 2
ref-clock eth1 ql-config            : 2
ref-clock eth1 ql-mode              : disable
ref-clock eth1 ssm-cvid             : none
```

Remote EtherHaul 1200

```
Default>show ref-clock
ref-clock host prio                 : 255
ref-clock host status               : backup-1
ref-clock host ql-actual            : 11
ref-clock host ql-config            : 11
ref-clock host ql-mode              : disable
ref-clock host ssm-cvid             : none
ref-clock eth0 prio                 : 100
ref-clock eth0 status               : active
ref-clock eth0 ql-actual            : 2
ref-clock eth0 ql-config            : 14
ref-clock eth0 ql-mode              : enable
ref-clock eth0 ssm-cvid             : none
```

Figure 7-4 illustrates a SyncE scenario in which there is a holdover situation due to radio failure:

- The local EtherHaul 1200 receives timing information on Eth 1 from PRC (ql 2), and distributes it to all interfaces.
- There is no input on the remote EtherHaul 1200 because the radio link is down.
- The remote EtherHaul 1200 switches to holdover mode, maintaining the PRC it received previously and distributing it with its own ql (ql 11).

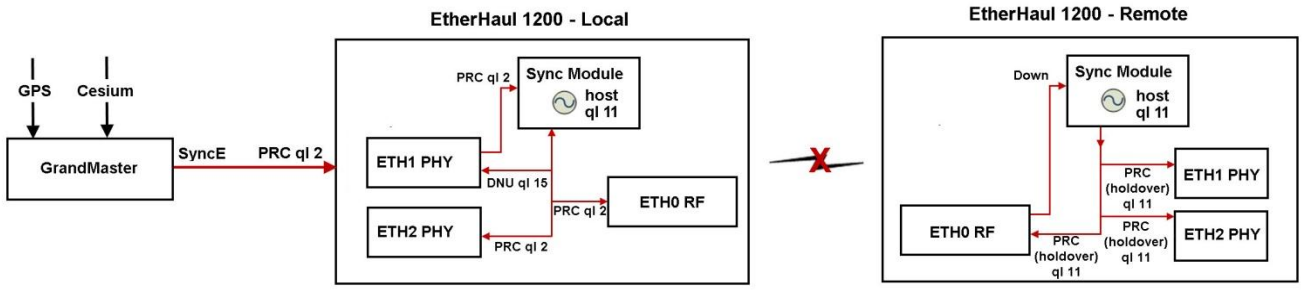


Figure 7-4 Typical SyncE Scenario – Holdover Due to Radio Failure

The configuration for this scenario is:

Local EtherHaul 1200

```
Default>show ref-clock

ref-clock host prio                  : 255
ref-clock host status                : backup-1
ref-clock host ql-actual             : 11
ref-clock host ql-config             : 11
ref-clock host ql-mode               : disable
ref-clock host ssm-cvid              : none

ref-clock eth1 prio                  : 200
ref-clock eth1 status                : active
ref-clock eth1 ql-actual             : 2
ref-clock eth1 ql-config             : 2
ref-clock eth1 ql-mode               : disable
ref-clock eth1 ssm-cvid              : none
```

Remote EtherHaul 1200

```
Default>show ref-clock

ref-clock host prio                  : 255
ref-clock host status                : active
ref-clock host ql-actual             : 11
ref-clock host ql-config             : 11
ref-clock host ql-mode               : disable
ref-clock host ssm-cvid              : none

ref-clock eth0 prio                  : 100
ref-clock eth0 status                : down
ref-clock eth0 ql-actual             : 15
ref-clock eth0 ql-config             : 14
ref-clock eth0 ql-mode               : enable
ref-clock eth0 ssm-cvid              : none
```

Figure 7-5 illustrates a SyncE scenario in which there is a holdover situation due to line failure:

- Because of the line failure, the local EtherHaul 1200 does not receive timing information from PRC. The local EtherHaul therefore switches to holdover mode, maintains the timing information it received previously over Eth1, and distributes this information with its own ql (ql 11).
- The remote EtherHaul 1200 receives and is locked on its Eth0 source and distributes timing information from this source to its interfaces.
- DNU (Do Not use, ql 15) is returned to the source in order to prevent timing loops.

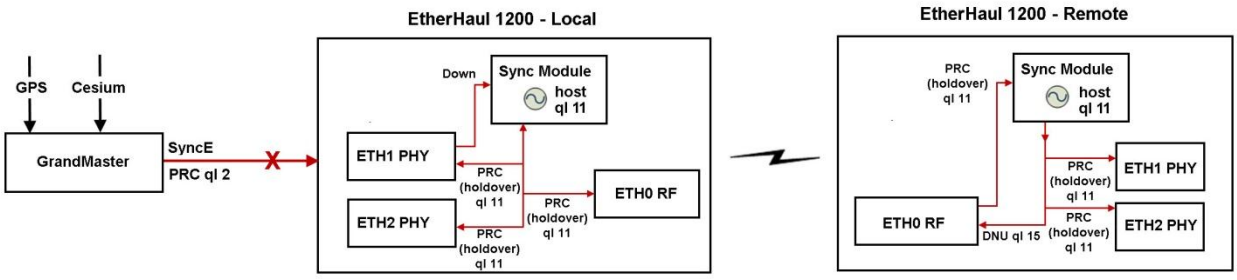


Figure 7-5 Typical SyncE Scenario – Holdover Due to Line Failure

The configuration for this scenario is:

Local EtherHaul 1200

```
Default>show ref-clock

ref-clock host prio                    : 255
ref-clock host status                  : active
ref-clock host ql-actual               : 11
ref-clock host ql-config               : 11
ref-clock host ql-mode                 : disable
ref-clock host ssm-cvid                : none

ref-clock eth2 prio                    : 200
ref-clock eth2 status                  : down
ref-clock eth2 ql-actual               : 15
ref-clock eth2 ql-config               : 2
ref-clock eth2 ql-mode                 : disable
ref-clock eth2 ssm-cvid                : none
```

Remote EtherHaul 1200

```
Default>show ref-clock
```

```
ref-clock host prio                    : 255
ref-clock host status                  : backup-1
ref-clock host ql-actual               : 11
ref-clock host ql-config               : 11
ref-clock host ql-mode                 : disable
ref-clock host ssm-cvid                : none

ref-clock eth0 prio                    : 100
ref-clock eth0 status                  : active
ref-clock eth0 ql-actual               : 11
ref-clock eth0 ql-config               : 14
ref-clock eth0 ql-mode                 : enable
ref-clock eth0 ssm-cvid                : none
```

7.4.4 SyncE Alarms

Event	Classification	Default Severity	Destination
Reference Clock Switch	Event	N/A	Trap (ref-clock switch), Log
Reception of QL EEC1 or Worse	Alarm indicating a previous element in the chain is in holdover or failed	Medium	Trap (generic alarm), Log, Active Alarm List
Reception of QL better than EEC1	Event	N/A	Trap (generic alarm), Log, Remove Reception of QL EEC1 and Worse from Active Alarm List.

7.5 Configuring Ethernet Ring Protection (ERP)

Ethernet Ring Protection (ERP) is a network resiliency protocol defined in ITU-T G.8032. The EtherHaul 1200 supports ERP G.8032v2, with backwards compatibility to previous versions. ERP support enables protection for any point of failure in the network. This means that network connectivity is maintained in the event that the Ethernet link, the radio link, or even the entire EtherHaul 1200 fails. This provides resiliency for both Ethernet-Ethernet rings that typically protect single site connectivity and Ethernet-RF rings that typically protect against RF network failure.

ERP is a relatively simple protocol that operates at the network level on the set of nodes that constitute the ring or set of rings. ERP monitors the Ethernet layer to discover and identify Signal Failure (SF) conditions, and prevents loops within the ring by blocking one of the links (either a pre-determined link or a failed link). ERP verifies at all times the ring is closed that frames will not be looped. This is accomplished by taking down a Ring protection Link (RPL) whenever there is no failure in the ring.

Using ERP, EtherHaul 1200 provides protection and recovery switching within 50 ms for typical rings. The ERP mechanism uses a very small percentage of total available bandwidth.

Figure 7-6 illustrates the basic ERP protection mechanism. In normal ring operation, the RPL is blocked. In a failure condition, the failed link is blocked, R-APS messages are sent from the nodes adjacent to the failed links in order to unblock the RPL, and an FDB flush is performed on all ring nodes as necessary.

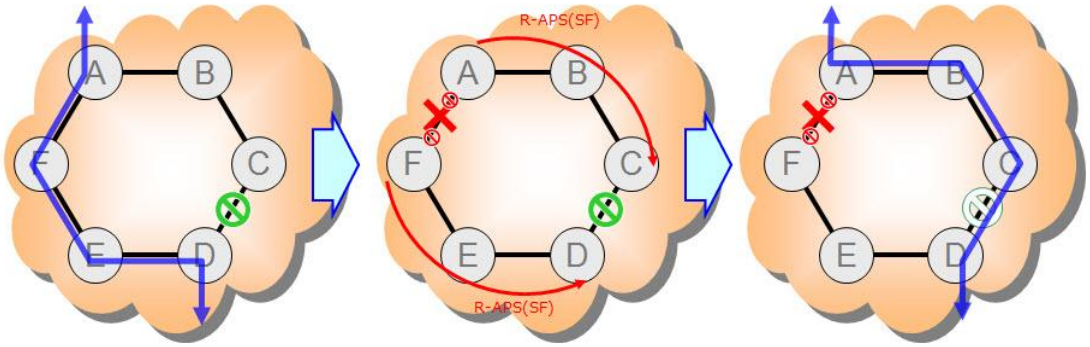


Figure 7-6 Basic ERP Protection Mechanism

7.5.1 Supported ERP Features

Among the ERP features supported by the EtherHaul 12000 are:

- Backwards compatibility to previous versions
- Revertive and non-revertive behavior
- Flush logic with the Node-ID and BPR (Blocked Port Reference) mechanism
- Administrative commands (manual and forced switch, clear)

- Ability to block RPL at both ends of the link (RPL owner and RPL neighbor)
- Multiple logical ERP instances over a given physical ring

7.5.2 ERP Ring Commands

To set a ring, use the following command:

```
Default>set ring
set ring <ring-index-list>  [ring-id <value>] [type <value>] [fdb-
id <value>] [role <value>] [cw-port <value>] [acw-port <value>]
[raps-md-level <value>] [raps-svid <value>][raps-cvid <value>]
[version <value>] [revertive <value>] [hold-off-timer <value>]
[guard-timer <value>] [wtb-timer <value>] [wtr-timer <value>]
[action <value>]
<ring-index-list>      : <list 1..16>
Default>
```

To display ring statistics, use the following command:

```
Default>show ring all statistics
ring 1 raps-tx          : 1443 <--- ACW-RPL (owner) originate RAPS
ring 1 raps-rx          : 1443 <----------- Received RAPS
ring 1 local-sf-cnt     : 0 (Signal Failure)
ring 1 remote-sf-cnt    : 2    (Signal Failure)
ring 1 nr-cnt           : 1 (No request)
ring 1 nr-rb-cnt        : 2 (No request Request blocked)
ring 1 elapsed-time     : 0000:02:00:24
```

To display ring events, use the following command:

```
Default>show log

Jul 5 14:27:21 sw cad: link down eth eth0
Jul 5 14:27:21 sw cad: modulation change qpsk 1 4 0.5
Jul 5 14:27:22 sw cad: local Signal Fail at 1 CW unblocked ACW blocked
Jul 5 14:30:43 sw cad: remote Signal Fail at 1 CW unblocked ACW blocked
Jul 5 14:30:43 sw cad: link up eth eth0
Jul 5 14:30:43 sw cad: modulation change qpsk 2 2 0.5
Jul 5 14:31:43 sw cad: ERP 1is ready Role none
```

7.5.3 ERP Administrative Commands

The EtherHaul 1200 provides two commands for blocking a particular ring port:

- **Forced Switch (FS)** – Can be used even if there is an existing condition. Multiple FS commands are supported per ring. FS commands can be used to enable immediate maintenance operations.
- **Manual Switch (MS)** – Not effective if there is an existing FS or SF condition. Also, MS commands are overridden by new FS and SF conditions. New MS commands are ignored.

Additionally, a Clear command can be used to cancel an existing FS or MS command on the ring port. The Clear command can also be used at an RPL owner node to trigger reversion.

The following examples illustrate how to use the administrative commands to control manual switching to the backup and block a particular ring port.

```
Left_Slave> set ring 3 action
cw-ms | acw-ms | cw-fs | acw-fs | clear
Left_Slave> set ring 3 action


Right_Master>set ring 3 action acw-fs
Set done: ring 3
Right_Master>show log
Aug  4 21:09:39 sw cad: local Forced switch at 200 CW unblocked
ACW blocked


Right_Master>show ring all state
ring 3 state                  : fs
Right_Master>


Right_Master>set ring 3 action clear
Set done: ring 3
Right_Master>show log
Aug  4 21:09:39 sw cad: local Forced switch at 200 CW unblocked
ACW blocked
Aug  4 21:10:46 sw cad: ERP 200is ready Role acw-rpl


Right_Master>
Right_Master>set ring 3 action acw-ms
Set done: ring 3
Right_Master>show log
Aug  4 21:43:18 sw cad: local Manual switch at 200 CW unblocked
ACW blocked
```

```
Right_Master>set ring 3 action clear
Set done: ring 3
Right_Master>show log
Aug  4 21:43:18 sw cad: local Manual switch at 200 CW unblocked
ACW blocked
Aug  4 21:44:36 sw cad: ERP 200is ready Role acw-rpl
```

7.5.4 ERP Timers

Different timers are used to determine the time of fault reports and switching in order to assure only necessary switching for permanent failures.

Timer	Description
Hold-off	Timer for ensuring stability of failure before triggering action to avoid reporting a fault in case of intermittent failure. 0..10000 mSec (in 100mSec steps)
Guard	Timer for protecting device against old R-APS messages. 10..2000 mSec (in 10mSec steps)
Wait-to-Block	Timer for delaying switching triggered by administrative command (FS/MS). 5000..7000 mSec (in 100mSec steps)
Wait-to-Restore	Timer for delaying revertive operation. 1..12 minutes

7.5.5 ERP Configuration Example

The following example illustrates an ERP configuration:

```
Left_Master>show ring
ring 1 ring-id          : 1
ring 1 type             : ring
ring 1 fdb-id           : 1
ring 1 role             : none
ring 1 cw-port          : eth1
ring 1 acw-port         : eth0
ring 1 raps-md-level    : 7
ring 1 raps-svid        : none
ring 1 raps-cvid        : 100
ring 1 version          : v2
ring 1 revertive        : yes
ring 1 hold-off-timer   : 0
ring 1 guard-timer      : 500
ring 1 wtb-timer        : 5500
ring 1 wtr-timer        : 1
```

```
Right_Slave_72>show ring
ring 1 ring-id          : 1
ring 1 type             : ring
ring 1 fdb-id           : 1
ring 1 role             : acw-rpl
ring 1 cw-port          : eth0
ring 1 acw-port         : eth1
ring 1 raps-md-level    : 7
ring 1 raps-svid        : none
ring 1 raps-cvid        : 100
ring 1 version          : v2
ring 1 revertive        : yes
ring 1 hold-off-time    : 0
ring 1 guard-timer      : 500
ring 1 wtb-timer        : 5500
ring 1 wtr-timer        : 1
```

```
ring 1 cw-status-data  : unblocked      ring 1 cw-status-data  : unblocked
ring 1 acw-status-data : unblocked      ring 1 acw-status-data : blocked
ring 1 cw-status-raps  : unblocked      ring 1 cw-status-raps  : unblocked
ring 1 acw-status-raps : unblocked      ring 1 acw-status-raps : blocked
ring 1 state           : idle           ring 1 state           : idle
ring 1 last-state-time : 2011.07.05     ring 1 last-state-time : 2011.06.27
ring 1 idle-percent    : 97.731606      ring 1 idle-percent    : 97.658112
ring 1 protect-percent : 1.249336       ring 1 protect-percent : 1.230652
ring 1 ms-percent      : 0.000000       ring 1 ms-percent      : 0.000000
ring 1 fs-percent      : 0.000000       ring 1 fs-percent      : 0.000000
ring 1 pending-percent : 1.019058       ring 1 pending-percent : 1.111240
ring 1 cw-node-id      : 00:00:00       ring 1 cw-node-id      : 00:00:00
ring 1 cw-bpr          : 0              ring 1 cw-bpr          : 0
ring 1 acw-node-id     : 00:24:a4       ring 1 acw-node-id     : 00:24:a4
ring 1 acw-bpr         : 0              ring 1 acw-bpr         : 0
```

The following example illustrates how to configure ERP on a ring:

```
Left_Slave>

# ring configuring
set ring 3 ring-id 200 type ring fdb-id 1 role none cw-port eth1
acw-port eth0 raps-cvid 100
set ring 3 raps-md-level 7 version v2 revertive yes hold-off-timer
0 guard-timer 500 wtb-timer 5500 wtr-timer 1

Left_Slave>

Right_Master>
# ring configuring
set ring 3 ring-id 200 type ring fdb-id 1 role acw-rpl cw-port
eth0 acw-port eth1 raps-cvid 100
set ring 3 raps-md-level 7 version v2 revertive yes hold-off-timer
0 guard-timer 500 wtb-timer 5500 wtr-timer 1

Right_Master>
```

8 Monitoring the System

This chapter explains how to monitor system events, status, and statistics, and includes the following topics:

- Viewing Active Alarms
- Viewing Alarm History and System Events
- Events configuration (masking)
- Viewing Radio Statistics
- Viewing VLAN Statistics
- Viewing Queue Statistics
- Viewing Ethernet Statistics

8.1 Viewing Active Alarms

You can display active alarms using the Web EMS or the CLI. For a detailed explanation of EtherHaul events and alarms, and instructions on how to use them in diagnosing EtherHaul system problems, refer to *EtherHaul Diagnostics* on page 140.

To display all active alarms using the Web EMS, click **Events** on the Web EMS Main screen. Active alarms appear in the Alarms section of the Events screen, including the date and time the alarm occurred.

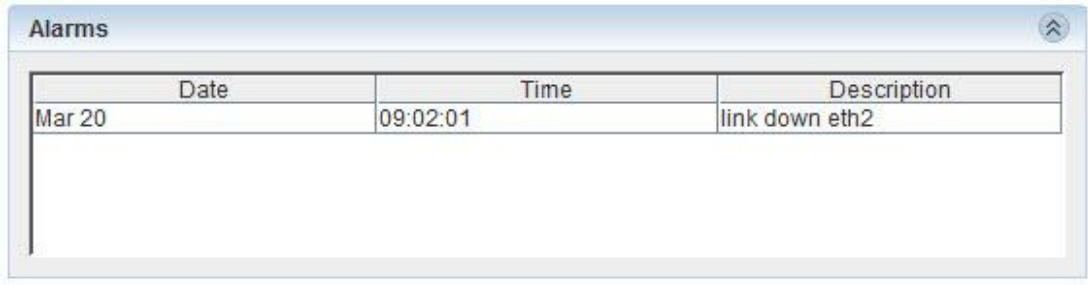


Figure 8-1 Web EMS Events Screen – Alarms Section

To display all active alarms using the CLI, use the **`show alarms`** command. All active alarms appear, including the date and time the alarm occurred.

```
2010.7.10   9:45:21   temperature high
2010.7.10   9:50:13   link down eth0
```

8.2 Viewing Alarm History and System Events

You can display a log of alarms and system events using the Web EMS or the CLI. For a detailed explanation of EtherHaul events and alarms, and instructions on how to use them in diagnosing EtherHaul system problems, refer to *EtherHaul Diagnostics* on page 140.

To display a log of alarms and system events using the Web EMS, click **Events** on the Web EMS Main screen. A log of alarms and system events appears in the Logs section of the Events screen, including the date and time the alarm or event occurred.

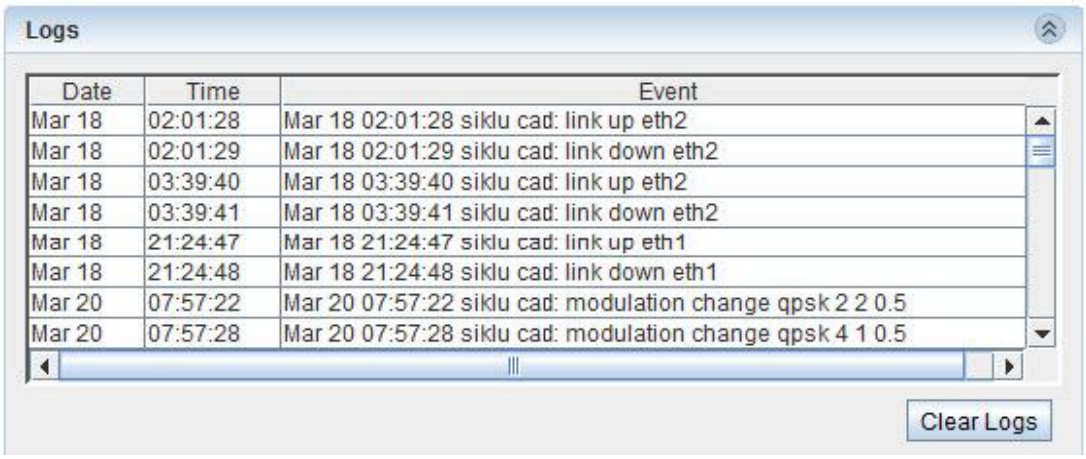


Figure 8-2 Web EMS Events Screen – Logs Section

To display a log of alarms and system events using the CLI, use the **`show log`** command. A log of alarms and system events appears, including the date and time the alarm or event occurred.

```
2010.7.10   9:35:11   temperature high
2010.7.10   9:36:13   link down eth0
2010.7.10   9:36:49   link up eth0
2010.7.10   9:40:04   temperature normal
2010.7.10   9:45:21   temperature high
2010.7.10   9:50:13   link down eth0
```

To clear all system logs, use the **`clear log`** command.

8.3 Events Configuration (Masking)

The EtherHaul supports masking of individual/group alarms. In case alarm is masked, it will not be displayed in the Active Alarms and Event Log and trap will not be sent.

By default, none of the alarms is masked.

To mask an alarm, set the event-cfg mask value to yes.

```
set event-cfg <event-cfg-id-list>  [mask <value>]
```

Use the following command to view the events configuration:

```
Support-14>show event-cfg
event-cfg link-down                    mask                    : no
event-cfg temperature-high             mask                    : no
event-cfg cfm-fault-alarm              mask                    : no
event-cfg synthesizer-unlock           mask                    : no
event-cfg poe-status-low               mask                    : no
event-cfg loopback-enabled             mask                    : no
event-cfg tx-mute-enabled              mask                    : no
event-cfg ql-eec1-or-worse             mask                    : no
event-cfg cold-start                   mask                    : no
event-cfg modulation-change            mask                    : no
event-cfg sfp-in                       mask                    : no
event-cfg ref-clock-switch             mask                    : no
event-cfg erp-ready                    mask                    : no
event-cfg erp-forced-switch            mask                    : no
event-cfg erp-manual-switch            mask                    : no
event-cfg erp-signal-fail              mask                    : no
event-cfg erp-invalid-version          mask                    : no
event-cfg rx-ql-eec1                   mask                    : no
event-cfg poe-incompatible             mask                    : no
```

8.4 Viewing Radio Statistics

You can display radio statistics using the Web EMS or the CLI. Radio statistic counters can be used to identify radio errors. When there are no errors on **In Errored Octets**, **In Errored Packets**, and **In Lost Packets** in the current radio statistics, this indicates that the radio link is operating without errors.

Radio errors observed in these indicators do not necessarily indicate frame-loss on the Ethernet service. The ARQ (Automatic Repeat reQuest) algorithm uses selective repeat (retransmission) to eliminate radio BER.

The **arq-in-loss** and **arq-out-loss** indicate frame-loss over the radio that can be noticed by the Ethernet service.

8.4.1 Viewing Radio Statistics Using the Web EMS

To display radio statistics using the Web EMS, click **Radio** on the Web EMS Main screen and click the RF Statistics section.

The RF Statistics section of the Radio screen includes the following two tabs:

- **Current** – Real time statistics counters since the last time the RF statistic counters were cleared.

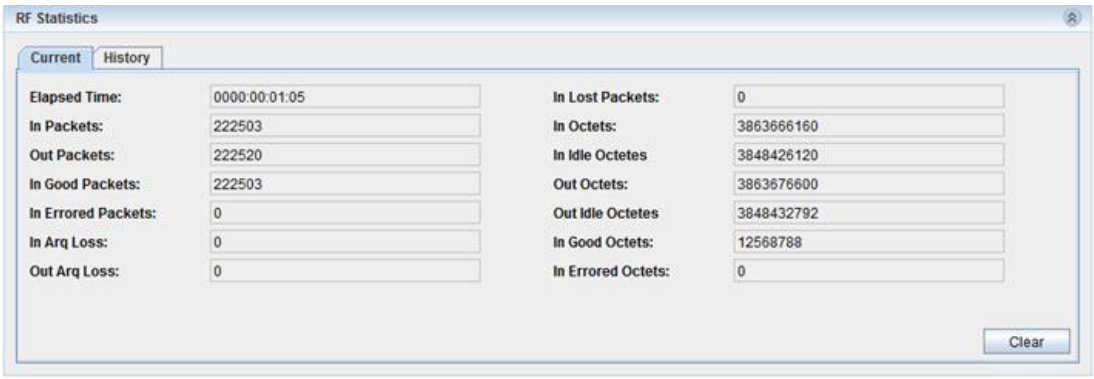
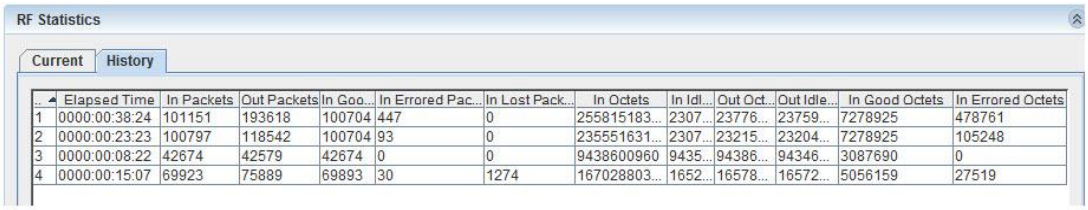


Figure 8-3 RF Statistics Screen – Current Tab

- **History** – Displays 96 intervals of 15 minutes (total 24 hours) of the statistics counters.



	Elapsed Time	In Packets	Out Packets	In Goo...	In Errored Pac...	In Lost Pack...	In Octets	In Idl...	Out Oct...	Out Idle...	In Good Octets	In Errored Octets
1	0000:00:38:24	101151	193618	100704	447	0	255815183...	2307...	23776...	23759...	7278925	478761
2	0000:00:23:23	100797	118542	100704	93	0	235551631...	2307...	23215...	23204...	7278925	105248
3	0000:00:08:22	42674	42579	42674	0	0	9438600960	9435...	94386...	94346...	3087690	0
4	0000:00:15:07	69923	75889	69893	30	1274	167028803...	1652...	16578...	16572...	5056159	27519

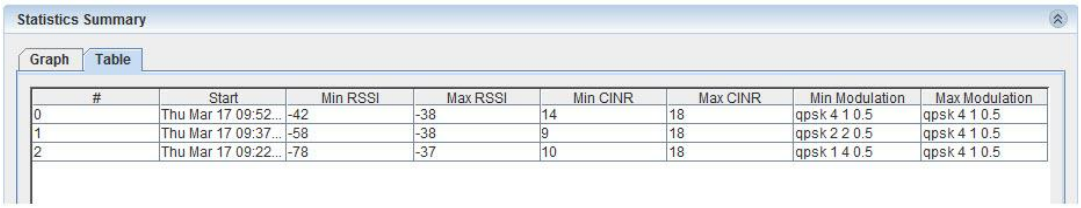
Figure 8-4 RF Statistics Screen – History Tab

For a description of the radio statistics, refer to *Table 11-6*.

To clear the statistic counters, click **Clear** on the Current tab.

8.4.2 Viewing a Statistics Summary Using the Web EMS

You can display a summary of the ODU's radio statistics in graph or table format using the Web EMS. To display a summary of the ODU's radio statistics, click **Radio** on the Web EMS Main screen and click the Statistics Summary section.



#	Start	Min RSSI	Max RSSI	Min CINR	Max CINR	Min Modulation	Max Modulation
0	Thu Mar 17 09:52...	-42	-38	14	18	qpsk 4 1 0.5	qpsk 4 1 0.5
1	Thu Mar 17 09:37...	-58	-38	9	18	qpsk 2 2 0.5	qpsk 4 1 0.5
2	Thu Mar 17 09:22...	-78	-37	10	18	qpsk 1 4 0.5	qpsk 4 1 0.5

Figure 8-5 Web EMS – Statistics Summary Table

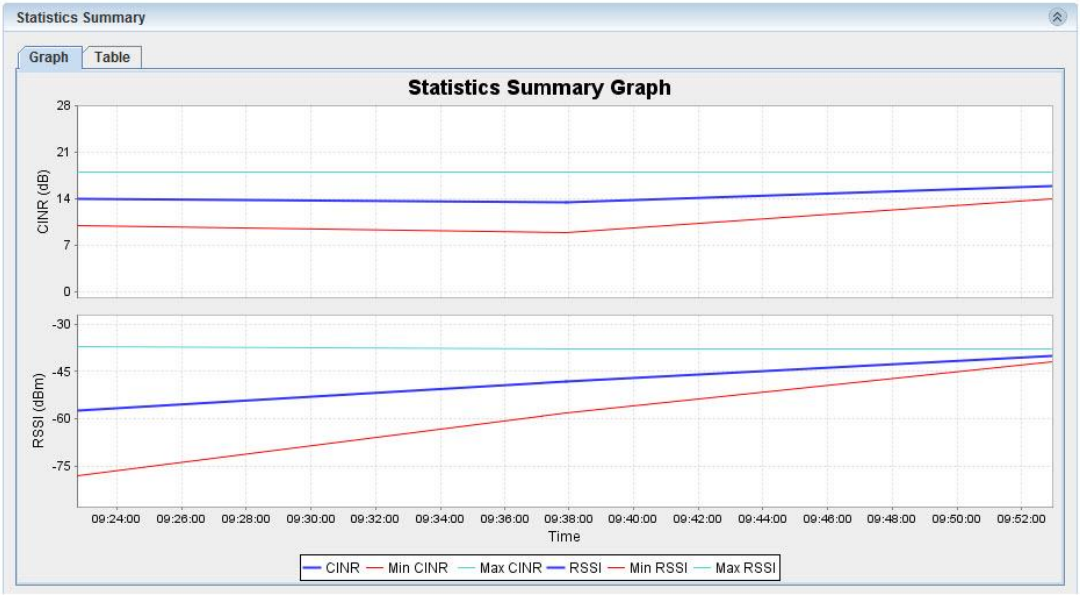


Figure 8-6 Web EMS – Statistics Summary Graph

8.4.3 Viewing Radio Statistics Using the CLI

Use the **`show rf statistics`** command to display radio statistics using the CLI. Statistics are gathered for 96 intervals of 15 minutes (total 24 hours), recording the minimum and maximum values per interval.

```
Local_Site>show rf statistics

rf in-octets              : 32535265564
rf in-idle-octets         : 29775780985
rf in-good-octets         : 9370230
rf in-errored-octets      : 0
rf out-octets             : 30552267600
rf out-idle-octets        : 30531707551
rf in-pkts                : 129957
rf in-good-pkts           : 129452
rf in-errored-pkts        : 0
rf in-lost-pkts           : 0
rf out-pkts               : 231519
rf min-cinr               : 13
rf max-cinr               : 18
rf min-rssi               : -56
rf max-rssi               : -33
rf min-modulation         : qpsk 2 2 0.5
rf max-modulation         : qpsk 4 1 0.5
rf arq-in-loss            : 0
rf arq-out-loss           : 0
rf elapsed-time           : 0000:00:45:51
```

To clear the statistic counters using the CLI, use the **`clear rf statistics`** command.

Table 11-6 on page 181 lists and describes the radio statistics. *Table 11-7* on page 181 lists the index pointers to the statistics history of the RF object.

8.4.4 Viewing Radio Statistics Summary Using the CLI

Use the **`show rf statistics-summary`** command to display a summary of radio statistics using the CLI. Statistics are gathered for 96 intervals of 15 minutes (total 24 hours), recording the minimum and maximum values per interval. Statistics are gathered for 96 intervals of 15 minutes (total 24 hours), recording the minimum and maximum values per interval.

```
Local_Site>show rf statistics-summary 0 95

#  start                 min-   max-  min-  max   min-           max-          valid
                         rssi   rssi  cinr  cinr  modulalation   modulation

0  2011.03.17  10:22:58  -76    -33   15    18    qpsk 1 4 0.5   qpsk 4 1 0.5  unknown
1  2011.03.17  10:07:57  -76    -24   -128  -128  qpsk 1 4 0.5   qpsk 1 4 0.5  unknown
2  2011.03.17  09:52:56  -76    -10   -128  -128  qpsk 1 4 0.5   qpsk 1 4 0.5  unknown
3  2011.03.17  09:37:55  -76    -38   9     18    qpsk 2 2 0.5   qpsk 4 1 0.5  unknown
4  2011.03.17  09:22:48  -76    -37   10    18    qpsk 1 4 0.5   qpsk 4 1 0.5  unknown
```

8.5 Viewing VLAN Statistics

You can display VLAN statistics using the Web EMS or the CLI. To display VLAN statistics using the Web EMS, click **Bridge** on the WEB EMS Main screen and click the Statistics section.

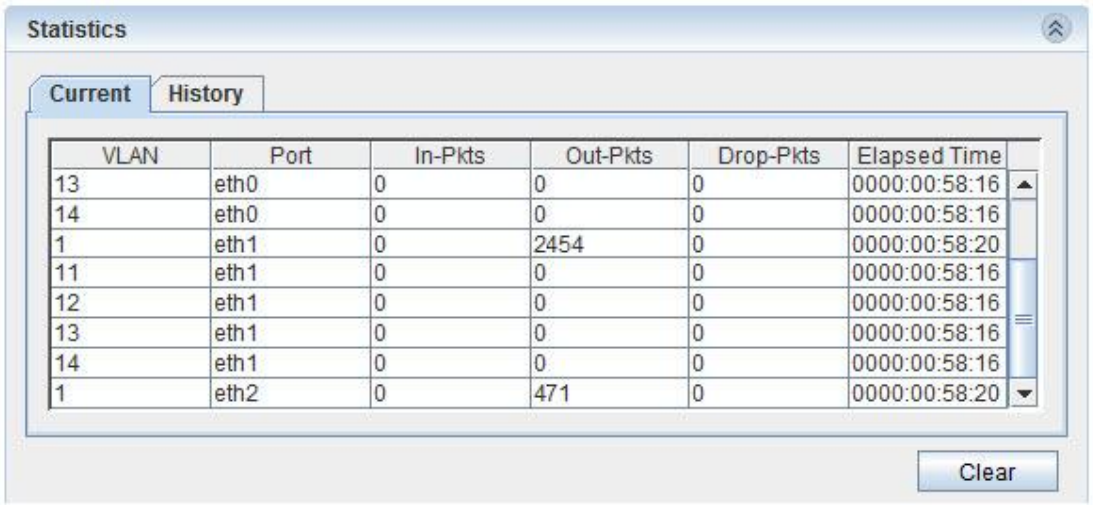


Figure 8-7 Web EMS – Current VLAN Statistics

For information on displaying VLAN statistics using the CLI, and a description of the VLAN attributes, refer to *Displaying VLAN Details* on page 68 and *VLAN Table Attributes* on page 68.

8.6 Viewing Queue Statistics

You can use the CLI to display statistics for outgoing queues and incoming queues.

8.6.1 Viewing Outgoing Queue Statistics

Use the following command to display statistics for outgoing queues:

```
show out-queue {{eth0, eth1, eth2, rf} | all} {1..8 | all}
statistics
```

Counters of all outgoing queues appear, as follows:

```
Default>> show out-queue eth1 all statistics
interface   qid   tx     drop   elapsed-time
eth1        1     1321   3      0001:02:15:09
eth1        2     1543   1      0001:02:15:09
eth1        3     1435   0      0001:02:15:09
eth1        4     2345   0      0001:02:15:09
eth1        5     4563   0      0001:02:15:09
eth1        6     4563   0      0001:02:15:09
eth1        7     6547   9      0001:02:15:09
eth1        8     1256   0      0001:02:15:09
```

Note that for **rf** there are only four queues. Therefore, only numbers from 1 to 4 (or **all**) are valid for the second ID. If **all** is specified, only four queues are displayed.

Use the following command to clear the outgoing queue statistics:

```
clear out-queue {{eth0, eth1, eth2, rf} | all} {1..8 | all}
statistics
```

Table 11-24 on page 208 lists and describes the outgoing queue attributes.

8.6.2 Incoming Queues Commands

Currently Incoming Queues are defined only for rf. However, the design should take into account the possibility that the other interfaces will also have incoming queues and their statistics may be different from rf.

Use the following command to display statistics for incoming queues:

```
show in-queue {rf | all} {1..4 | all} statistics
```

Counters of all incoming queues appear, as follows:

```
Interface     qid    good   error  lost   elapsed-time
```

Note that for **rf** there are only four queues. Therefore, only numbers from 1 to 4 (or **all**) are valid for the second ID. If **all** is specified, only four queues are displayed.

Use the following command to clear the incoming queue statistics:

```
clear in-queue {rf | all} {1..4 | all} statistics
```

Table 11-25 on page 208 lists and describes the incoming queue attributes.

8.7 Viewing Ethernet Statistics

You can display statistics on EtherHaul's Ethernet interfaces using the Web EMS or the CLI.

8.7.1 Viewing Ethernet Statistics Using the Web EMS

To display Ethernet statistics using the Web EMS, click the icon of the interface for which you want to view statistics on the EMS Web Main screen (*Figure 3-11*), then click the Statistics section of the Interfaces screen.

The Statistics section includes the following tabs:

- **Current** – Real time statistics counters since the last time the Ethernet statistic counters were cleared.

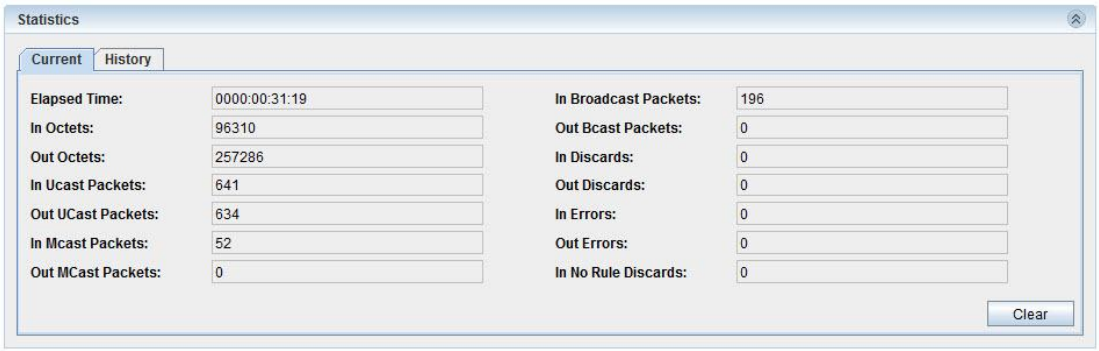


Figure 8-8 Statistics Screen – Current Tab

- **History** – Displays 96 intervals of 15 minutes (total 24 hours) of the statistics counters.

To clear the statistic counters, click **Clear** on the Current tab.

Table 11-21 on page 204 lists and describes the Ethernet statistics.

8.7.2 Viewing Ethernet Statistics Using the CLI

To display Ethernet statistics using the Web EMS, use the following command:

```
show  eth <ext-bridge-port-list> statistics
```

Table 11-21 on page 204 lists and describes the Ethernet statistics.

9 Performing System Administration

This chapter describes procedures that involve system administration rather than the network itself, and includes the following topics:

- Configuring Encryption
- Working with Configuration Files
- Configuring Users
- Upgrading the ODU Software
- Monitoring CLI Sessions
- Viewing System Inventory
- Upgrading the License Key
- Performing Address Translation
- Siklu File System (SFS)
- Command Line Scripts
- Configuring NTP
- Viewing User Activity Log
- Managing SNMP

9.1 Configuring Encryption

The EtherHaul supports 128bit and 256bit AES encryption with Static key. This means that the encryption key (32/64 characters long) must be inserted manually into both ends of the link. If there is an encryption mismatch, traffic will not go over the link.

The encryption license must be enabled in order to configure encryption. The EtherHaul system supports AES encryption protocol, which is capable of delivering encrypted transmission over the link.

9.1.1 Loading Encryption License Key

Encryption is a licensed feature that requires a license for operation. Before setting the encryption, verify that the encryption license key is available. Refer to *Upgrading the License Key* on page 129.

9.1.2 Setting up a Static Key

Use the following commands to set up a Static Key:

```
Default > set encryption encryption static-key static-key
0123456789abcdef0123456789abcdef
Set done: encryption

The string of either 32 (128bits) or 64 (256bits) hexadecimal
digits
```

9.2 Working with Configuration Files

The EtherHaul system supports the use of stored network configurations. Generally, a stored configuration is automatically loaded on system startup or following a system reset.

9.2.1 Saving Configurations

A stored configuration is created by saving the currently active (running) configuration as the default configuration.

Note:

The running configuration EtherHaul is not automatically saved in non-volatile RAM.

If a system reset occurs before a particular configuration is saved, the EtherHaul will perform a startup using the current stored configuration, or if none exists, the factory default configuration.

To save the running configuration, use the following CLI command or click **Save Configuration** on the Web EMS main screen:

```
Default>>copy running-configuration startup-configuration
running-configuration copied to startup-configuration
```

9.2.2 Viewing Configurations

You can display either the running or the default EtherHaul network configuration with the following command:

```
Default>copy running-configuration display
Default>copy startup-configuration display
```

9.2.3 Restoring the Default Configuration

In order to restore the default configuration, the startup-configuration must be removed and the ODU rebooted.

You can clear the startup configuration with the **`clear startup-configuration`** command or click **Restore to Default** in the Commands section of the Advanced Settings screen of the Web EMS:

```
Default>clear startup-configuration
startup-configuration cleared
```

On the next startup after this command is executed, the EtherHaul system will revert to the hard-coded factory default parameters.

Pressing the ODU's 'reset' push-button on the AUX port for more than 5 seconds will reset the ODU and restore the default configuration.

9.2.4 Rollback Operations

You can roll back system configurations. This is a safety measure to prevent unwanted system changes in the event that a loss of communication occurs while performing configuration activities. The Rollback timeout function reloads the saved startup configuration in the event that no command is entered within a predefined timeout period.

A Rollback timeout is especially recommended when configuring remote elements that are being managed over the link.

To specify the Rollback timeout period, use the following command:

`set rollback timeout <duration-in-seconds>`

When Rollback is used, a timer will run (and will restart) whenever a CLI command is entered. In the event that no CLI command is entered within the timeout period, the system automatically resets and wakes up with the saved startup configuration.

Note that the rollback timer resets to zero after each new CLI command. The rollback timer expires when it reaches the value specified by `<duration-in-seconds>`.

To cancel a rollback, use the **`clear rollback`** command. This command cancels the Rollback function. This means that the System will not automatically roll back to any previous configuration.

You can enter the **`clear rollback`** command any time before the end of a Rollback timeout period in order to cancel a rollback timeout.

Rollback can also be controlled from the Web-EMS main screen.

9.3 Configuring Users

The EtherHaul system supports multiple users, and enables you to choose from a selection of user types with different access privileges.

To add a new user:

1. Connect to the ODU. Refer to *Connecting to the ODU Using the Web EMS* on page 36.
2. In the Web EMS Main screen, click **Advanced Settings** and click the Users section.

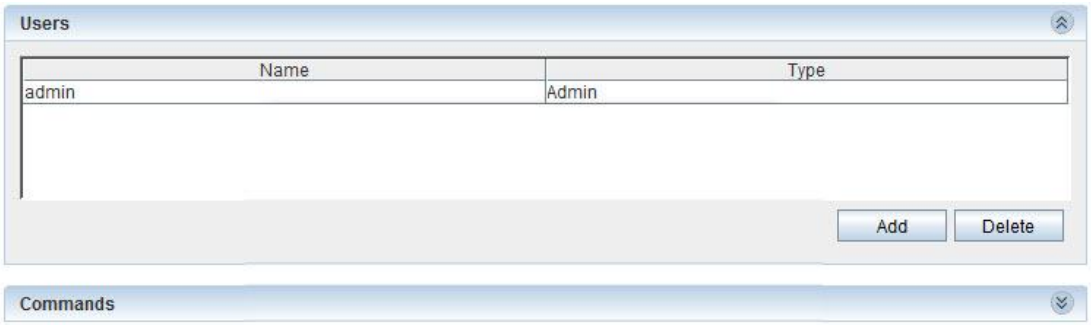


Figure 9-1 Web EMS Advanced Settings Screen – Users Section

3. Click **Add**. The Add User window is displayed.

Figure 9-2 Web EMS – Add Users Screen

4. In the **User Name** field, enter the user name.
5. In the **Password** field, enter a password for the user.
6. In the **Type** field, select from a list of user types. The user type defines the user's access privileges.
   - **User** – Read-only access, but cannot view user names, passwords, and other security settings.
   - **Tech** – Read-only access to configuration settings. Can clear statistics, alarms, and log lists, and run diagnostics.
   - **Super** – Read-write access, but no access to user names, passwords, and other security settings.
   - **Admin** – Full access except for access to debugging tools. A default admin user is built into the system, with the user name **`admin`** and the password **`admin`**. Only one admin type user can be defined.
7. Click **Apply** to save the changes.

9.4 Upgrading the ODU Software

The EtherHaul system supports switching in real time between two software versions. EtherHaul maintains an active (running) and a standby software version simultaneously. This enables you to upgrade the software with minimal interruption of service.

An external FTP server is required for software download. When you download a software version, the downloaded version replaces the standby version.

Figure 9-3 shows the relationship between flash banks and software images in the EtherHaul system.

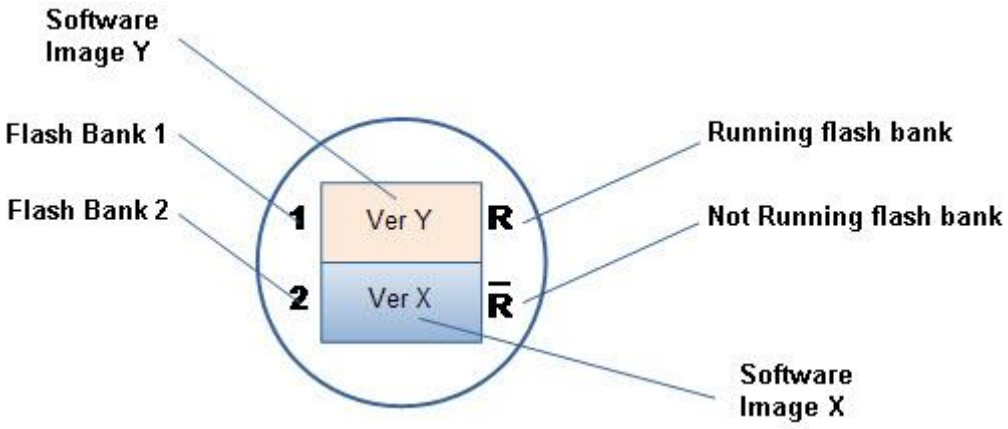


Figure 9-3 Flash Banks and Software Images

You can download and activate a new software version using either the Web EMS or the CLI.

9.4.1 Upgrading the ODU Software Using the Web EMS

To upgrade the ODU software:

1. Connect to the ODU. Refer to *Connecting to the ODU Using the Web EMS* on page 36.
2. From the Web EMS Main screen, click **Advanced Settings** and click the Software section of the Advanced Settings screen. The Software section displays both the active and the standby software versions. The software version is followed by the creation date and time of the version. The first digit of the version number represents the major version number, the second digit represents the minor version number, the third digit represents the SVN revision, and the fourth digit represents the version build number.

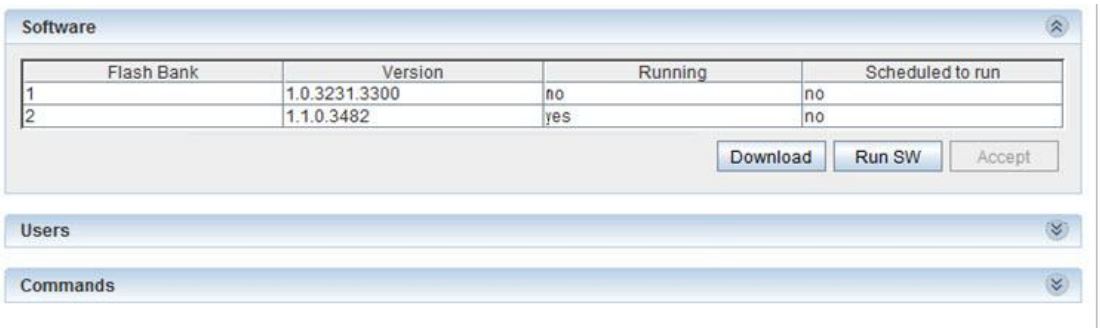


Figure 9-4 Web EMS – Software Section

3. Click **Download**. The Software Download window is displayed.

Figure 9-5 Web EMS – Software Download Window

4. In the Software Download window, enter the following details for the FTP server from which you are downloading the software:
   - **Username**
   - **Password**
   - **IP address**

- **File name –** The file name of the software version you want to download.

5. Click **Apply** to download the software. The Software Download window closes, and the software is downloaded to the standby flash bank of the ODU.
6. Once the software has been downloaded, click **Run SW** in the Software screen. The downloaded software version is activated.

9.4.2 Upgrading the ODU Software Using the CLI

You can use the **`show sw`** command to display the active and standby software versions.

```
Flash Bank  Version                    Running     Scheduled to run
1           0.2.1.0 2010-05-18 15:58:13    yes          no
2           0.2.0.1865 2010-05-20 14:59:57  no          no
```

The software version is followed by the creation date and time of the version. The first digit of the version number represents the major version number, the second digit represents the minor version number, the third digit represents the SVN revision, and the fourth digit represents the version build number.

To upgrade the software:

1. Use the command **`copy sw <from-url>`** to copy a specified software version to the ODU, where **`<from-url>`** represents the URL of the FTP server which you are downloading the new software version. The software version image is copied from the specified URL to the standby flash bank of the ODU.
2. Use the following command to reset the system with the formerly standby software version as the active version:

```
run sw  {immediate | next-rst}
        {<accept-timeout-sec> | no-timeout}
```

   - If **`immediate`** is specified as the first parameter on the command line, then a reset is performed immediately. This is the default value.
   - If **`next-rst`** is specified as the first parameter on the command line, then the next system reset that occurs (for whatever reason) will cause the system to wake up with the software version stored in the standby flash bank.
   - If **`<accept-timeout-sec>`** is specified as the second parameter on the command line, then this duration in seconds is used as the safety timeout period in order to manually enter the command **`accept sw`**.
   - If **`no-timeout`** is specified as the second parameter on the command line, then the command **`accept sw`** is not expected and the standby software version automatically becomes the active software version.

3. If the system reactivates after reset with a software version stored in the standby flash bank, use the **`accept sw`** command to make the standby version the active version. If you do not execute the **`accept sw`** command before the accept-timeout-sec period specified in Step 2 ends, the system resets and wakes up running the software version image stored in the active flash bank. Effectively, this means that the software version rolls back. Note that such a rollback also occurs if a reset occurs (for whatever reason) before the **`accept sw`** command is entered.

9.5 Monitoring CLI Sessions

Use the following command to display active CLI sessions:

```
show loginsession [{my | all}]
```

In response, the software displays the following:

```
Session ID     Session Time
xx             dddd:hh:mm:ss
yy             dddd:hh:mm:ss
```

Where:

xx or **yy** is a two-digit integer from 00 to 99, and

dddd:hh:mm:ss – days(0000 – 9999):hours(00 – 24):minutes(00 – 60):seconds(00 – 60)

To display only the CLI session of the user entering the command, use the **`show loginsession my`** command.

To display all active CLI session, use the **`show loginsession all`** command.

9.6 Viewing System Inventory

You can display a system inventory list using the Web EMS or the CLI.

- *Table 11-2* on page 168 lists and describes the physical inventory attributes. All of these attributes are read-only.
- For a list and description of the system inventory entities and their relationships, refer to *Physical Inventory Entities* on page 174.
- The EtherHaul serial number and product type can be viewed under the “chassis” class in the Web EMS or can be accessed with the following CLI command:

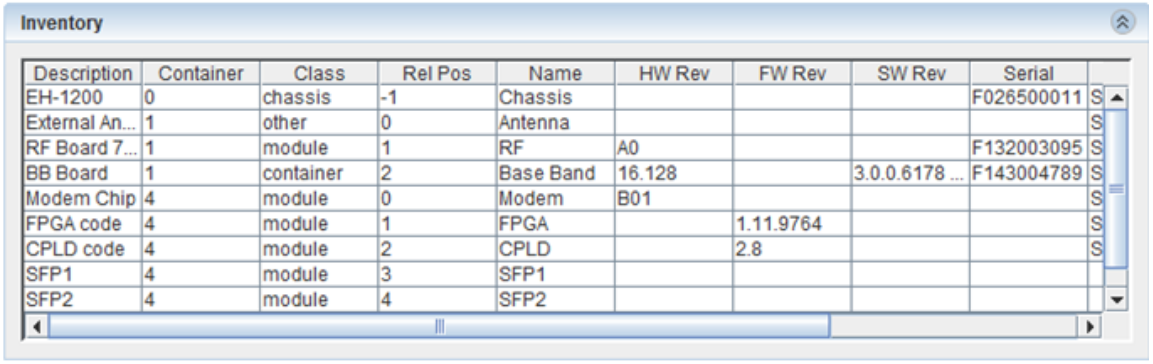
```
default>show inventory 1

inventory 1 desc                    : EH-1200
inventory 1 cont-in                 : 0
inventory 1 class                   : chassis
inventory 1 rel-pos                 : -1
inventory 1 name                    : Chassis
```

```
inventory 1 hw-rev                  :
inventory 1 fw-rev                  :
inventory 1 sw-rev                  :
inventory 1 serial                  : F026500011
inventory 1 mfg-name                : Siklu
inventory 1 model-name              : EH-1200-ODU-2ft
inventory 1 fru                     : true
```

9.6.1 Viewing System Inventory Using the Web EMS

To view the ODU's inventory list using the Web EMS:

1. In the Web EMS Main screen, click **System**. The System screen is displayed.
2. Click the Inventory section of the System screen, which lists parts, sub-parts, and their details.



Description	Container	Class	Rel Pos	Name	HW Rev	FW Rev	SW Rev	Serial	
EH-1200	0	chassis	-1	Chassis				F026500011	S
External An...	1	other	0	Antenna					S
RF Board 7...	1	module	1	RF	A0			F132003095	S
BB Board	1	container	2	Base Band	16.128		3.0.0.6178 ...	F143004789	S
Modem Chip	4	module	0	Modem	B01				S
FPGA code	4	module	1	FPGA		1.11.9764			S
CPLD code	4	module	2	CPLD		2.8			S
SFP1	4	module	3	SFP1					
SFP2	4	module	4	SFP2					

Figure 9-6 System Screen – Inventory Section

9.6.2 Viewing System Inventory Using the CLI

To display a list and description of the system inventory, use the following command:

```
show  inventory [{<ph-idx-range> | all}
   [{desc | cont-in | class | rel-pos | name | hw-rev
   | fw-rev | sw-rev | serial | mfg-name | model-name | fru
   | last-change | info}]]
```

9.7 Upgrading the License Key

You can order the following EtherHaul 1200 software licenses (capacity steps and feature availability depends on the platform):

- Data rate (Capacity)
- Layer 2 networking capabilities –OAM, Resiliency.
- Synchronization – Synchronous Ethernet (ITU-T G.8261)
- Encryption

Upgrading a license requires loading (using FTP) a license key that is generated by Siklu based on your EtherHaul 1200 serial number.

```
Default>copy license ://<ftp_user>:<ftp_password>@<FTP server IP
address>/<license_file_name>
…
finished
```

Once you have loaded the license file to the ODU, you can activate the license.

- To view the available licenses according to the loaded license file ("Permission") and the current configuration ("Status"):

```
default>show license

license  oam              status     :  enable
license  oam              permission :  enable

license  synce            status     :  enable
license  synce            permission :  enable

license  encryption       status     :  enable
license  encryption       permission :  enable

license  data-rate        status     :  500
license  data-rate        permission :  1000

license  resiliency       status     :  disable
license  resiliency       permission :  disable
```

- to activate license:

```
Default>set license data-rate status 1000

Set done: license
```

9.8 Performing Address Translation

The ARP table is used to map between IP addresses and physical addresses. Use the following command to create and modify entries in the ARP table

```
set   arp
      [ip-address <mac-address>]
```

If the ARP entry does not already exist, the **set arp** command creates it and assigns the attributes specified. Upon creation, in the event that the interface address or the default router address is not specified, the entry is created with the default value that has been defined for the VLAN.

If the ARP entry already exists, then the **set arp** command replaces the attributes that are currently defined for the entry with the value specified in the command.

Use the following command to display ARP entries:

show arp [<ip-address>]

Use the following command to delete ARP entries and clear their associated statistics:

clear arp [<ip-address>]

Table 11-35 on page 219 lists and describes the ARP table attributes.

9.9 Siklu File System (SFS)

9.9.1 Understanding SFS

With SFS, all files can be listed and classified (binary, text file, and so on), including files on remote servers.

SFS minimizes the required prompting for many commands, such as the **copy** CLI command. You can enter all of the required information in the command line, rather than waiting for the system to prompt you. For example, to copy a file to an FTP server, you can specify the specific location on the device of the source file, the specific location of the destination file on the FTP server, and the username and password to use when connecting to the FTP server. Alternatively, you can enter the minimal form of the command.

SFS enables you to navigate to different directories and list the files in a directory.

9.9.2 Specifying Files Using URLs

9.9.2.1 Specifying Files on Network Servers

To specify a file on a network server, use one of the following forms:

ftp://username:password@Location/subdirectory/filename

The *location* can be an IP address or a host name.

The file path (directory and filename) is specified relative to the directory used for file transfers. For example, on UNIX file servers, FTP paths start in the home directory associated with the username.

The following example specifies the file named **mill-config** on the server named **enterprise.siklu.com**. The device uses the username **liberty** and the password **secret** to access this server via FTP.

Since there is currently no DNS, the location is specified as IP Address in the dotted notation.

ftp://liberty:secret@127.23.46.17/mill-config

9.9.2.2 Specifying Local Files

Use the **[prefix:[directory/]]filename** syntax to specify a file located on the device specified by prefix. For example, **flash:backup-config** specifies the file named **backup-config** in the **configs** directory of Flash memory. Some devices do not support directories.

9.9.2.3 Supported Storage Devices

Table 9-1 lists and describes the currently supported file storage devices.

Table 9-1 Supported Support Devices

Device Identification	Description
ftp	FTP server (external server)
flash	Local flash memory (linux shell /var/siklu/etc).
eprom	RF module ROM. No directories.

The **/scripts directory** resides under flash (**flash:scripts**).

9.9.3 File System Commands

9.9.3.1 Command List

Table 9-2 lists and describes the file system commands.

Table 9-2 File System Commands

Command	Purpose
dir <device:>	Lists files stored at the device; works only for flash and eprom; available to all types of users.
copy <from-url> <to-url>	Copy file; root, admin and super are allowed to copy from any device to any device; Tech and user are allowed to copy files from the local devices (namely: flash, ram, eprom) to the network devices (namely ftp) but not vice versa; they are not allowed to copy files between the local devices.
del <url>	works only for flash; available only for root, admin and super.

9.9.3.2 Displaying the List of Stored Files

The command **dir** displays the list of the stored files in table format:

<Num> <Size> <date> <time> <name>

Where:

Num=The sequential number

size=File size in bytes

data=Storage data

time=Storage time

name-File name

9.9.4 SFS Examples

The following example copies the file **demo.txt** from an ftp server with the IP address **192.168.0.100**, username **srv**, and password **admin**.

```
Default>copy ftp://srv:admin@192.168.0.100/demo.txt flash:demo.txt
…
finished
```

The following example copies the file **demo.txt** from flash to server (home directory).

```
Default>copy flash:demo.txt ftp://srv:admin@192.168.0.100/demo.txt
…
finished
```

The following example displays files at the flash.

```
Default>dir flash:

Num       Size  Date       Time      Name
-----------------------------------------
 1          2  02.03.2011 14:59:32  demo.txt
 2       1035  23.02.2011 09:35:11  finallog
 3       6122  24.02.2011 11:06:32  rf.ini
 4          8  12.02.2011 21:20:43  rftype_cfg
 5       5613  02.03.2011 08:51:19  startup-configuration.txt
 6        566  02.03.2011 08:51:19  startup-debug-configuration.txt
 7       5688  02.03.2011 16:51:45  scripts/clear_statistics
 8       2121  25.02.2011 08:50:24  scripts/qos-dscp
 9       2117  24.02.2011 21:07:14  scripts/qos-pcp
 10       2078  13.03.2011 09:42:39  scripts/qos-vid
 11       5688  02.03.2011 16:51:45  scripts/clear_statistics
 12        373  21.03.2011 17:29:05  scripts/system_info
```

9.10 Command Line Scripts

EtherHaul supports the use of pre-composed, multiple-line command scripts. A script is simply a list of CLI commands, saved in a text file, that runs locally on the ODU. Script output is displayed on a script output screen and can be copied and saved.

9.10.1 Displaying Scripts

To display scripts using the Web EMS:

1. In the Web EMS Main screen, click **Advanced Setup**. The Advanced Setup screen is displayed.
2. Click the Scripts section of the Advanced Setup screen.

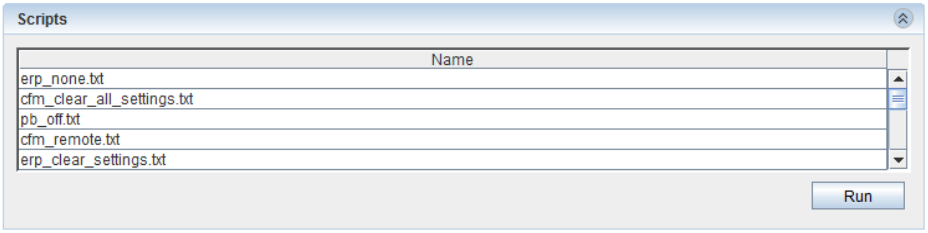


Figure 9-7 Web EMS Advanced Setup Screen – Scripts Section

3. Click **Add**. The Add VLAN window is displayed.

9.10.2 Running Scripts

1. Click the Scripts section of the Advanced Setup screen.
2. Highlight the script and select **Run**. The ODU will run the specified script.

9.10.3 Adding Scripts

You can write scripts in a text file and then copy them to the system. The script must consist of valid CLI commands. To include comments in the script, type # at the beginning of the line. The following is an example of a command line script:

```
# Demo Script
# This script sets the ODU to static mode, saves the
configuration, and resets the system.
set rf mode static qpsk 4 1 0.5
copy running-configuration startup-configuration
reset system
```

To add the script text file to the system, use an ftp server to transfer the file to the **`scripts`** directory under flash (**`flash/scripts`**). The following example transfers the script **`D.txt`** to the system.

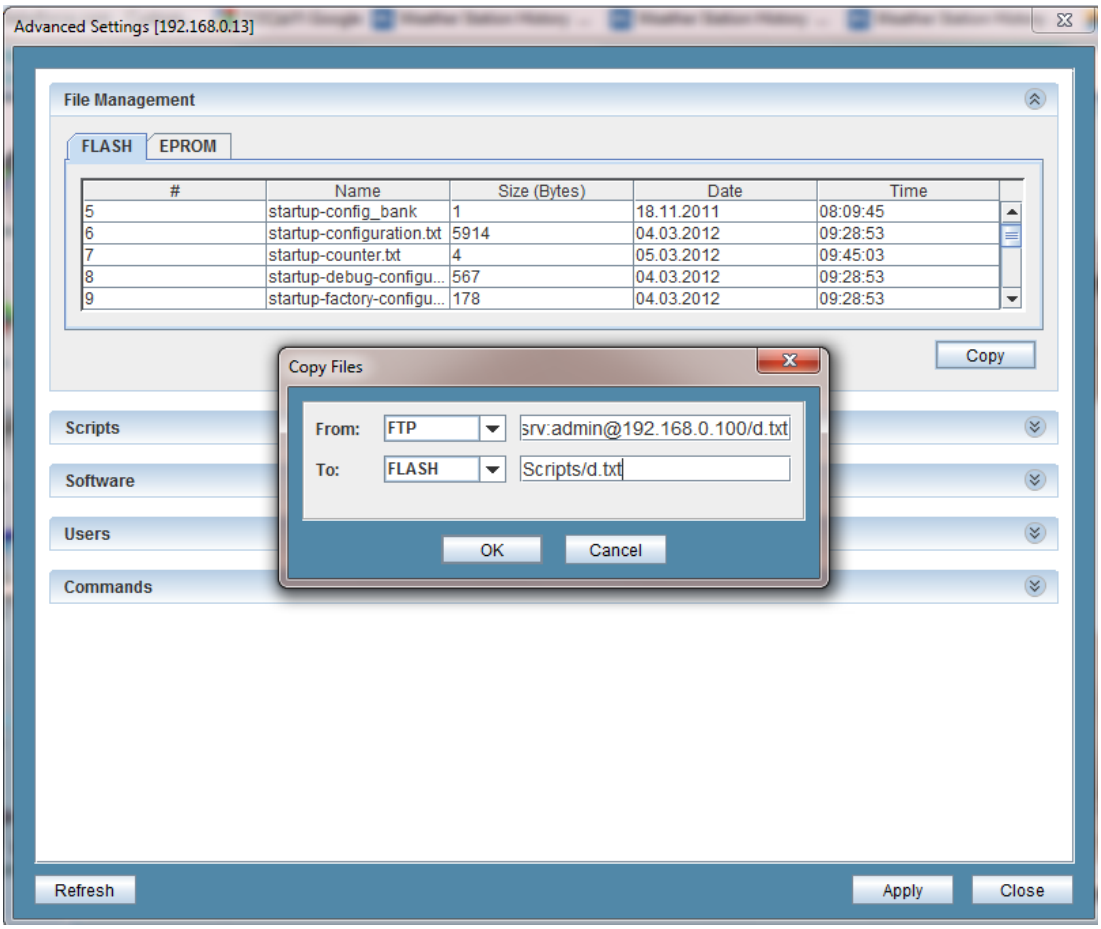


Figure 9-8 Adding Scripts

9.10.4 Viewing Script Content

You cannot display script content directly from the CLI. To view the content of a script, transfer the script to the server and view it with a text editor.

In the same manner, you cannot edit scripts directly on the ODU. To edit a script, transfer the script to the server and edit it with a text editor. Then transfer the new script back to the ODU, overwriting the existing script.

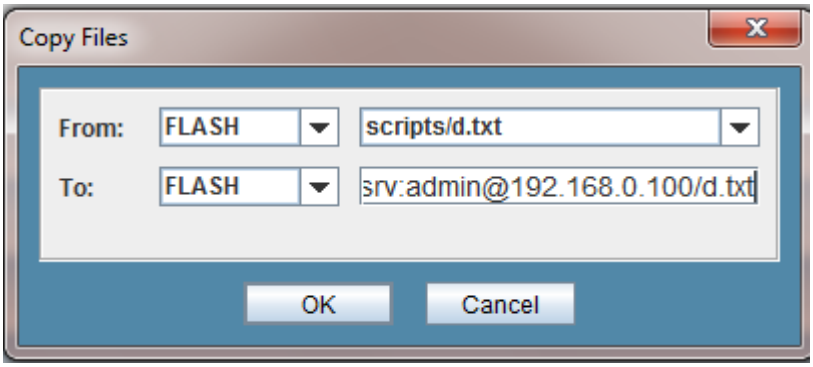


Figure 9-9 Copying Scripts

9.10.5 Command Line Scripts using the CLI

Use the **show script** command to display the names of all script files stored in the local directory.

```
Default>show script
```

Use the run script command to execute scripts.

```
Default>run script <script-filename>
```

To add the script text file to the system, use an ftp server to transfer the file to the **scripts** directory under flash (**flash:scripts**). The following example transfers the script **DemoScript.txt** to the system.

```
Default>copy ftp://srv:admin@192.168.0.100/DemoScript.txt
flash:scripts/DemoScript.txt
…
Finished
```

You cannot display script content directly from the CLI. To view the content of a script, transfer the script to the server and view it with a text editor.

```
Default>copy flash:scripts/DemoScript.txt
ftp://srv:admin@192.168.0.100/ DemoScript.txt
…
finished
```

Use the delete command to delete scripts from **flash:scripts**:

```
Default>del flash:scripts/DemoScript.txt
```

9.11 Configuring NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of network elements over packet-switched, variable-latency data networks.

The EtherHaul 1200 supports NTP client. It can synchronize the host clock to any NTP server in the LAN/Internet to deliver accurate and reliable time.

NTP provides a connectionless service (UDP in the Transport Layer).

9.11.1 NTP Configuration

Use the following command to configure NTP:

```
set ntp  <idx> [server <ip-addr>] [tmz -12..14]
```

Use the following command to display the NTP settings:

```
show ntp [{<idx> | all}[{server | tmz | info}]]
```

Use the following command to clear the NTP settings:

```
clear ntp {<idx> | all}
```

```
* tmz = Time Zone Shift
ntp 1 server                : 192.168.0.222
ntp 1 tmz                   : 2
Right_Master>
```

9.12 Viewing User Activity Log

The ODU stores a log of all activities performed on the ODU.

Information recorded:

- Date, Time, Type (CLI, SNMP), User Name and the command.
- Upon execution of each SNMP set request, a CLI command functionally equivalent to the SNMP set request will be constructed and added to the log.
- In case of SNMPv2 the write community name will be put into the log as the user name.
- In case of SNMPv3 the message user name will be put into the log.

Example:

Left-13>show user-activity-log

Dec 23 08:08:44 sw cad: User: cli admin : set system name Right_11

Dec 23 08:09:44 sw cad: User: cli admin : set rf tx-mute enable

Dec 23 08:10:05 sw cad: User: cli admin : set rf tx-mute disable

Dec 23 08:12:24 sw cad: User: cli admin : clear log

Dec 23 08:16:08 sw cad: User: cli admin : copy sw ftp://192.168.0.254/pub/siklu-uimage-30-5444

Dec 23 08:45:48 sw cad: User: cli tech : run sw immediate no-timeout

Dec 23 09:06:36 sw cad: User: cli admin : copy running-configuration startup-configuration

Dec 23 09:13:09 sw cad: User: cli admin : clear log

Dec 24 02:36:48 sw cad: User: cli admin : set rf mode alignment

Dec 24 02:43:06 sw cad: User: cli admin : reset rf

Dec 24 02:44:34 sw cad: User: cli admin : set license data-rate 1000

9.13 Managing SNMP

The EtherHaul supports SNMPv2 and SNMPv3. SNMP managers and users can be configured.

9.13.1 SNMP Managers

The following command sets the SNMP Trap Destination lists:

set snmp-mng *<ip-addr-list>* ***[udp-port*** *<0..65535>**] [security-name*** *<string>**] [snmp-version {v2 | v3}]***

set snmp-mng <1..5> [ip-addr <value>] [udp-port <0..65535>] [snmp-version {v2 | v3}] [security-name <value>] [engine-id <value>]

Security name is trap community name in the case of SNMPv2 and user name in the case of SNMPv3.

Default ***udp-port*** is 162.

Default ***security-name/trap community*** is “public”.

Default **snmp-version** is v2.

To view the SNMP manager list:

default>show snmp-mng

snmp-mng 1 ip-addr : 192.168.0.100

snmp-mng 1 udp-port : 162

snmp-mng 1 snmp-version : v2c

snmp-mng 1 security-name : public

snmp-mng 1 engine-id : local

9.13.2 SNMP Agent Communities

The following command sets the SNMP agent communities:

set snmp-agent [read-com <value>] [write-com <value>] [snmp-version <value>]

Default ***read-com*** is “public”.

Default ***write-com*** is “private”.

Default **snmp-version** is v2.

To view the SNMP agent communities:

default>show snmp-agent

snmp-agent read-com : public

snmp-agent write-com : private

nmp-agent snmp-version : v2c

9.13.3 SNMPv3 Users Settings

The following command sets the SNMP users settings:

set snmp-user <engine-id> <user> <auth> <priv>

<engine-id> : | local | string

<auth> : none | {md5 <passphrase>} | {sha <passphrase>}

<priv> : none | {des <passphrase>} | {aes <passphrase>}

auth-passphrase and privacy-passphrase are ASCII strings. Together with internally calculated Engine ID these strings are used to produce authentication and privacy keys respectively.

If no parameters except from the user name are supplied to the set command then an entry for the user indentified by the name is created while privacy and authentication algorithms are set to NULL.

If no privacy algorithm (des or aes) is supplied then the privacy algorithm is set to NULL.

If no privacy-passphrase is supplied then the privacy-passphrase is the same as authentication passphrase.

10 EtherHaul Diagnostics

The EtherHaul system's highly reliable and easy-to-use radio link features a wide range of built-in indicators and diagnostic tools designed to enable you to quickly evaluate a link's performance, identify operating faults, and resolve them.

The general diagnostics process for an EtherHaul link is to identify whether there is a problem that needs to be addressed, to isolate the root cause of the problem, and to implement the steps that are required to solve the problem.

The following is a partial list of events that can cause system problems:

- End equipment problems (such as connection or device configuration issues)
- External hardware faults
- System level configuration issues
- Hardware faults that require radio link replacement

This chapter describes the EtherHaul diagnostics features, and offers basic instructions on how to use these features to isolate and resolve operating faults in the ODUs or in the EtherHaul network. The chapter includes the following topics:

- The Troubleshooting and Diagnostics Process
- EtherHaul ODU LEDs
- EtherHaul System Alarms and Events
- EtherHaul System Statistics
- EtherHaul System Loopbacks

10.1 The Troubleshooting and Diagnostics Process

Follow this step-by-step process whenever you encounter a problem with the link.

Define the Problem

Isolating a problem's symptoms is the first step in corrective maintenance. It is important to define the problem clearly and fully.

Define the problem as either a **customer-impact type** (for example, loss of element management, or no Ethernet services over the link) or a **product-related type** (for example, a link is down or an ODU does not power up).

Check and Gather Relevant Information

Examining the link's status indications will provide both current and historical information regarding the link's performance and alarms.

Indications include ODU LEDs, System Alarms and System Statistics.

Use these indications to further refine the problem and help to assess possible causes, both physical and logical, in the EtherHaul system.

Isolate the Fault

Further isolate and characterize the problem using all available link indications.

Ascertain if the problem is related to:

- End-equipment configuration or an interconnection
- A hardware fault in the link's accessories (such as a cable)
- Configuration settings (this can be verified using the CLI)
- A hardware fault in one of the ODUs
- A result of larger network propagation problem

Note that Loopback indications are especially useful when isolating the fault's component and network location.

Correct the Fault

Once the fault is isolated, implement the necessary corrective actions until resolution of the problem is confirmed.

Whenever possible, it is recommended that commissioning tests be repeated in order to verify that the problem link is now operating correctly.

10.2 EtherHaul ODU LEDs

The following table lists the possible status of all LEDs, together with a description for purposes of diagnostics.

LED	Color	Description
PWR (Power)	Green – Power OK	Blink Green – Device boot
	Red – Power Failure	
	Off – No Alarms	
RF	Green – Link Up	Blink Green – RF activity
	Orange – Alignment Mode	
	Off – Link Down	
ETH1/2:	Green – Link 1G	Blink Green – 1G activity
	Orange – Link 10/100	Blink Orange – 10/100 activity
	Off – No Link (Carrier)	

10.3 EtherHaul System Alarms and Events

The following table lists all System Alarms and Events, together with their severity, possible cause and corrective actions.

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Cold Start	Event [Trap, Log]	The ODU is re-initializing due to a Power-Up or Reset action.	N/A	N/A
Link Down	Alarm High [Trap, Log, Active Alarm List]	The communication link (either the RF or one of the Ethernet ports) is not operational.	**Ethernet:** 1) A cable is disconnected. 2) Configuration mismatch between the ODU and end-equipment. **RF Link:** 1) Configuration mismatch between sides (frequency, modulation, RF role, etc.) 2) Line-of-Sight disruption or antennas not aligned. 3) Faulty ODU	**Ethernet:** 1) Check the cable connection. 2) Check the CLI configuration and end-equipment configuration. **RF Link:** 1) Check the configuration. 2) Isolate the problem using loopbacks. 3) Check cable connections and antenna alignment. 4) Replace ODU

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Link Up	Event [Trap, Log]	The communication link (either the RF or one of the Ethernet ports) is operational.	N/A	N/A
Modulation Change	Event [Trap, Log]	The modulation setting for the RF link (currently in Adaptive mode) has changed.	N/A	N/A
Temperature High	Alarm Medium [Trap, Log, Active Alarm List]	The ODU temperature has exceeded a predefined threshold.	1) The ODU is installed in extreme temperature conditions. 2) Wrong temperature reading made in the ODU	1) Check the ODU installation and verify that it is installed in accordance with environmental specifications. 2) Replace ODU
Temperature Normal	Event [Trap, Log]	The temperature of the device has returned to the normal range. This event clears a Temperature High alarm.	N/A	N/A
SFP In	Event [Trap, Log]	SFP inserted	N/A	N/A
SFP Out	Event [Trap, Log]	SFP extracted	N/A	N/A
Reference Clock Source Change	Event [Trap, Log]	The reference clock source for the EtherHaul system has changed.	N/A	N/A
CFM Fault Alarm	Alarm High [Trap, Log, Active Alarm List]	A maintenance end-point (MEP) has a persistent defect condition.	Varies	1) Use the reported OID to determine the source of the fault.
CFM Fault Recovery	Event [Trap, Log]	All MEP defects have been cleared and the alarm has been cleared from the Active Alarm List.	N/A	N/A

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Synthesizer Locked	Event [Trap, Log]	The synthesizer has been locked.	N/A	N/A
Synthesizer Unlocked	Alarm High [Trap, Log, Active Alarm List]	The synthesizer has been unlocked.	N/A	N/A
POE Status Low	Alarm High [Trap, Log, Active Alarm List]	The power level being drawn by the ODU from the Ethernet is low.	Problematic PoE, ODU or connection	1) Check voltage and current supply to the PoE 2) Check cable 3) Replace PoE 4) Replace ODU
POE Status Normal	Event [Trap, Log]	The power level being drawn by the ODU from the Ethernet is normal.	N/A	N/A
ERP Ready	Event [Trap, Log]	ERP is ready for operation	N/A	N/A
Forced Switch	Event [Trap, Log]	ERP event	N/A	N/A
Manual Switch	Event [Trap, Log]	ERP event	N/A	N/A
Signal Fail	Event [Trap, Log]	ERP event	N/A	N/A
Invalid version	Event [Trap, Log]	ERP event	N/A	N/A
Loopback Enabled	Alarm Low [Trap, Log, Active Alarm List]	User enabled loopback	User action	N/A
Loopback Disabled	Event [Trap, Log]	Loopback cleared	User action	N/A
Tx Mute Enabled	Alarm Low [Trap, Log, Active Alarm List]	User enabled Tx Mute	User action	N/A
Tx Mute Disabled	Event [Trap, Log]	Tx Mute cleared	User action	N/A

Indication	Classification and Severity	Explanation	Probable Cause	Corrective Actions
Reception of QL EEC1 or Worse	Alarm Low [Trap, Log, Active Alarm List]	SyncE quality received on the link is same or worse that the ODU's internal clock quality	Network changes or sync failure	N/A
Reception of QL better than EEC1	Event [Trap, Log]	SyncE quality restored	N/A	N/A

10.4 EtherHaul System Statistics

The EtherHaul system uses advanced RF and Ethernet counters to provide real-time performance statistics for radio transmission activities, Ethernet ports, and VLAN traffic.

The following statistics enable quick analysis of system and component performance in support of troubleshooting and diagnostics.

Hint:

For more details on system statistics, refer to *Monitoring the System* on page 112.

10.4.1 RF Statistics

Check RF statistic counters to identify radio errors and check the radio status history. The RF statistics consist of real time statistic counters since the last time the counters were cleared.

The RF transmission quality indicators are **`rf in-errored-pkts`**, **`rf in-lost-pkts`** and **`rf-in-errored-octets`**. A rise in these indicators indicates radio errors. No errors in these indicators indicates that the radio link is operating without errors.

Radio errors observed in these indicators do not mean necessarily frame-loss on the Ethernet service. The ARQ (Automatic Repeat reQuest) algorithm uses selective repeat (retransmission) to eliminate radio BER.

The **`arq-in-loss`** and **`arq-out-loss`** will indicate frame-loss over the radio that will be noticed by the Ethernet service

For detailed explanations of all RF statistics, refer to *Viewing Radio Statistics* on page 114.

10.4.2 VLAN Statistics

You can display statistic counters of each EtherHaul component per VLAN:

```
Default>>show vlan all statistics
component  vlan  port  in-pkts  out-pkts  drop-pkts  elapsed-time
c1         1     host  0        0         0          0000:00:00:32
c1         100   host  96       0         0          0000:00:00:32
c2         1     eth0  0        0         0          0000:00:00:32
c2         100   eth0  100      127       0          0000:00:00:32
c2         110   eth0  0        28601     0          0000:00:00:32
c2         120   eth0  0        28601     0          0000:00:00:32
c2         130   eth0  0        57180     0          0000:00:00:32
c3         1     eth1  0        0         0          0000:00:00:32
c3         110   eth1  28601    0         0          0000:00:00:32
c3         120   eth1  28601    0         0          0000:00:00:32
c3         130   eth1  71518    0         0          0000:00:00:32
c4         1     eth2  0        0         0          0000:00:00:32
c4         100   eth2  224      196       0          0000:00:00:32
```

Observe the **in-pkts**, **out-pkts** and **dropped-pkts** for each VLAN.

Note that packets may be dropped due to traffic exceeding the radio link's maximum bandwidth.

For detailed explanations of all VLAN statistics, refer to *Viewing VLAN Statistics* on page 117.

10.4.3 Ethernet Statistics

You can display Ethernet statistics counters per Ethernet port.

```
Default>show eth all statistics
eth eth0 elapsed-time          : 0000:00:41:17
eth eth0 in-octets             : 18835233
eth eth0 in-ucast-pkts         : 4294967357
eth eth0 in-discards           : 0
eth eth0 in-errors             : 0
eth eth0 out-octets            : 19839102
eth eth0 out-ucast-pkts        : 63
eth eth0 out-errors            : 0
eth eth0 in-mcast-pkts         : 44
eth eth0 in-bcast-pkts         : 247622
eth eth0 out-mcast-pkts        : 247737
eth eth0 out-bcast-pkts        : 0
eth eth0 out-discards          : 0
eth eth0 in-no-rule-discards   : 0
```

Observe the **discard** and **error** counters to evaluate the performance of the Ethernet transmission.

For detailed explanations of all Ethernet statistics, refer to *Viewing Ethernet Statistics* on page 119.

10.5 EtherHaul System Loopbacks

The EtherHaul radio uses Ethernet and RF loopbacks designed to enable fault isolation and Ethernet service performance testing.

- **Ethernet Loopback –** Internal and external loopbacks are performed on the interface, testing the local ODU, the radio link, and the remote ODU.
- **RF (Radio) Loopback –** Internal loopback is performed on the ODU's RF output.

Note:

After activating Loopback, it is important to **clear all RF and Ethernet statistics** in order to receive the most accurate results for analysis.

Use system alarms as well as statistic displays to determine if Loopback testing has passed or failed.

10.5.1 Loopback Diagrams

10.5.1.1 System Loopback Points

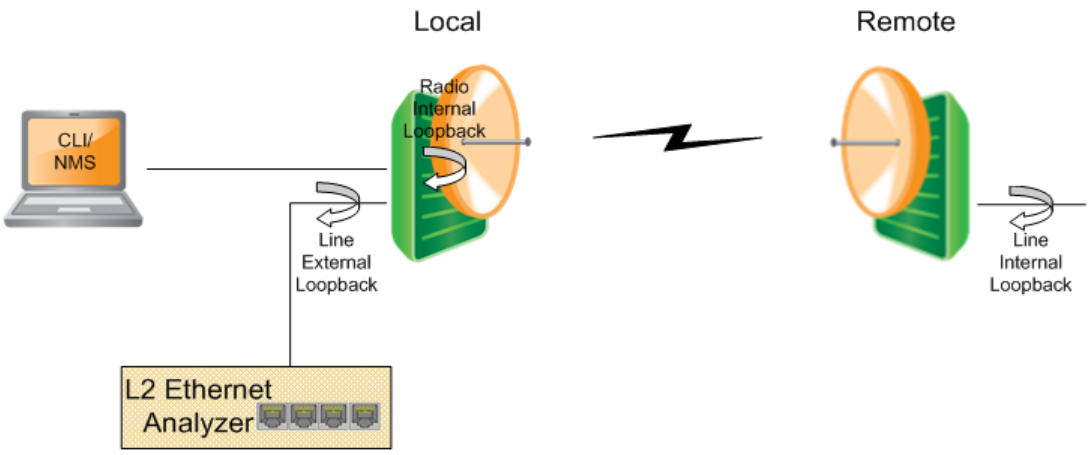


Figure 10-1 EtherHaul 1200 System Loopback Points

10.5.1.2 Ethernet External Line Loopback Point

The Ethernet traffic from the customer's end-equipment or Ethernet analyzer is looped on the Ethernet interface (Eth1 or Eth2), enabling testing of the connection (cable/fiber) and the interface between end-equipment and the ODU.

When testing a link from one side (local), an external line loopback should be applied on the local unit.

The loopback can be applied separately for Eth1 and Eth2, and can be set with or without MAC Address swapping.

Set the loopback mode to external for the desired Ethernet port and set the loopback-timeout in seconds:

```
set eth eth1 loopback-timeout 300
set eth eth1 loopback-mode external-mac-swap
```

Use the following command to clear the loopback:

```
set eth eth1 loopback-mode disable
```

10.5.1.3 RF (Radio) Internal Loopback Point

The Ethernet traffic from a customer's end-equipment or Ethernet analyzer is looped on the ODU's radio output, enabling testing of the connection (cable/fiber), the interface between end-equipment and the ODU and the local ODU.

The loopback should be set with MAC Address swapping and on specific modulation profile.

Set the loopback mode on the RF menu and set the loopback-timeout in seconds:

```
set rf loopback-timeout 300
set rf loopback-mode internal-mac-swap qam64 4 1 0.5
```

Use the following command to clear the loopback:

```
set rf loopback-mode disable
```

Note:

For error-free operation at high modulation profiles, no interference should be present. Switch off remote ODU or change its frequency to eliminate risk of interference.

10.5.1.4 Ethernet Internal Line Loopback Point

An Internal External loop returns the received frames to the radio side, enabling you to test Ethernet traffic across the link.

The Ethernet traffic from the Customer's end-equipment or Ethernet analyzer is looped at the Ethernet interface of the remote ODU, enabling testing of the connection (cable/fiber), the interface between end-equipment and the ODU, both local and remote ODUs, and the radio transmission.

The loopback can be applied separately for Eth1 and Eth2, and can be set with or without MAC Address swapping.

Set the loopback mode to internal for the desired Ethernet port and set the loopback-timeout in seconds:

```
set eth eth1 loopback-timeout 300
set eth eth1 loopback-mode internal-mac-swap
```

Use the following command to clear the loopback:

```
set eth eth1 loopback-mode disable
```

11 Using the EtherHaul CLI

This chapter describes how to use the EtherHaul Command Line Interface (CLI) client to configure and maintain EtherHaul devices on your network, and includes the following topics:

- Invoking the CLI
- CLI Command Syntax
- Viewing the CLI Command History
- Invoking CLI Help and Autocompletion
- CLI Error Messages
- Viewing the EtherHaul Statistics History
- CLI Managed Object Reference
- Management Object Attributes
- Radio Object Attributes
- Encryption Object Attributes
- Connectivity Fault Management (CFM) Object Attributes
- Network Object Attributes

11.1 Invoking the CLI

1. Run a standard SSH client. You can use a common, open source SSH client programs such as PuTTY.
2. Enter the ODU's IP address and open the connection. The default IP address is 192.168.0.1.
3. Login as user **admin**.
4. Enter the password **admin**.

When a successful connection is established, the ODU responds as follows:

```
Siklu-OS
>
Default>
```

EtherHaul CLI commands should only be entered at the above prompt.

11.2 CLI Command Syntax

After invoking the CLI, you can input commands. Each CLI command is submitted to the EtherHaul device for execution, after which a response is typically returned.

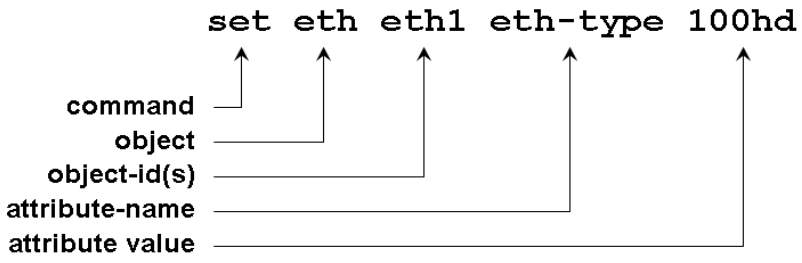
Each command line submitted to the CLI consists of:

1. A unique command that specifies the action(s) to be performed.
2. The object type on which action(s) will be performed.
3. The identifier(s) for the object(s) on which action(s) will be performed.
4. Zero or more object attributes that typically specify the value or characteristics for each action.

A CLI command line typically uses the following basic form:

command object <object-id(s)> [attribute-name <attribute-value>]

For example:



11.2.1 Basic Conventions

- CLI commands are not case sensitive.
- You can abbreviate commands and parameters as long as they contain enough letters to be distinguished from any other currently available commands or parameters.
- The commands entered from the CLI can apply to the entire system, to a specific port, or to a specific VLAN.

11.2.2 Common Syntax Rules

This document uses the following notation conventions when presenting CLI usage examples. These syntax conventions are found in commands, index names, objects and attributes.

Syntax	Meaning
{a | b | c}	One of the specified values must be entered in the command line
<name>	The name of a required attribute, explained in an accompanying or referenced section.
[name]	The name of an optional attribute, explained in an accompanying or referenced section.
n…m	Represents a number or integer series from n to m.

11.2.3 Repeatedly Used Identifiers

This document uses the following identifying conventions when presenting CLI usage examples. These syntax conventions are used primarily to represent various types of objects and lists that are to be specified on the command line.

For more information on using identifiers in the EtherHaul CLI, refer to *Designating Named Objects* on page 158.

Convention	Meaning
<comp-id>	A single component ID (one of c1, c2, c3, c4, c4, s1)
<bridge-port>	A single port name (one of host, eth0, eth1, eth2, c1, c2, c3, c4, c4, s1)
<fdb-id>	A single FID (number from 1 to 64)
<vid>	A single VID (number from 1 to 4094)
<mac-addr>	A MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (*e.g.*, 00-AF-DD-1E-2D-A3).
<ip-addr>	A standard dotted notation IP address (*e.g.*, 10.0.15.74)
<ip-mask>	The IP address mask, *i.e.*, the number of bits that constitute the IP network address prefix.
<comp-id-list>	A comma-separated list of the component IDs, *e.g.*, c1, c2, c3, c4, c4, s1. Any combination of the component IDs can be included in the list. For details, refer to *Designating Named Objects* on page 158.
<c-comp-id-list>	A comma-separated list of the C-component IDs, *e.g.,* c1, c2, c3, c4, c4. Any combination of the component IDs can be included in the list. For details, refer to *Designating Named Objects* on page 158.
<bridge-port-list>	A comma-separated list of port names, *e.g.*, host, eth0, eth1, eth2, c1, c2, c3, c4, c4, s1. Any combination of the names can be included in the list. For details, refer to *Designating Named Objects* on page 158.
<eth-list>	A comma-separated list of external port names, *e.g.*, host, eth0, eth1, eth2. Any combination of the names can be included in the list. For details, refer to *Designating Named Objects* on page 158.

Convention	Meaning
<ext-bridge-port-list>	A comma-separated list of external port names, *e.g.*, host, eth0, eth1, eth2. Any combination of the names can be included in the list. For details, refer to *Designating Named Objects* on page 158.
<vid-list>	A list of ranges of VIDs from 1 to 4094. The notation covers comma-separated lists of the numbers within the specified range, as well a range of numbers separated by a hyphen, *e.g.*, 5-25. For details, refer to *Designating Indexed Objects* on page 159.
<fdb-id-list>	A list of ranges of FIDs from 1 to 64. The notation covers comma-separated lists of the numbers within the specified range, as well as a range of numbers separated by a hyphen, *e.g.*, 5-25. For details, refer to *Designating Indexed Objects* on page 159.
<comp-id>	A single component ID (one of c1, c2, c3, c4, c4, s1)
<bridge-port>	A single port name (one of host, eth0, eth1, eth2, c1, c2, c3, c4, c4, s1)
<fdb-id>	A single FID (number from 1 to 64)
<vid>	A single VID (number from 1 to 4094)
<mac-addr>	A MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (*e.g.*, 00-AF-DD-1E-2D-A3).
<ip-addr>	A standard dotted notation IP address (*e.g.*, 10.0.15.74)
<ip-mask>	The IP address mask, *i.e.*, the number of bits that constitute the IP network address prefix.
<qid-list>	A range of numbers from 1 to 8.
<hist-range>	A list of ranges of history interval numbers from 0 to 95. The notation covers comma-separated lists of the numbers within the specified range, as well as a range of numbers separated by a hyphen, *e.g.*, 5-25. For details, refer to *Designating Indexed Objects* on page 159.

11.2.4 CLI Command Types

The CLI uses a limited number of commands to create, maintain, and monitor an EtherHaul configuration.

To perform this operation…	…use this CLI Command:
Create, update or modify an object	Set
Display the characteristics or values of an object	Show
Reset or delete specified characteristics or values of an object	Clear
Reset the RF or System	Reset

The following sections describe the generic use of these routine CLI commands.

When performing non-routine activities, some additional commands are used, including **`copy`**, **`run`**, and **`accept`**. See, e.g., *Upgrading the ODU Software* on page 125 and *Performing Address Translation* on page 130.

Hint: CLI command syntax changes to fit the EtherHaul object being managed or displayed. For specific command syntax and execution details, see the information that accompanies a particular object, starting in *CLI Managed Object Reference* on page 165.

11.2.4.1 Set Commands

The Set command is used to create, update and modify the characteristics of dynamic objects in the EtherHaul configuration and values for a chosen object. Examples of dynamic objects are: VLANs, MEPs, and Static MAC Addresses.

The generic form the Set command is:

`set object-name <object-ids> [attribute-name <value>]` … `[attribute-name <value>]`

If a dynamic object does not already exist, the Set command creates it and assigns the attributes specified. Upon creation, in the event that an attribute is not explicitly specified, the entry is created with the default value for that attribute.

If the dynamic object already exists, then the Set command will replace the attributes that are currently defined for the entry with those specified in the command.

If a **`set`** command is entered in an incomplete or invalid form, when possible, the CLI will respond with an execution error message that specifies the reason for the error. For more information on error handling in the CLI, refer to *CLI Error Messages* on page *11.5*163.

11.2.4.2 Show Commands

The Show command is used to display the current characteristics and other values for a chosen object.

The generic form the Show command is:

`show object-name <object-ids> [attribute-name]`

If a **`show`** command is entered in an incomplete form, when possible, the CLI will automatically complete missing object-ids with the keyword **`all`**, and missing attributes with the keyword **`info`**.

For example:

When this Command is entered…	…the CLI interprets the Command as:
`show system`	`show system info.`
`show eth`	`show eth all info.`
`show bridge-port`	`show bridge-port all info`
`show bridge-port c2`	`show bridge-port c2 all info`
`show bridge-port c2 eth0`	`show bridge-port c2 eth0 info`
`show vlan`	`show vlan all info`
`show vlan s1`	`show vlan s1 all info`
`show vlan s1 123-170`	`show vlan s1 123-170 info`

For more information on the EtherHaul CLI autocompletion feature, see *Invoking CLI Help and Autocompletion* on page 161.

Note:

The autocompletion mechanism does not enable the omission of object-ids or attributes which are required for correct command interpretation.

For example, **`show vlan 123-170`** will not be correctly autocompleted because it lacks a required reference to the object **`s1`**.

When a **`show`** command is entered with the names or ids of an object that does not exist, the reference to the non-existing object is ignored and the information requested is displayed for all existing objects.

11.2.4.3 Display Formats

Both line-by-line and table methods are available for displaying attributes. The method used depends upon the object being displayed.

Line-by-line per attribute displays the objects in the form:

`<object-name> <object-id> <attribute-name>: <value>`

Note that multiple **<object-ids>** may be displayed using this form.

The Table display method presents the information in blocks and omits the object name and IDs, as in the form:

```
<attribute-name>     <attribute-name>     <attribute-name>
<value>              <value>                 <value>
```

11.2.4.4 Clear Commands

The Clear command is used to reset or delete the specified values for a chosen object.

The generic form of the Clear command is:

```
clear object-name <object-ids> [attribute-name]
```

Nearly all **`clear`** commands require that at least one object identifier follow the object name in the command line. Alternatively, an object identifier may be replaced on the command line with the word **`all`**, which typically will be interpreted as "the whole range" (or "the whole set") of identifiers for the specified object.

11.2.4.5 Reset Commands

There are two Reset commands used in the EtherHaul system. Reset commands are used exclusively during initialization or reboot activities.

Reset RF

Resetting the RF returns the radio and modem hardware to its default settings. The command does not change a system configuration.

```
Default>reset rf
```

Reset RF is required whenever an RF Mode change is made from Alignment to Adaptive or Static.

Note:

Resetting the RF causes a service disruption of approximately **2 seconds** in duration.

Reset System

Resetting the System reboots and reloads the currently saved system startup configuration.

```
Default>reset system
```

Reset System is used for power up and is required after software upgrades.

Note:

Resetting the System causes a service disruption of approximately **90 seconds** in duration.

11.2.5 Designating Objects in CLI Commands

The CLI requires explicit identifiers to perform operations on the objects in an EtherHaul configuration. You can designate a specific object (*e.g.*, a bridge) by using its unique identifier.

Two types of object identifiers are used in the CLI:

- Object Names
- Object Indexes

11.2.6 Designating Named Objects

Certain EtherHaul CLI objects are identified by symbolic names. These names are static and are always assigned to the same EtherHaul object type. Using static names generally makes system configuration much easier and more consistent from network to network.

For example, the designation:

`eth eth0`

refers to the *Wireless Port*, while the designation:

`bridge-port s1 c3`

refers to *Port c3* on *Component s1*.

The following lists all named objects used in the CLI, together with the EtherHaul objects that they reference:

CLI Name	Referenced Object
eth0	Wireless port
eth1	Wired Ethernet port 1
eth2	Wired Ethernet port 2
host	Internal CPU
s1	S-component 1
c1	C-component 1
c2	C-component 2
c3	C-component 3
c4	C-component 4

The CLI supports specifying a list of named objects by entering multiple comma-separated names.

For example:

`eth eth0, host, eth1`

specifies to three **`eth`** objects: *eth0, host* and *eth1*;

`bridge c1, c2, s1`

specifies three bridge components: *c1, c2* and *s1*; and

`egress host, s1`

specifies two egress ports: *host* and *s1*.

Hint:

When using the **show** and **clear** commands, the keyword **all** may be substituted for a list of object names. In this context, "all" means all of the objects.

For example: **eth all** is identical to **eth host, eth0, eth1, eth2**.

11.2.6.1 Multi-Dimensional Object Lists

To specify objects in a multi-dimensional object list, the symbol names (or comma-delimited lists of names) are entered one after another, and are separated by spaces. The generic syntax is as follows:

```
object {<name1>}  {<name2>}  {<name3>}
```

For example:

bridge-port c1 host, s1

specifies the bridge ports *c1 host* and *c1 s1*.

Note that not every combination of keywords is valid. For example, the command **bridge-port c1, c2 host** is invalid, because two different C-components cannot be associated with the same port.

11.2.6.2 Designating Indexed Objects

Countable EtherHaul CLI objects are specified by their unique identifying keyword, followed by the object's index number. A VLAN is a typical, countable object. For example:

```
vlan 230
```

refers to the VLAN with the index number 230.

A complete list of indexed objects is specified in a command using a comma-separated series. For example:

vlan 230, 330, 430

refers to VLANs with the index numbers 230, 330 and 430.

It is also possible to specify a range of indexed objects in a command. For example:

```
vlan 230-270
```

refers to VLANs with the index numbers 230 to 270, inclusive.

Finally, a mixed method may be used for specifying indexed objects in a command, enabling references to both a range of objects and to individual objects. For example:

vlan 230-270, 300, 401-410

refers to VLANs with the index numbers 230 to 270, VLAN number 300 and VLANs 401 to 410.

Designating indexed objects is valid in all **`set`**, **`show`** and **`clear`** commands. If the **`show`** command is executed for indexed objects which do not exist, the non-existing objects are ignored and the command is only executed for existing objects.

Hint:

When using the **`show`** and **`clear`** commands, the keyword **`all`** may be substituted for an indexed numerical range. In this context, "all" means the entire object range.

For example: **`vlan all`** is identical to **`vlan 1-4094`**.

11.2.6.3 Multi-Dimensional Objects with Indexes

The CLI supports multi-dimensional objects with numerical indexes. If they appear then their indexes (or lists of ranges of indexes) are placed one after another and are separated by spaces. The generic syntax is as follows: *object {<idx1>} {<idx2>} {<idx3>}*.

More specifically: *object 2, 9, 23-25* means the collection of double indexed objects: {2, 23}, {2, 24}, {2, 25}, {9, 23}, {9, 24}, {9, 25}.

For **show** and **clear** commands you can use the word **all** instead of either index. For example: *object 2, 9 all* or *object all 23-25* or *object all all*.

11.3 Viewing the CLI Command History

The EtherHaul CLI maintains a history of the 100 most recent commands. This is especially useful when recalling long, complex or repetitive entries.

To recall commands from the history buffer, you can press the following keys:

Key press	Result
Up Arrow	Recall commands in the history buffer, beginning with the most recent command. Press the key repeatedly to recall successively older commands.
Down Arrow	Return to more recent commands in the history buffer, after recalling one or more commands with the Up Arrow key. Press the key repeatedly to recall successively more recent commands.

11.4 Invoking CLI Help and Autocompletion

The EtherHaul CLI assists you both actively and passively, as follows:

- You can explicitly request syntax help on the command line.
- You can explicitly request autocompletion assistance on the command line.
- The CLI command interpreter always checks the validity and completeness of a string that is entered on the command line.
  - When a command is determined to be invalid, the CLI responds with a help message. If possible, the command interpreter will derive the intended command from the initial entry and will explain the syntax of the command and the range of allowed values.
  - When a command is determined to be incomplete (for example, if a required object or attribute is missing), the CLI responds with a choice of variants that represent the possible values, based on your initial entry.

The following table summarizes the ways to invoke CLI help and autocompletion features:

Feature	Description
Help <*string*>	Returns a help line for the requested command and object. For example: **Default> help set vlan xxx** *Will return:* **Default> set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress <bridge-ports>] [untagged <bridge-ports>] where <bridge-ports> are port names or none fdbid in range 1..64 and relevant for s-vlans only**

Feature	Description
<*string*> ?	Returns a detailed list of commands that begin with a particular character string. For example: **Default> set vlan?** *Will return:* **Default> set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress <bridge ports>] [untagged <bridge ports>] where <bridge ports> are port names or none fdbid in range 1..64 and relevant for s-vlans only** Following printout, the CLI prompts you with the command that was input: **Default> set vlan xxx**
<*string*> <tab>	Automatically completes a specific command name. For example: **Default> set vl <tab>** **Default> set vlan** **Default> se vl 33 e** **Default> set vlan 33 egress** If more than one command matches the string that you entered, the CLI indicates that an ambiguous command has been entered. Note that the autocompletion feature does not function for indexes, MAC addresses or IP addresses.
? or Help (without a string)	Returns a list of top-level CLI commands only.

11.5 CLI Error Messages

EtherHaul CLI issues three types of error messages:

- **%Ambiguous command**. This error occurs when the command entered can only be partially interpreted. If possible, following the error message, a help syntax line is returned to assist you in correcting the command. For example:

```
Default> sh i
%Ambiguous command: sh i
show system, show bridge, show bridge-port, show eth, show
vlan-common, show vlan, show fdb, show fdb-table, show ip,
show rf, show arp, show cvlan-reg, show pep-vp, show svid-
xlat, show cfm-md, show crm-ma, show cfm-mep, show cfm-ccm,
show cfm-peer-mep-db
Default> sh i
```

- **%Invalid input**. This error occurs when the command entered includes an attribute value that is outside of the range allowed. To assist you, the CLI returns the entered command with a question mark (?) added, immediately following the erroneous parameter, as well as the entire command syntax. For example:

```
Default> set vlan c1 5000 egress 1, 3
%Invalid input: set vlan c1 5000 (?) egress 1, 3
set vlan <comp-id-list> <vid-list> [fdb-id <fdbid>] [egress
<bridge-ports>] [untagged <bridge-ports>] where <bridge-
ports> are port names  or none fdbid in range 1..64 and
relevant for s-vlans only
```

- **General Execution Errors**. This error occurs when the command entered has correct syntax but cannot be executed for some reason. Such error messages are often application or object dependant.

11.6 Viewing the EtherHaul Statistics History

The EtherHaul CLI enables you to view standard operational and performance statistics for various objects in the system.

View the statistics history using the **show** command:

```
show <object> <comp-id> statistics
     [{<hist-range> | all}]
```

For example:

```
show RF statistics
```

Hint:

For a complete description of available statistics, refer to *Monitoring the System* on page 112.

11.6.1 Using Statistics Intervals

You can specify a range of history intervals for the requested object statistics.

When a statistics interval is requested, the CLI returns information in the following format:

```
Interval    Start     End
<num>       <time>       <time>
```

Where:

<num> = is the interval number, from 0 to 95. Interval 0 is the current interval, while intervals 1 to 95 hold statistics collected from 15 to 1425 minutes ago. The duration time for each interval is 15 minutes.

<time> = is the interval time, displayed in a format that is identical to the System Up Time (*Table 11-1*).

When a history interval is not specified in the command line, the CLI will display the ordinary accumulative counters associated with the object.

Note:

Using the **clear statistics** command will erase all accumulative counters as well as the counters for Interval 0.

11.7 CLI Managed Object Reference

This section describes all EtherHaul System objects that can be created, modified, displayed or deleted using the command line interface.

Use Figure 11-1 to quickly identify and locate a specific EtherHaul object according to its logical function in the EtherHaul System.

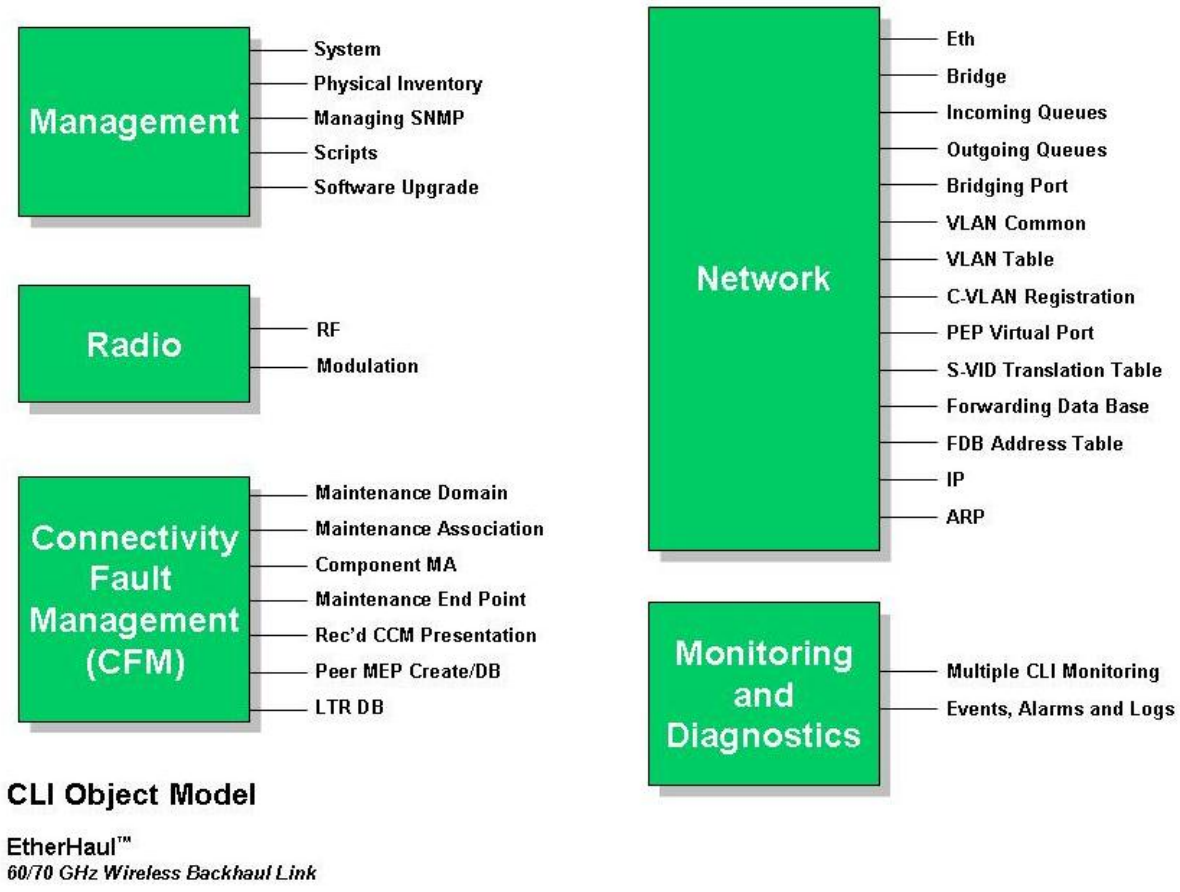


Figure 11-1 The EtherHaul CLI Object Model

11.8 Management Object Attributes

This section lists and describes the attributes of network commands.

11.8.1 System Object Attributes

Table 11-1 System Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
System Description (description)	A text string describing the system. Generally includes the full name and version identification of the system's hardware type, operating-system, and networking software.	sysDescr (1.3.6.1.2.1.1.1)	Variable ASCII text	RO	EH-1200 HW W.X SW Y.Z., where W.X =the HW version Y.Z =the SW version
System Object ID (snmp-id)	The vendor's authoritative identification of the network management subsystem contained in the entity.	sysObiectID (1.3.6.1.2.1.1.2)	1.3.6.1.4.1.31926	RO	1.3.6.1.4.1.31926
System Up Time (up-time)	The length of time that has passed since the network management portion of the system was last re-initialized.	sysUpTime (1.3.6.1.2.1.1.3)	ddd:hh:mm:ss, where ddd=decimal integer representing days (it can be an arbitrary number of digits) hh=two-digit decimal integer representing the hours of a day [0..23] mm=two-digit decimal integer representing minutes of an hour [0..59] ss=two-digit decimal integer representing seconds of a minute [0..59]	RO	N/A
System Contact (contact)	A text string identifying the contact person responsible for this managed node, together with information on how to contact this person.	sysContact (1.3.6.1.2.1.1.4)	Up to 256 characters. If no contact information exists, the value returns a zero-length string.	RW	"sysContact undefined"

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
System Name (name)	A name assigned by the administrator to this managed node. Generally, by convention, this is the node's fully-qualified domain name. This value is also used as the system prompt string. If no System Name is assigned the system prompt will read "Default."	sysName (1.3.6.1.2.1.1.5)	Up to 256 characters. If no system name exists, the value returns a zero-length string.	RW	"Default"
System Location (location)	The physical location of this node (e.g., 'telephone closet, 3rd floor').	sysLocation (1.3.6.1.2.1.1.6)	Up to 256 characters. If no system location exists, the value returns a zero-length string.	RW	"sysLocation undefined"
Input Voltage (voltage)	The system input voltage.	sikluSysVoltage (1.3.6.1.4.1.31926.1.1)	Integer	RO	N/A
Enclosure Temperature (temperature)	The system enclosure temperature.	sikluSysTemperature (1.3.6.1.4.1.31926.1.2)	Integer	RO	N/A
System Date and Time (date, time)	The host's local date and time of day.	hrSystemDate (1.3.6.1.2.1.25.1.2) As defined in RFC 2790	yyyy-mm-dd hh:mm:ss, where: yyyy= year (0 – 9999) mm= month (1 – 12) dd= day (1 – 31) hh= hour (0 – 24) mm= minute (0 – 60) ss= second (0 – 60)	RW	None

11.8.2 Physical Inventory Object Attributes

Table 11-2 Physical Inventory Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Inventory Index	The index for the table entry.	entPhysicalIndex (1.3.6.1.2.1.47.1.1.1.1.1)	integer32 (1..2147483647)	integer
Physical Descriptor (desc.)	A textual description of physical entity. This object should contain a string that identifies the manufacturer's name for the physical entity, and should be set to a distinct value for each version or model of the physical entity.	entPhysicalDescr (1.3.6.1.2.1.47.1.1.1.1.2)	character string	character string
Contained In (cont-in)	The value of entPhysicalIndex for the physical entity which contains this physical entity. A value of zero indicates this physical entity is not contained in any other physical entity. Note that the set of containment relationships define a strict hierarchy; that is, recursion is not allowed. In the event that a physical entity is contained by more than one physical entity (e.g., double-wide modules), this object should identify the containing entity with the lowest value of entPhysicalIndex.	entPhysicalContainedIn (1.3.6.1.2.1.47.1.1.1.1.4)	integer32 (0..2147483647)	integer

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Class (class)	An indication of the general hardware type of the physical entity. If no appropriate standard registration identifier exists for this physical entity, then the value 'other(1)' is returned. If the value is unknown by this agent, then the value 'unknown(2)' is returned.	entPhysicalClass (1.3.6.1.2.1.47.1.1.1.1.5)	INTEGER { other(1), unknown(2), chassis(3), backplane(4), container(5), -- e.g., chassis slot or daughter-card holder powerSupply(6), fan(7), sensor(8), module(9), -- e.g., plug-in card or daughter-card port(10), stack(11), -- e.g., stack of multiple chassis entities cpu(12) }	{other, unknown, chassis, backplane, container, power-supply, fan, sensor, module, port, stack, cpu}
Parent Relative Position (rel-pos)	An indication of the relative position of this child component among all its sibling components. Sibling components are defined as entPhysicalEntries that share the same instance values of each of the entPhysicalContainedIn and entPhysicalClass objects. An NMS can use this object to identify the relative ordering for all sibling components of a particular parent (identified by the entPhysicalContainedIn instance in each sibling entry).	entPhysicalParentRelPos (1.3.6.1.2.1.47.1.1.1.1.6)	integer32 (-1..2147483647)	integer

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Name (name)	The textual name of the physical entity. The value of this object should be the name of the component as assigned by the local device and should be suitable for use in commands entered at the device's `console'. This might be a text name (e.g., `console') or a simple component number (e.g., port or module number, such as `1'), depending on the physical component naming syntax of the device. If there is no local name, or if this object is otherwise not applicable, then this object contains a zero-length string.	entPhysicalName (1.3.6.1.2.1.47.1.1.1.1.7)	character string	character string
Physical Hardware Revision (hw-rev)	The vendor-specific hardware revision string for the physical entity. The preferred value is the hardware revision identifier actually printed on the component itself (if present). Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific hardware revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.	entPhysicalHardwareRev (1.3.6.1.2.1.47.1.1.1.1.8)	character string	character string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Firmware Revision (fw-rev)	The vendor-specific firmware revision string for the physical entity. Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific firmware revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.	entPhysicalFirmwareRev (1.3.6.1.2.1.47.1.1.1.1.9)	character string	character string
Physical Software Revision (sw-rev)	The vendor-specific software revision string for the physical entity. Note that if revision information is stored internally in a non-printable (e.g., binary) format, then the agent must convert such information to a printable format, in an implementation-specific manner. If no specific software revision string is associated with the physical component, or if this information is unknown to the agent, then this object will contain a zero-length string.	entPhysicalSoftwareRev (1.3.6.1.2.1.47.1.1.1.1.10)	character string	character string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Physical Serial Number (serial)	The vendor-specific serial number string for the physical entity. The preferred value is the serial number string actually printed on the component itself (if present). Not every physical component will have a serial number, or even need one. Physical entities for which the associated value of the entPhysicalIsFRU object is equal to 'false(2)' (e.g., the repeater ports within a repeater module), do not need their own unique serial number. An agent does not have to provide write access for such entities, and may return a zero-length string.	entPhysicalSerialNum (1.3.6.1.2.1.47.1.1.1.1.11)	character string (up to 32 chars)	character string (up to 32 chars)
Physical Manufacturer Name (mfg-name)	The name of the manufacturer of this physical component. The preferred value is the manufacturer name string actually printed on the component itself (if present). If the manufacturer name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.	entPhysicalMfgName (1.3.6.1.2.1.47.1.1.1.1.12)	character string	character string
Physical Model Name (model-name)	The vendor-specific model name identifier string associated with this physical component. The preferred value is the customer-visible part number, which may be printed on the component itself. If the model name string associated with the physical component is unknown to the agent, then this object will contain a zero-length string.	entPhysicalModelName (1.3.6.1.2.1.47.1.1.1.1.13)	character string	character string

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	CLI Syntax
Field Replaceable Unit Indicator (fru)	This object indicates whether or not this physical entity is considered a 'field replaceable unit' by the vendor. If this object contains the value 'true(1)' then this entPhysicalEntry identifies a field replaceable unit. For all entPhysicalEntries that represent components permanently contained within a field replaceable unit, the value 'false(2)' should be returned for this object.	entPhysicalIsFRU (1.3.6.1.2.1.47.1.1.1.1.16)	{true (1), false(2)}	{replaceable | not-replaceable}
Last Change Time (last-change)	The value of sysUpTime at the time the configuration of the entity has changed.	1.3.6.1.2.1.47.1.4.1 (entLastChangeTime)	TimeTicks	ddd:hh:mm:ss, wherein ddd – decimal integer representing days (it may include arbitrary number of digits), hh – two-digit decimal integer representing hours of day [0..23], mm – two-digit decimal integer representing minutes of hour [0..59], ss – two-digit decimal integer representing seconds of minute [0..59].

11.8.3 Physical Inventory Entities

Figure 11-2 shows all physical inventory entities and their relationship.

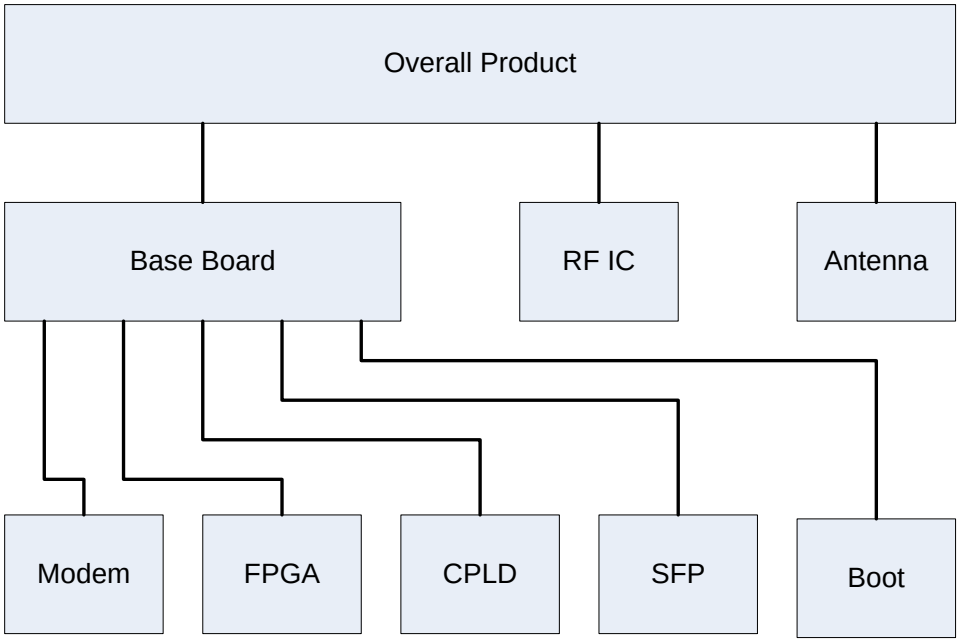


Figure 11-2 Physical Inventory Hierarchy Scheme

11.8.3.1 Overall Product

Attribute	Value
Inventory Index	1
Descriptor	“Siklu EH-1200”
Contained In	0
Class	chassis
Parent Relative Position	-1
Name	“EH-1200”
Hardware Revision	empty
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	“Siklu”
Model Name	“EH-1200”
Field Replaceable Unit Indicator	replaceable

11.8.3.2 Antenna

Attribute	Value
Inventory Index	2
Descriptor	“Siklu Antenna”
Contained In	1
Class	other
Parent Relative Position	0
Name	“Antenna”
Hardware Revision	empty
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.3 RF IC

Attribute	Value
Inventory Index	3
Descriptor	“Siklu EH-1200 RF IC”
Contained In	1
Class	module
Parent Relative Position	1
Name	“RF IC”
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.4 Base Band Board

Attribute	Value
Inventory Index	4
Descriptor	“Siklu EH-1200 Base Band Board”
Contained In	1
Class	container
Parent Relative Position	2
Name	“Base Band Board”
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	<to be read in runtime>
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.5 Modem

Attribute	Value
Inventory Index	5
Descriptor	“Siklu EH-1200 Modem”
Contained In	4
Class	module
Parent Relative Position	0
Name	“Modem”
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.6 FPGA

Attribute	Value
Inventory Index	6
Descriptor	“Siklu EH-1200 FPGA”
Contained In	4
Class	module
Parent Relative Position	1
Name	“FPGA”
Hardware Revision	empty
Firmware Revision	<to be read in runtime>
Software Revision	empty
Serial Number	empty
Manufacturer Name	empty
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.7 CPLD

Attribute	Value
Inventory Index	7
Descriptor	“Siklu EH-1200 CPLD”
Contained In	4
Class	module
Parent Relative Position	2
Name	“CPLD”
Hardware Revision	empty
Firmware Revision	<to be read in runtime>
Software Revision	empty
Serial Number	empty
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.8.3.8 SFP

Attribute	Value
Inventory Index	7
Descriptor	“Siklu EH-1200 SFP”
Contained In	4
Class	module
Parent Relative Position	3
Name	“SFP”
Hardware Revision	<to be read in runtime>
Firmware Revision	empty
Software Revision	empty
Serial Number	empty
Manufacturer Name	<to be read in runtime>
Model Name	empty
Field Replaceable Unit Indicator	replaceable

11.8.3.9 Boot

Attribute	Value
Inventory Index	8
Descriptor	“Siklu EH-1200 Boot”
Contained In	4
Class	module
Parent Relative Position	5
Name	“Boot”
Hardware Revision	empty
Firmware Revision	empty
Software Revision	<to be read in runtime>
Serial Number	empty
Manufacturer Name	“Siklu”
Model Name	empty
Field Replaceable Unit Indicator	not-replaceable

11.9 Radio Object Attributes

11.9.1 RF Object Attributes

This section lists configurable RF attributes (Table 11-3) and read-only RF attributes (Table 11-5) separately.

Table 11-3 Configurable RF Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Number of Channels (num-of-channels)	The maximum allowed bandwidth, expressed in MHz.	rfNumOfChannels (1.3.6.1.4.1.31926.2.1.1.2)	1..2	2
Operational Frequency (frequency)	The frequency at which the RF operates, expressed in MHz.	rfOperationalFrequency (1.3.6.1.4.1.31926.2.1.1.4)	50000..80000	74000
Role (role)	The current role of the RF device.	rfRole (1.3.6.1.4.1.31926.2.1.1.5)	master, slave	master
Mode Selector (mode)	The current RF device operating mode. When static mode is specified, only certain sub-parameter combinations will produce a valid result. When an invalid combination is specified on the command line, the CLI will respond with: “the modulation does not exist in the modulation table.”	rfModeSelector (1.3.6.1.4.1.31926.2.1.1.6)	adaptive, static, alignment When static mode is specified, additional sub-parameters are used to define additional relevant operating characteristics, as shown in Table 11-4.	adaptive
CINR Low (cinr-low)	The lowest acceptable value for CINR, expressed in decibels (dB).	rfCinrLow (1.3.6.1.4.1.31926.2.1.1.13)	-128..127	0
CINR Interval (cinr-interval)	The interval used to determine the value for CINR, expressed in milliseconds.	rfCinrInterval (1.3.6.1.4.1.31926.2.1.1.15)	0..2000	0
RSSI Interval (rssi-interval)	The interval used to determine the value for RSSI, expressed in milliseconds.	rfRssiInterval(1.3.6.1.4.1.31926.2.1.1.16)	0..2000	0
RX Link ID (rx-link-id)	The RF receive link ID.	rfRxLinkId (1.3.6.1.4.1.31926.2.1.1.22)	Varies	0
TX Link ID (tx-link-id)	The RF transmit link ID.	rfTxLinkId (1.3.6.1.4.1.31926.2.1.1.23)	Varies	0
Transmit Asymmetry (tx-asymmetry)	Percentage of the TX part in the airframe.		integer. CLI syntax is {10tx-90rx |25tx-75rx | 50tx-50rx | 75tx-25rx | 90tx-10rx}.	50tx-50rx

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Lowest Modulation	Dropping below the Lowest Mode causes RF link failure, wherein: mod = Modulation type. {QPSK, QAM16, QAM64} scnum = The number of subchannels [1..4] rep = Repetition {1, 2, 4} fec = FEC {0.5, 0.67, 0.8} frame = The frame number to be used for the execution of the new modulation (only in static mode) The mode must be present in the Modulation Table			

Table 11-4 Static Mode Sub-Parameters

Argument	Description	Values	SNMP Reference
modu	modulation	QPSK, QAM16, QAM64	rfModulationType (1.3.6.1.4.1.31926.2.1.1.7)
num-subch	Number of subchannels	1..4	rfNumOfSubchannels (1.3.6.1.4.1.31926.2.1.1.8)
repete	Repetitions	1, 2, 4	rfNumOfRepetitions (1.3.6.1.4.1.31926.2.1.1.9)
fec	FEC rate	0.5, 0.67, 0.8	rfFecRate (1.3.6.1.4.1.31926.2.1.1.10)

Table 11-5 Read-Only RF Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Channel Width (channel-width)	The channel width, expressed in MHz.	rfChannelWidth (1.3.6.1.4.1.31926.2.1.1.3)	250	N/A
RX State (rx-state)	The current state of the RF receive link.	rfRxState (1.3.6.1.4.1.31926.2.1.1.25)	1= Sync 2= Search countdown 3= Found countdown 4= Normal	N/A
TX State (tx-state)	The current state of the RF transmit link.	rfTxState (1.3.6.1.4.1.31926.2.1.1.24)	1= Sync 2= Search countdown 3= Found countdown 4= Normal	N/A
Operational State (operational)	The current operating state of the RF device.	rfOperationalState (1.3.6.1.4.1.31926.2.1.1.17)	up, down	N/A
Average CINR	Average carrier to interference noise ratio [-6..30] This object is only accessible via SNMP.	rfAverageCinr (1.3.6.1.4.1.31926.2.1.1.18)	integer	
Average RSSI	Average received signal strength indication, measured in DB. [-100..-60] This object is only accessible via SNMP.	rfAverageRssi (1.3.6.1.4.1.31926.2.1.1.19)	integer	

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
RF Temperature (rf-temperature)	The current temperature of the RF device.	rfTemperature (1.3.6.1.4.1.31926.2.1.1.26)	Varies	N/A

11.9.2 Radio Statistics

Table 11-6 Radio Statistic Descriptions

Attribute (CLI Attribute Name)	Description	SNMP Object ID
Incoming Octets (in-octets)	The total number of octets received from the RF link.	rfInOctets (1.3.6.1.4.1.31926.2.2.1.1)
Incoming Idle Octets (in-idle-octets)	The total number of octets received from the RF link while idle.	rfInIdleOctets (1.3.6.1.4.1.31926.2.2.1.2)
Incoming Good Octets (in-good-octets)	The number of good octets received from the RF link.	rfInGoodOctets (1.3.6.1.4.1.31926.2.2.1.3)
Incoming Erroneous Octets (in-errored-octets)	The number of received erred octets from the RF link.	rfInErroredOctets (1.3.6.1.4.1.31926.2.2.1.4)
Outgoing Octets (out-octets)	The total number of octets transmitted to the RF link.	rfOutOctets (1.3.6.1.4.1.31926.2.2.1.5)
Outgoing Idle Octets (out-idle-octets)	The total number of octets transmitted to the RF link while idle.	rfOutIdleOctets (1.3.6.1.4.1.31926.2.2.1.6)
Incoming Packets (in-pkts)	The total number of packets received from the RF link.	rfInPkts (1.3.6.1.4.1.31926.2.2.1.7)
Incoming Good Packets (in-good-pkts)	The total number of good packets received from the RF link.	rfInGoodPkts (1.3.6.1.4.1.31926.2.2.1.8)
Incoming Erroneous Packets (in-errored-pkts)	The total number of erred packets received from the RF link.	rfInErroredPkts (1.3.6.1.4.1.31926.2.2.1.9)
Incoming Lost Packets (in-lost-pkts)	The total number of lost packets received from the RF link.	rfInLostPkts (1.3.6.1.4.1.31926.2.2.1.10)
Outgoing Packets (out-pkts)	The total number of packets transmitted to the RF link.	rfOutPkts (1.3.6.1.4.1.31926.2.2.1.11)

Table 11-7 Statistics History for the RF Object

usrHistoryObjectIndex	usrHistoryObjectVariable
1	rfInOctets (1.3.6.1.4.1.31926.2.2.1.1)
2	rfInIdleOctets (1.3.6.1.4.1.31926.2.2.1.2)
3	rfInGoodOctets (1.3.6.1.4.1.31926.2.2.1.3)
4	rfInErroredOctets (1.3.6.1.4.1.31926.2.2.1.4)
5	rfOutOctets (1.3.6.1.4.1.31926.2.2.1.5)

usrHistoryObjectIndex	usrHistoryObjectVariable
6	rfOutIdleOctets (1.3.6.1.4.1.31926.2.2.1.6)
7	rfInPkts (1.3.6.1.4.1.31926.2.2.1.7)
8	rfInGoodPkts (1.3.6.1.4.1.31926.2.2.1.8)
9	rfInErroredPkts (1.3.6.1.4.1.31926.2.2.1.9)
10	rfInLostPkts (1.3.6.1.4.1.31926.2.2.1.10)
11	rfOutPkts (1.3.6.1.4.1.31926.2.2.1.11)

11.10 Encryption Object Attributes

Table 11-8 Encryption Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Encryption	Encryption Mode. This attribute is only visible to an admin user.		{disabled | static-key}	disabled	Encryption
Static Key	This is the only key (this is to say the current key and next key are always the same and equal to this configured key.		string of 32 hexadecimal digits	92E3C28020570998E74B41C06A58BB40	Static Key

11.11 Connectivity Fault Management (CFM) Object Attributes

11.11.1 Maintenance Domain (MD) Object Attributes

Table 11-9 MD Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for this MD when the management entity wants to create a new entry in that table. An MD Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP or LTR DB.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
Name (name)	Each MD has a unique name. This facilitates easy identification of administrative responsibility for each Maintenance Domain.	dot1agCfmMdName (1.3.111.2.802.1.1.8.1.5.2.1.1)	{dns-like | mac-and-unit | string} "<name according to format>"	RC	Empty
Format (format)	Represents a type (and the resulting format) of the MD Name. Can be up to 256 characters.	dot1agCfmMdFormat (1.3.111.2.802.1.1.8.1.5.2.1.2)	{dns-like | mac-and-unit | string} "<name according to format>"	RC	String
Level (level)	Represents the Maintenance Domain Level.	dot1agCfmMdMdLevel (1.3.111.2.802.1.1.8.1.5.2.1.4)	0..7	RC	0
MHF Creation (mhf-creation)	Enumerated value indicating whether the management entity can create MHFs (MIP Half Function) for this MD.	dot1agCfmMdMhfCreation (1.3.111.2.802.1.1.8.1.5.2.1.5)	{none | default | explicit}	RC	None
MHF ID Permission (mhf-permission)	Enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this MD.	dot1agCfmMdMhfIdPermission (1.3.111.2.802.1.1.8.1.5.2.1.6)	{none | chassis | mgmg | chassis-mgmg}	RC	None

11.11.2 Maintenance Association (MA) Object Attributes

Table 11-10 MA Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table MD Domain when the management entity wants to create a new entry in that table. Entering the MD Index for an MA enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1 .5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1 .6.1.1.1)		N/A	
MA Format (format)	A value that represents a type (and the resulting format) of the MD Name.	dot1agCfmMaNetFor mat(1.3.111.2.802.1. 1.8.1.6.1.1.2)	{vid | string | vpnid}	RW	vid
MA Name (name)	The short MA name. The type/format of this object is determined by the value of the dot1agCfmMaNetNameType object. This name must be unique within a MD.	dot1agCfmMaNetNa me (1.3.111.2.802.1.1.8.1 .6.1.1.3)	{vid | string | vpnid} "<name according to format>"	RC	1
Interval (interval)	The interval to be used between CCM transmissions by all MEPs in the MA.	1.3.111.2.802.1.1.8.1. 6.1.1.4 (dot1agCfmMaNetCc mInterval)	{3.3ms | 10ms | 100ms | 1s | 10s | 1min | 10min}	RC	1s

11.11.3 Component MA Object Attributes

Table 11-11 Component MA Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Component	The bridge component within the system to which the information in this dot1agCfmMaCompEntry applies. The component must be defined in the Bridge component table (*Table 11-22*).	ieee8021CfmMaCom ponentId (1.3.111.2.802.1.1.8.1 .6.4.1.1)	component <comp-id-list>	N/A	

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. Entering the MD Index for a Component MA enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
Service Selector (vlan)	Service Selector identifier to which the MP is attached, or 0, if none. The type of the Service Selector is defined by the value of ieee8021CfmMaCompPrimarySelectorType. In the current implementation the type is always VLAN ID. Thus the Service Selector is the Primary VLAN ID with which the Maintenance Association is associated, or 0 if the MA is not attached to any VID. The VLAN must be defined in the VLAN Table (*Table 11-28*).	ieee8021CfmMaCompPrimarySelectorOrNone (1.3.111.2.802.1.1.8.1.6.4.1.3)	{none | 1..4094}	RC	None
MHF Creation (mhf-creation)	Enumerated value indicating whether the management entity can create MHFs (MIP Half Function) for this MA.	ieee8021CfmMaCompMhfCreation (1.3.111.2.802.1.1.8.1.6.4.1.4)	{mhf-creation none | default | explicit | defer}	RC	defer
MHF ID Permission (mhf-permission)	Enumerated value indicating what, if anything, is to be included in the Sender ID TLV (21.5.3) transmitted by MPs configured in this MA.	ieee8021CfmMaCompIdPermission (1.3.111.2.802.1.1.8.1.6.4.1.5)	{mhf-permission none | chassis | mgmg | chassis-mgmg}	RC	None

11.11.4 Maintenance End Point (MEP) Object Attributes

This section includes separate tables for configurable MEP object attributes (*Table 11-12*) and read-only MEP object attributes (*Table 11-13*).

Table 11-12 Configurable MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. Entering the MD Index for a MEP enables use of the common command structure.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An MA Index entry cannot be deleted if it is used as the key in MA, MEP, Received CCM Presentation, Peer MEP Create or LTR DB.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. Adding an entry with a specific MEPID creates associated entries in the Peer MEP DB. Similarly, deleting a specific MEPID entry causes deletion of association entries in the Peer MEP DB.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC	1
Interface (interface)	The index of the interface either of a Bridge Port, or an aggregated IEEE 802.1 link within a Bridge Port, to which the MEP is attached. The component associated with the MEP interface must exist in the Component MA Table. In addition, only one MEP can be defined for the same combination of Interface, Direction and Primary VLAN.	1.3.111.2.802.1.1.8.1.7.1.1.2 (dot1agCfmMepIfIndex)	{eth0 | eth1 | eth2 | host}	RC	eth1
Direction (dir)	The direction in which the MEP is facing on the Bridge Port. Only one MEP can be defined for the same combination of Interface, Direction and Primary VLAN.	1.3.111.2.802.1.1.8.1.7.1.1.3 (dot1agCfmMepDirection)	{up | down}	RC	down

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
Primary VLAN (vlan)	An integer indicating the Primary VID of the MEP. A value of 0 indicates that either the Primary VID is that of the MEP's MA, or that the MEP's MA is not associated with any VID. The associated VLAN must be defined in the VLAN Table (*Table 11-28*). In addition, only one MEP can be defined for the same combination of Interface, Direction and Primary VLAN.	1.3.111.2.802.1.1.8.1.7.1.1.4 (dot1agCfmMepPrimaryVid)	0..4094	RC	0
Administrative State (admin-state)	The administrative state of the MEP. True (active) indicates that the MEP is to function normally; False (inactive) indicates that the MEP is to cease functioning.	1.3.111.2.802.1.1.8.1.7.1.1.5 (dot1agCfmMepActive)	{active | inactive}	RC	Inactive
CCI (cci)	If set to True, the MEP will generate CCM messages.	1.3.111.2.802.1.1.8.1.7.1.1.7 (dot1agCfmMepCciEnabled)	{enabled | disabled}	RC	disabled
Message Priority (msg-prio)	The priority value for CCMs and LTMs transmitted by the MEP. The default value is the highest priority value allowed passing through the Bridge Port for any of the MEP VIDs. The Management Entity can obtain the default value for this variable from the priority regeneration table by extracting the highest priority value in this table on this MEP's Bridge Port (1 is lowest, followed by 2, then 0, then 3-7).	1.3.111.2.802.1.1.8.1.7.1.1.8 (dot1agCfmMepCcmLtmPriority)	0..7	RC	0
Lowest Primary Defect (low-defect)	An integer specifying the lowest priority defect that is allowed to generate a fault alarm.	1.3.111.2.802.1.1.8.1.7.1.1.10 (dot1agCfmMepLowPrDef)	{all-def | mac-rem-err-xcon | rem-err-xcon | err-xcon | xcon | no-xcon}	RC	mac-rem-err-xcon
Alarm Time (alarm-time)	The time that a defect must be present before a fault alarm is issued.	1.3.111.2.802.1.1.8.1.7.1.1.11 (dot1agCfmMepFngAlarmTime)	250..000	RC	250
Reset Time (reset-time)	The time that a defect must be absent before resetting a fault alarm.	1.3.111.2.802.1.1.8.1.7.1.1.12 (dot1agCfmMepFngResetTime)	250..1000	RC	1000

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
LBM Destination MAC Address (lbm-dst-mac)	A unicast destination MAC address specifying the target MAC address field to be transmitted. This address will be used if the value for the column dot1agCfmMepTransmitLbmDestIsMepId is False.	1.3.111.2.802.1.1.8.1.7.1.1.27 (dot1agCfmMepTransmitLbmDestMacAddress)	Mac address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RC	00-00-00-00-00-00
LBM Destination MEPID (lbm-dst-mepid)	The MA End Point Identifier of another MEP in the same MA to which the LBM is to be sent. This address will be used if the value of the column dot1agCfmMepTransmitLbmDestIsMepId is True.	1.3.111.2.802.1.1.8.1.7.1.1.28 (dot1agCfmMepTransmitLbmDestMepId)	Integer	RC	0
LBM Destination Type (lbm-dst-type)	The destination type indicator for purposes of Loopback transmission, either the unicast destination MAC address of the target MEP or the MEPID of the target MEP.	1.3.111.2.802.1.1.8.1.7.1.1.29 (dot1agCfmMepTransmitLbmDestIsMepId)	{mac | mepid}	RC	mac
Number of LBMs to Transmit (lbm-tx-num)	The number of Loopback messages to be transmitted.	1.3.111.2.802.1.1.8.1.7.1.1.30 (dot1agCfmMepTransmitLbmMessages)	1..1024	RC	1
LBM Data TLV (lbm-tx-data)	An arbitrary amount of data to be included in the Data TLV, if the Data TLV is selected to be sent.	1.3.111.2.802.1.1.8.1.7.1.1.31 (dot1agCfmMepTransmitLbmDataTlv)	String of hexadecimal digits. Two digits constitute an octet thus the length must be even.	RC	Empty String
LBM Transmit VLAN Priority (lbm-tx-prio)	Priority. 3-bit value to be used in the VLAN tag, if present in the transmitted frame.	1.3.111.2.802.1.1.8.1.7.1.1.32 (dot1agCfmMepTransmitLbmVlanPriority)	0..7	RC	0
LBM Transmit VLAN Drop Eligibility (lbm-tx-drop)	Drop Enable bit value to be used in the VLAN tag, if present in the transmitted frame. For more information about VLAN Drop Enable, see IEEE 802.1ad.	1.3.111.2.802.1.1.8.1.7.1.1.33 (dot1agCfmMepTransmitLbmVlanDropEnable)	{enable | disable}	RC	Enable
LTM Destination MAC Address (ltm-dst-mac)	A unicast destination MAC address specifying the target MAC Address Field to be transmitted. This address will be used if the value of the column dot1agCfmMepTransmitLtmTargetIsMepId is False.	1.3.111.2.802.1.1.8.1.7.1.1.38 (dot1agCfmMepTransmitLtmTargetMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RC	00-00-00-00-00-00

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
LTM Destination MEPID (ltm-dst-mepid)	The MA End Point Identifier of another MEP in the same MA to which the LTM is to be sent. This address will be used if the value of the column dot1agCfmMepTransmitLtmTargetIsMepId is True.	1.3.111.2.802.1.1.8.1.7.1.1.39 (dot1agCfmMepTransmitLtmTargetIsMepId)	0..8191	RC	0
LTM Destination Type (ltm-dst-type)	The destination type indicator for purposes of LTM transmission, either the unicast destination MAC address of the target MEP or the MEPID of the target MEP.	1.3.111.2.802.1.1.8.1.7.1.1.40 dot1agCfmMepTransmitLtmTargetIsMepId	{mac | mepid}	RC	mac
LTM Transmit TTL (ltm-tx-ttl)	The TTL field indicates the number of hops remaining to the LTM. Decremented by 1 by each Linktrace Responder that handles the LTM. The value returned in the LTR is one less than that received in the LTM. If the LTM TTL is 0 or 1, the LTM is not forwarded to the next hop, and if 0, no LTR is generated.	1.3.111.2.802.1.1.8.1.7.1.1.41 (dot1agCfmMepTransmitLtmTtl)	0..250	RC	64
Transmit LBM Status (lbm-tx-status)	A Boolean flag set to True by the Bridge Port to indicate that another LBM may be transmitted. Reset to False by the MEP Loopback Initiator State Machine. Setting the status to True (tx-pending) will initiate LBM sending. The number of LBM sent is defined by the Number of LBM to Transmit. After transmitting the specified number of LBM the value automatically changes to False (tx-idle). Note that if the Number of LBM to Transmit is zero the status turns to False (tx-idle) immediately.	1.3.111.2.802.1.1.8.1.7.1.1.26 (dot1agCfmMepTransmitLbmStatus)	{tx-pending, tx-idle}	RC	tx-idle
Transmit LTM Status (ltm-tx-status)	A Boolean flag set to True by the Bridge Port to indicate that another LTM may be transmitted. Reset to False by the MEP Linktrace Initiator State Machine. Setting the status to True (tx-pending) will initiate LTM sending. Only one message is sent, after which the value automatically changes to False (tx-idle). Note that if the Number of LTM to Transmit is zero the status turns to False (tx-idle) immediately.	1.3.111.2.802.1.1.8.1.7.1.1.36 (dot1agCfmMepTransmitLtmStatus)	{tx-pending, tx-idle}	RC	tx-idle

Table 11-13 Read-Only MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax
Fault Notification Generator State (fng-state)	The current state of the MEP Fault Notification Generator state machine. See 802.1ag clauses 12.14.7.1.3:f and 20.35.	1.3.111.2.802.1.1.8.1.7.1.1.6 (dot1agCfmMepFngState)	{reset | defect | report-defect | defect-reported | defect-clearing}
MEP MAC Address (mac)	MAC address of the MEP.	1.3.111.2.802.1.1.8.1.7.1.1.9 (dot1agCfmMepMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)
Highest Priority Defect (high-defect)	The highest priority defect that has been present since the MEPs Fault notification Generator State Machine was last in the reset state.	1.3.111.2.802.1.1.8.1.7.1.1.13 (dot1agCfmMepHighestPrDefect)	{none | rdi-ccm | mac-status | remote-ccm | error-ccm | xcon-ccm}
MEP Defects (defects)	A vector of Boolean error conditions from IEEE 802.1ag Table 20-1, any of which may be true. A MEP can detect and report a number of defects, and multiple defects can be present at the same time.	1.3.111.2.802.1.1.8.1.7.1.1.14 (dot1agCfmMepDefects)	Any combination of: {rdi-ccm, mac-status, remote-ccm, error-ccm, xcon-ccm}
CCM Sequence Errors (ccm-seq-errors)	The total number of out-of-sequence CCMs that have been received from all remote MEPs.	1.3.111.2.802.1.1.8.1.7.1.1.17 (dot1agCfmMepCcmSequenceErrors)	Integer
CCM Transmit Counter (ccm-tx)	Total number of Continuity Check messages transmitted.	1.3.111.2.802.1.1.8.1.7.1.1.18 (dot1agCfmMepCciSentCcms)	Integer
LBM Transmit Result (lbm-tx-result)	Indicates the result of the operation.	1.3.111.2.802.1.1.8.1.7.1.1.34 (dot1agCfmMepTransmitLbmResultOK)	{ok | not-ok}
LBM Transmit Sequence Number (lbm-tx-sn)	The Loopback Transaction Identifier (dot1agCfmMepNextLbmTransId) of the first LBM sent. The value returned is undefined if dot1agCfmMepTransmitLbmResultOK is False.	1.3.111.2.802.1.1.8.1.7.1.1.35 (dot1agCfmMepTransmitLbmSeqNumber)	Integer
LBM Next Sequence Number (lbm-next-sn)	Next sequence number/transaction identifier to be sent in a Loopback message. This sequence number can be zero when it wraps around.	1.3.111.2.802.1.1.8.1.7.1.1.19 (dot1agCfmMepNextLbmTransId)	Integer
Incoming In Order LBR Counter (lbr-in-order)	Total number of valid, in-order Loopback Replies received.	1.3.111.2.802.1.1.8.1.7.1.1.20 (dot1agCfmMepLbrIn)	Integer
Incoming Out of Order LBR Counter (lbr-out-of-order)	The total number of valid, out-of-order Loopback Replies received.	1.3.111.2.802.1.1.8.1.7.1.1.21 (dot1agCfmMepLbrInOutOfOrder)	Integer
Transmit LBR Counter (lbr-tx)	Total number of Loopback Replies transmitted.	1.3.111.2.802.1.1.8.1.7.1.1.25 (dot1agCfmMepLbrOut)	Integer
LTM Next Sequence Number (ltm-next-sn)	Next transaction identifier/sequence number to be sent in a Linktrace message. This sequence number can be zero when it wraps around.	1.3.111.2.802.1.1.8.1.7.1.1.23 (dot1agCfmMepLtmNextSeqNumber)	Integer

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax
Unexpected Incoming LTR (ltr-unexpected)	The total number of unexpected LTRs received.	1.3.111.2.802.1.1.8.1.7.1.1.24 (dot1agCfmMepUnexpLtrIn)	Integer
LTM Transmit Result (ltm-tx-result)	Indicates the result of the operation.	1.3.111.2.802.1.1.8.1.7.1.1.42 (dot1agCfmMepTransmitLtmResult)	{ok | not-ok}
LTM Transmit Sequence Number (ltm-tx-sn)	The LTM Transaction Identifier (dot1agCfmMepLtmNextSeqNumber) of the LTM sent. The value returned is undefined if dot1agCfmMepTransmitLtmResult is False.	1.3.111.2.802.1.1.8.1.7.1.1.43 (dot1agCfmMepTransmitLtmSeqNumber)	Integer

11.11.5 CCM Message Object Attributes

Table 11-14 CCM Message Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access	Default
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A	
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A	
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC	1
Last Error Condition CCM (last-error-ccm)	The last-received CCM that triggered an DefErrorCCM fault.	1.3.111.2.802.1.1.8.1.7.1.1.15 (dot1agCfmMepErrorCcmLastFailure)		RO	
Last Xcon Condition CCM (last-xcon-ccm)	The last-received CCM that triggered an DefErrorCCM fault.	1.3.111.2.802.1.1.8.1.7.1.1.16 (dot1agCfmMepXconCcmLastFailure)		RO	

11.11.6 Peer MEP Object Attributes

Table 11-15 Peer MEP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A
Peer MEPID	Integer identifying a specific Peer MA End Point.	dot1agCfmMaMepListIdentifier (1.3.111.2.802.1.1.8.1.6.3.1.1)	1..8191	N/A

11.11.7 Peer MEP Database Attributes

Table 11-16 Peer MEP Database Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Peer MEPID	Integer identifying a specific Peer Maintenance Association End Point.	1.3.111.2.802.1.1.8.1.7.3.1.1 (dot1agCfmMepDbRMepIdentifier)	1..8191	N/A
Peer MEP State (state)	The operational state of the remote MEP IFF State machines. This state machine monitors the reception of valid CCMs from a remote MEP with a specific MEPID. It uses a timer that expires in 3.5 times the length of time indicated by the dot1agCfmMaNetCcmInterval object.	1.3.111.2.802.1.1.8.1.7.3.1.2 (dot1agCfmMepDbRMepState)	{idle | start | failed | ok}	RO
Peer MEP Failed OK Time (failed-ok-time)	The time (SysUpTime) at which the peer MEP state machine last entered either the Failed or OK state.	1.3.111.2.802.1.1.8.1.7.3.1.3 (dot1agCfmMepDbRMepFailedOkTime)	ddd:hh:mm:ss, wherein ddd – decimal integer representing days (it may include arbitrary number of digits), hh – two-digit decimal integer representing hours of day [0..23], mm – two-digit decimal integer representing minutes of hour [0..59], ss – two-digit decimal integer representing seconds of minute [0..59].	RO
Peer MEP MAC Address (mac)	The MAC address of the remote MEP.	1.3.111.2.802.1.1.8.1.7.3.1.4 (dot1agCfmMepDbMacAddress)	MAC address in the form NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RO
Remote Defect Indication (rdi)	State of the RDI bit in the last received CCM. On corresponds to True.	1.3.111.2.802.1.1.8.1.7.3.1.5 (dot1agCfmMepDbRdi)	{on | off}	RO
Peer Port Status (port-status)	An enumerated value of the Port status TLV received in the last CCM from the remote MEP or the default value psNoPortStateTLV indicating either no CCM has been received, or that no port status TLV was received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.6 (dot1agCfmMepDbPortStatusTlv)	{none | blocked | up}	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Peer Interface Status (if-status)	An enumerated value of the Interface status TLV received in the last CCM from the remote MEP or the default value isNoInterfaceStatus TLV indicating either no CCM has been received, or that no interface status TLV was received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.7 (dot1agCfmMepDbInterfaceStatusTlv)	{none | up | down | testing | unknown | dormant | not-present | lower-layer-down}	RO
Peer Chassis ID Subtype (chassis-id-subtype)	This object specifies the format of the Chassis ID received in the last CCM.	1.3.111.2.802.1.1.8.1.7.3.1.8 (dot1agCfmMepDbChassisIdSubtype)	{chassis-comp | if-alias | port-comp | mac | net-addr | if-name}	RO
Peer Chassis ID (chassis-id)	The Chassis ID. The format of this object is determined by the value of the dot1agCfmLtrChassisIdSubtype object.	1.3.111.2.802.1.1.8.1.7.3.1.9 (dot1agCfmMepDbChassisId)	Hexadecimal string	RO
Management Address Domain (mng-addr-domain)	The TDomain that identifies the type and format of the related dot1agCfmMepDbManAddress object, used to access the SNMP agent of the system transmitting the CCM. Received in the CCM Sender ID TLV from that system.	1.3.111.2.802.1.1.8.1.7.3.1.10 (dot1agCfmMepDbManAddressDomain)	{snmp-udp, snmp-ieee802}	RO
Management Address (mng-addr)	The TAddress that can be used to access the SNMP agent of the system transmitting the CCM, received in the CCM Sender ID TLV from that system. If the related object dot1agCfmMepDbManAddressDomain contains the value 'zeroDotZero', this object dot1agCfmMepDbManAddress must have a zero-length OCTET STRING as a value.	1.3.111.2.802.1.1.8.1.7.3.1.11 (dot1agCfmMepDbManAddress)	IP Address – dotted notation. MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO

11.11.8 LTR Object Attributes

Table 11-17 LTR Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
MD Index	Value to be used as the index of the MA table entries for the MD when the management entity wants to create a new entry in that table. An entry cannot be created if a corresponding MD Index does not exist.	dot1agCfmMdIndex (1.3.111.2.802.1.1.8.1.5.2.1.1)	Integer	N/A
MA Index	Index of the MA table (dot1agCfmMdMaNextIndex), which needs to be inspected to find an available index for row-creation. An entry cannot be created if a corresponding MA Index does not exist.	dot1agCfmMaIndex (1.3.111.2.802.1.1.8.1.6.1.1.1)		N/A
MEPID	An integer that is unique for all the MEPs in the same MA that identifies a specific MA End Point. An entry cannot be created if a corresponding MEPID does not exist.	1.3.111.2.802.1.1.8.1.7.1.1.1 (dot1agCfmMepIdentifier)	integer	RC
LTR SN	Transaction identifier/sequence number returned by a previous transmit linktrace message command, indicating which LTM's response is going to be returned.	1.3.111.2.802.1.1.8.1.7.2.1.1 (dot1agCfmLtrSeqNumber)	Integer	N/A
LTR Received TTL (rx-ttl)	TTL field value for a returned LTR	1.3.111.2.802.1.1.8.1.7.2.1.3 (dot1agCfmLtrTtl)	0..250	RO
LTR Forwarded Indicator (ltr-forward)	Indicates if a LTM was forwarded by the responding MP, as returned in the 'FwdYes' flag of the flags field.	1.3.111.2.802.1.1.8.1.7.2.1.4 (dot1agCfmLtrForwarded)	{forwarded | not-forwarded}	RO
LTR Relay Indicator (relay-action)	Possible values the Relay action field can take.	1.3.111.2.802.1.1.8.1.7.2.1.8 (dot1agCfmLtrRelay)	{hit | fdb | mpdb}	RO
LTR Chassis ID Subtype (chassis-id-subtype)	This object specifies the format of the Chassis ID returned in the Sender ID TLV of the LTR, if any.	1.3.111.2.802.1.1.8.1.7.2.1.9 (dot1agCfmLtrChassisIdSubtype)	{chassis-comp | if-alias | port-comp | mac | net-addr | if-name}	RO
LTR Chassis ID (chassis-id)	The Chassis ID returned in the Sender ID TLV of the LTR, if any. The format of this object is determined by the value of the dot1agCfmLtrChassisIdSubtype object.	1.3.111.2.802.1.1.8.1.7.2.1.10 (dot1agCfmLtrChassisId)	Format in accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
LTR Management Address Domain (mng-addr-domain)	The TDomain that identifies the type and format of the related dot1agCfmMepDbManAddress object, used to access the SNMP agent of the system transmitting the LTR.	1.3.111.2.802.1.1.8.1.7.2.1.11 (dot1agCfmLtrManAddressDomain)	{snmp-udp, snmp-ieee802}	RO
LTR Management Address (mng-addr)	The TAddress that can be used to access the SNMP agent of the system transmitting the LTR, received in the LTR Sender ID TLV from that system.	1.3.111.2.802.1.1.8.1.7.2.1.12 (dot1agCfmLtrManAddress)	IP Address – dotted notation. MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Ingress Action (ingr-action)	The value returned in the Ingress Action Field of the LTM. The value ingNoTlv(0) indicates that no Reply Ingress TLV was returned in the LTM.	1.3.111.2.802.1.1.8.1.7.2.1.13 (dot1agCfmLtrIngress)	{none | ok | down | blocked | vid}	RO
LTR Ingress MAC Address (ingr-mac)	MAC address returned in the ingress MAC address field. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.14 (dot1agCfmLtrIngressMac)	MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Ingress Port ID Subtype (ingr-port-id-subtype)	Format of the Ingress Port ID. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.15 (dot1agCfmLtrIngressPortIdSubtype)	{if-alias | port-comp | mac | net-addr | if-name | agent-circuit-id | local}	RO
LTR Ingress Port ID (ingr-port-id)	Ingress Port ID. The format of this object is determined by the value of the dot1agCfmLtrIngressPortIdSubtype object. If the dot1agCfmLtrIngress object contains the value ingNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.16 (dot1agCfmLtrIngressPortId)	Format in accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	RO
LTR Egress Action (egr-action)	The value returned in the Egress Action Field of the LTM. The value egrNoTlv(0) indicates that no Reply Egress TLV was returned in the LTM.	1.3.111.2.802.1.1.8.1.7.2.1.17 (dot1agCfmLtrEgress)	{none | ok | down | blocked | vid}	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
LTR Egress MAC Address (egr-mac)	MAC address returned in the ingress MAC address field. If the dot1agCfmLtrIngress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.18 (dot1agCfmLtrEgressMac)	MAC Address - NN-NN-NN-NN-NN-NN, where N is a hexadecimal number (for example 00-AF-DD-1E-2D-A3), the rest – hexadecimal string	RO
LTR Egress Port ID Subtype (egr-port-id-subtype)	Format of the Egress Port ID. If the dot1agCfmLtrEgress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.19 (dot1agCfmLtrEgressPortIdSubtype)	{if-alias | port-comp | mac | net-addr | if-name | agent-circuit-id | local}	RO
LTR Ingress Port ID (egr-port-id)	Egress Port ID. The format of this object is determined by the value of the dot1agCfmLtrEgressPortIdSubtype object. If the dot1agCfmLtrEgress object contains the value ergNoTlv(0), then the contents of this object are meaningless.	1.3.111.2.802.1.1.8.1.7.2.1.20 (dot1agCfmLtrEgressPortId)	Format in accordance with LTR Chassis ID Subtype. A hexadecimal string is used if no format is known.	RO
LTR Terminal MEP (trm-mep)	A boolean value stating whether the forwarded LTM reached a MEP enclosing its MA, as returned in the Terminal MEP flag of the Flags field.	1.3.111.2.802.1.1.8.1.7.2.1.5 (dot1agCfmLtrTerminalMep)	{on | off}	RO
LTR Last Egress Identifier (last-egr-id)	An octet field holding the Last Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Last Egress Identifier identifies the MEP Linktrace Initiator that originated, or the Linktrace Responder that forwarded, the LTM to which this LTR is the response. This is the same value as the Egress Identifier TLV of that LTM.	1.3.111.2.802.1.1.8.1.7.2.1.6 (dot1agCfmLtrLastEgressIdentifier)	8 pairs hexadecimal digits, each pair separated by dashes: NN-NN-NN-NN-NN-NN-NN-NN, for example: 00-00-00-AF-DD-1E-2D-A3	RO

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
LTR Next Egress Identifier (next-egr-id)	An octet field holding the Next Egress Identifier returned in the LTR Egress Identifier TLV of the LTR. The Next Egress Identifier Identifies the Linktrace Responder that transmitted this LTR, and can forward the LTM to the next hop. This is the same value as the Egress Identifier TLV of the forwarded LTM, if any. If the FwdYes bit of the Flags field is false, the contents of this field are undefined, i.e., any value can be transmitted, and the field is ignored by the receiver.	1.3.111.2.802.1.1.8.1.7.2.1.7 (dot1agCfmLtrNextEgressIdentifier)	8 pairs hexadecimal digits, each pair separated by dashes: NN-NN-NN-NN-NN-NN-NN-NN, for example: 00-00-00-AF-DD-1E-2D-A3	RO

11.12 Network Object Attributes

11.12.1 Ethernet Interface Attributes

This section lists configurable Ethernet Interface attributes (Table 11-18) and read-only Ethernet Interface attributes (Table 11-19) separately.

Table 11-18 Configurable Ethernet Interface Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Administrative Status (admin)	The desired operational state of the interface, expressed as an integer. There are no restrictions for adding an interface in the Down state to VLAN egress and untagged lists, or to FDP.	ifAdminStatus (1.3.6.1.2.1.2.2.1.7)	1 = Up (operational) 2 = Down (not operational) When the **set** command is used together with the **admin** attribute, the device will report the administrative status of the device immediately after command execution. For example: **`Interface eth7 admin set down`**	1 (Up)
State Trap (trap)	An integer that indicates whether linkUp/linkDown traps should be generated for this interface.	ifLinkDownTrapEnable (1.3.6.1.2.1.31.1.1.1.14)	1 = Enabled 2 = Disabled	1 = Enabled

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Alias (alias)	A text string containing an 'alias' name for the interface, as assigned by a network manager. This value provides a non-volatile 'handle' for the interface. The value of this attribute must be unique with respect to other interface aliases.	ifAlias (1.3.6.1.2.1.31.1.1.1.18)	Up to 256 characters. When the **set** command is used together with the **alias** attribute, only one interface can be addressed per invocation.	0 length string
Ethernet Type (eth-type)	This object identifier represents the operational type of MAU that the administrator has assigned. If auto-negotiation is not enabled or is not implemented for this MAU, the value of this attribute is used to determine the operational type of the MAU. In such a case, a set command is used to force the MAU into the specified operating mode. If auto-negotiation is implemented and enabled for this MAU, the operational type of the MAU is determined by auto-negotiation, and the value of this attribute denotes the type to which the MAU will automatically revert if/when auto-negotiation is later disabled.	ifMauDefaultType (1.3.6.1.2.1.26.2.1.1.11) Part of ifMauTable (1.3.6.1.2.1.26.2.1)	For possible values, refer to *Table 11-20*.	1000fd

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Auto Negotiation Admin Status (auto-neg)	An integer representing the administrative state of auto-negotiation signaling for the interface. Setting this attribute to enabled causes the auto-negotiation signaling ability of the interface to be operational. Setting this attribute to disabled causes the auto-negotiation signaling ability of the interface to be non-operational, and no auto-negotiation signaling will be performed. In such a case, the MAU type is forced to the value that has been assigned in the **`eth-type`** attribute.	ifMauAutoNegAdminStatus (1.3.6.1.2.1.26.5.1.1.1) Part of ifMauAutoNegTable (1.3.6.1.2.1.26.5.1)	1 = Enabled 2 = Disabled	Enabled
Loopback Mode (loopback-mode)	Loopback mode operation.	N/A	{disabled | external | internal}	Disabled
Loopback Timeout (loopback-timeout)	Loopback timeout, expressed in seconds.	N/A	Integer	Disabled
Alarm Propagation Mode (alarm-propagation)	Alarm propagation mode is used to define system behavior in case of a link failure	N/A	The possible alarm propagation values are: Disabled=No propagation is performed. Backward=The Ethernet link is set to down if the radio link is down or if a “Peer Eth Down” notification has been received at the radio interface. Forward=A “Peer Eth Down” notification is sent to the other end of the radio link if the Ethernet link is down. Both Directions=Both Backward and Forward alarm propagation is performed.	Disabled

Table 11-19 Read-Only Ethernet Interface Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Description (description)	A text string describing the interface. This value generally includes the manufacturer's name, the product name and the interface hardware and software versions.	ifDescr (1.3.6.1.2.1.2.2.1.2)	Variable text	{"Siklu EH-1200 Host"; " Siklu EH-1200 Eth 0"; "Siklu EH-1200 Eth 1"; "Siklu EH-1200 Eth 2"}
MTU Size (mtu)	The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.	ifMtu (1.3.6.1.2.1.2.2.1.4)	9216	9216
MAC Address (mac-addr)	The address of the interface at its protocol sub-layer.	ifPhysAddress (1.3.6.1.2.1.2.2.1.6)	host0 = <mac_base_address> (read from hardware) rf0 = <mac_base_address> + 1 eth1 = <mac_base_address> + 2 eth2 = <mac_base_address> + 3	NN-NN-NN-NN-NN-NN where NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Operational Status (operational)	The current operational state of the interface, expressed as an integer. When this attribute is in the Down state, but the Administrative Status attribute (**admin**) is in the Up state, then a fault condition is presumed to exist on the interface. If the Administrative Status attribute (**admin**) is in the Down state, then the **operational** attribute should also be in the Down state. If the Administrative Status attribute (**admin**) changes to the Up state, then the **operational** attribute should also change to the Up state if the interface is ready to transmit and receive network traffic. it should remain in the Down state if and only if there is a fault condition that prevents the interface from going to the Up state.	ifOperStatus (1.3.6.1.2.1.2.2.1.8)	1 = Up (Ready to pass packets) 2 = Down (Not available for host0)	N/A
Last Change Time (lastChange)	The value of sysUpTime at the time the interface entered its current operational state. If the current operational state was entered prior to the last reinitialization of the local network management subsystem, then the value of this attribute is 0.	ifLastChange (1.3.6.1.2.1.2.2.1.9)	ddd:hh:mm:ss, where: **ddd**=decimal integer representing days (it can be an arbitrary number of digits) **hh**=two-digit decimal integer representing the hours of a day [0..23] **mm**=two-digit decimal integer representing minutes of an hour [0..59] **ss**=two-digit decimal integer representing seconds of a minute [0..59]	N/A
Name (name)	The name of the interface.	ifName (1.3.6.1.2.1.31.1.1.1.1)	host, eth0, eth1, eth2	None

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Default
Connector (connector)	An integer that indicates whether the interface sublayer has a physical connector.	ifConnectorPresent (1.3.6.1.2.1.31.1.1.1.17)	1 =True (Connector is present) 2=False True (Connector is absent)	N/A
Actual Ethernet Type (eth-act-type)	This object identifier represents the operational type of the MAU, as determined by either: The result of the auto-negotiation process, or If auto-negotiation is not enabled or is not implemented for this MAU, then the value that has been assigned in the **`eth-type`** attribute is used.	ifMauType (1.3.6.1.2.1.26.2.1.1.3) Part of ifMauTable (1.3.6.1.2.1.26.2.1)	For possible values, refer to *Table 11-20*.	1000fd

Table 11-20 Ethernet Type Values

Value	Description
10hd	dot3MauType10BaseTHD (1.3.6.1.2.1.26.4.10)
10fd	dot3MauType10BaseTFD (1.3.6.1.2.1.26.4.11)
100hd	dot3MauType100BaseTXHD (1.3.6.1.2.1.26.4.15)
100fd	dot3MauType100BaseTXFD (1.3.6.1.2.1.26.4.16)
1000hd	dot3MauType1000BaseTHD (1.3.6.1.2.1.26.4.29)
1000fd	dot3MauType1000BaseTFD (1.3.6.1.2.1.26.4.30)
1000sxhd	dot3MauType1000BaseXHD (1.3.6.1.2.1.26.4.21)
1000sxfd	dot3MauType1000BaseXFD (1.3.6.1.2.1.26.4.22)
1000lxhd	dot3MauType1000BaseXHD (1.3.6.1.2.1.26.4.21)
1000lxfd	dot3MauType1000BaseXFD (1.3.6.1.2.1.26.4.22)

11.12.2 Ethernet Statistic Descriptions

Table 11-21 Ethernet Statistics

Attribute (CLI Attribute Name)	Description	SNMP Object ID
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.	ifInOctets 1.3.6.1.2.1.2.2.1.10
Incoming Unicast Packets (in-ucast-pkts)	The number of unicast packets received on the interface.	ifInUcastPkts 1.3.6.1.2.1.2.2.1.11
Discarded Incoming Packets (in-discards)	The number of packets which were chosen to be discarded due to RX FIFO full.	ifInDiscards 1.3.6.1.2.1.2.2.1.13
Erroneous Incoming Packets (in-errors)	The number of received erred packets.	ifInErrors 1.3.6.1.2.1.2.2.1.14
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.	ifOutOctets 1.3.6.1.2.1.2.2.1.16
Outgoing Unicast Packets (out-ucast-pkts)	The number of unicast packets transmitted out of the interface.	ifOutUcastPkts 1.3.6.1.2.1.2.2.1.17
Discarded Outgoing Packets (out-discards)	The number of outbound packets which were chosen to be discarded due to excessive collision or excessive deferral.	ifOutDisacrds 1.3.6.1.2.1.2.2.1.19
Erroneous Outgoing Packets (out-errors)	The number of outbound packets that could not be transmitted because of errors.	ifOutErrors 1.3.6.1.2.1.2.2.1.20
Incoming Multicast Packets (in-mcast-pkts)	The number of multicast packets received on the interface.	ifInMulticastPkts 1.3.6.1.2.1.31.1.1.1.2
Incoming Broadcast Packets (in-bcast-pkts)	The number of broadcast packets received on the interface.	ifInBroadcastPkts 1.3.6.1.2.1.31.1.1.1.3
Outgoing Multicast Packets (out-mcast-pkts)	The number of multicast packets transmitted out of the interface.	ifOutMulticastPkts 1.3.6.1.2.1.31.1.1.1.4
Outgoing Broadcast Packets (out-bcast-pkts)	The number of broadcast packets transmitted out of the interface.	ifOutBroadcastPkts 1.3.6.1.2.1.31.1.1.1.5

11.12.3 Bridge Object Attributes

Table 11-22 Bridge Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Component ID	Used to distinguish between the multiple virtual bridge instances within a PBB. The component id = s1 cannot be supplied as argument when using the **clear** command.	ieee8021BridgeBaseComponentId (1.3.111.2.802.1.1.2.1.1.1.1.1)		None[1]	
Bridge Address (addr)	The MAC address to be used by this bridge when it must be referred to in a unique fashion. It is the address of the Host interface (interface 1). The MAC base address is the same as the address of the Host interface 1.	ieee8021BridgeBaseBridgeAddress (1.3.111.2.802.1.1.2.1.1.1.1.2)	Octet string	RO	NN-NN-NN-NN-NN-NN where : NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3).
Component Number of Ports (num-ports)	The number of ports controlled by this bridging entity.	ieee8021BridgeBaseNumPorts (1.3.111.2.802.1.1.2.1.1.1.1.3)	Integer (32 bit)	RO	Always 2 for C-components Always 4 for S-components

11.12.4 Bridging Port Object Attributes

Table 11-23 Bridging Port Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (*Table 11-22*).	ieee8021BridgeBasePortComponentId (1.3.111.2.802.1.1.2.1.1.4.1.1)	<comp-id-list>	N/A	N/A

[1] This attribute is used as the index key to ieee8021BridgeBaseTable (1.3.111.2.802.1.1.2.1.1).

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Base Port	The number of the port for which this entry contains bridge management information. In the CLI port name is used instead of number	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	host, eth0, eth1, eth2, s1, c2, c3, c4	N/A	N/A
Bridge Port Interface Index (interface)	The interface that corresponds to this port.	ieee8021BridgeBasePortIfIndex (1.3.111.2.802.1.1.2.1.1.4.1.3)	host, eth0, eth1, eth2 In the current version, when a port is bound to an internal interface (s1, c1, c2, c3, c4) then the value for this attribute is 0.	RO	N/A
Bridge Port PVID (pvid)	The port-level VLAN ID that is assigned to untagged frames or Priority-Tagged frames received on the port. Each PVID must correspond to a valid VLAN on the corresponding component. In practice, this means that the VLAN must already be configured in the VLAN Table for the component before its VID can be assigned as the PVID for a port.	ieee8021QBridgePvid (1.3.111.2.802.1.1.4.1.4.5.1.1)	1..4094	RW	1
Bridge Port Default Priority (Prio)	An integer indicating the default ingress User Priority for this port. This attribute is relevant for protocols that do not support native User Priority, such as Ethernet.	ieee8021BridgePortDefaultUserPriority (1.3.111.2.802.1.1.2.1.3.1.1.1)	0..7	RW	0

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port Acceptable Frame Types (admit)	The frame types that will be accepted on the port and assigned to a VID. VID assignment is based on the PVID and VID Set for the port. When this is admitTagged(3), the device will discard untagged frames or Priority-Tagged frames received on this port. When admitAll(1), untagged frames or Priority-Tagged frames received on this port will be accepted. This attribute does not affect VLAN-independent Bridge Protocol Data Unit (BPDU) frames, such as MVRP or Spanning Tree Protocol (STP). However, it does affect VLAN-dependent BPDU frames, such as MMRP. If ingress filtering is enabled on the same port, then accepting untagged frames only is not compatible, since the combination effectively leads to discarding all frames on the port.	ieee8021QBridgePortAcceptableFrameTypes (1.3.111.2.802.1.1.4.1.4.5.1.2)	All= Admit all untagged and priority-tagged frames. Untagged= Admit untagged frames only. Tagged= Admit tagged frames only.	RW	All
Bridge Port Ingress Filtering (filter)	The ingress filtering state of the port. When Enabled, the device discards incoming frames for VLANs that do not include the port in its Member Set. When Disabled, the device accepts all incoming frames to the port. If untagged frames are admitted on the port, then ingress filtering is not compatible, since the combination effectively leads to discarding all frames on the port.	ieee8021QBridgePortIngressFiltering (1.3.111.2.802.1.1.2.1.4.5.3)	Enabled Disabled	RW	Disabled

11.12.5 Outgoing Queue Object Attributes

Table 11-24 Outgoing Queue Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Syntax	Access
Interface Name	Interface name		{eth0 | eth1 | eth2 | rf | all}	N/A
Queue ID	Queue ID		Range from 1 to 8	N/A
Tx Frame Counter	The counter of the per-Q transmitted frames.		tx 0..264	RO
Drop Frame Counter	The counter of the per-Q dropped frames.		drop 0..264	RO

11.12.6 Incoming Queue Object Attributes

Table 11-25 Incoming Queue Attributes

Attribute (CLI Attribute Name)	Description	Syntax	Access
Interface Name	Interface name	rf (currently only one, but may be extended in the future)	N/A
Queue ID	Queue ID	Range from 1 to 4	N/A
Good Frame Counter	The counter of the per-Q received good frames.	good 0..264	RO
Erroneous Frame Counter	The counter of the per-Q received erroneous frames.	error 0..264	RO
Lost Frame Counter	The counter of the per-Q lost rx frames.	lost 0..264	RO

11.12.7 IP Object Attributes

Table 11-26 IP Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Syntax	Value	Access	Default
IP Index	The index to the IP address table.	N/A	N/A	1..4	N/A	
IP Address (ip-addr)	The IP address to which this entry's addressing information pertains. The address type of this object is specified in ipAddressAddrType. All IP addresses in the table must be different.	1.3.6.1.2.1.4.34.1.2 (ipAddressAddr)	InetAddress	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 10.0.15.74)	RC	0.0.0.0
IP Address Mask (mask)	The subnet to which the IP address belongs.	N/A – not part of the MIB		ip mask in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 255.255.255.0)	RC	255.255.255.0
IP Default Router Address	The IP address of the default router represented by this row.	1.3.6.1.2.1.4.37.1.2 (ipDefaultRouterAddress)	InetAddress	ip address in the form X.X.X.X where X is a decimal number from 0 to 255 (for example 10.0.15.74)	NA	0.0.0.0
VLAN (vlan)	VLAN assigned to the IP. Two different IP addresses cannot be assigned the same VLAN (therefore all VIDs in the table must be different).	N/A		0..4094	RC	

11.12.8 VLAN Common Table Attributes

Table 11-27 VLAN Common Attributes

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Component ID	Used to distinguish between the multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (*Table 11-22*).	ieee8021QBridgeComponentId 1.3.111.2.802.1.1.4.1.1.1.1.1		s1

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
VLAN Version Number (version)	The version number of IEEE 802.1Q that this device supports.	ieee8021QBridgeVlanVersionNumber (1.3.111.2.802.1.1.4.1.1.1.1.2)	RO	version1
Maximum VLAN ID (max vid)	The maximum IEEE 802.1Q VLAN-ID that this device supports. Possible values are 1..4094.	ieee8021QBridgeMaxVlanId (1.3.111.2.802.1.1.4.1.1.1.1.3)	RO	n/a
Maximum Number of VLANs (max-num)	The maximum number of IEEE 802.1Q VLANs that this device supports. Possible values are 1..4094.	ieee8021QBridgeMaxSupportedVlans (1.3.111.2.802.1.1.4.1.1.1.1.4)	RO	n/a
Current Number of VLANs (curr-num)	The number of IEEE 802.1Q VLANs currently active on the network. This attribute is updated each time a VLAN is added or deleted from the network. Possible values are 1..4094.	ieee8021QBridgeNumVlans (1.3.111.2.802.1.1.4.1.1.1.1.5)	RO	n/a

11.12.9 VLAN Table Attributes

Table 11-28 VLAN Table Attributes

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Component Identifier	Used to distinguish between multiple virtual bridge instances within a PB. Component identifiers must be defined in the Bridge Component table (*Table 11-22*).	ieee8021QBridgeVlanStaticComponentId (1.3.111.2.802.1.1.4.1.4.3.1.1)	N/A	s1
VLAN ID	The VLAN-ID referring to this VLAN.	Ieee8021QBridgeVlanStaticVlanIndex (1.3.111.2.802.1.1.4.1.4.3.1.2)	N/A	1
Egress Ports Set (egress)	The set of ports that are permanently assigned by management to the egress list for this VLAN. Only those ports that belong to the corresponding component can be included in the set.	ieee8021QBridgeVlanStaticEgressPorts (1.3.111.2.802.1.1.4.1.4.3.1.4)	RC	Empty
Untagged Ports Set (Untagged)	The set of ports that should transmit egress packets for this VLAN as untagged. This set is allowed only for S-VLANs. This set must be subset of the **`Egress Ports Set`** attribute.	ieee8021QBridgeVlanStaticUntaggedPorts (1.3.111.2.802.1.1.4.1.4.3.1.4)	RC	Empty
FDB ID (fdb-id)	The ID of the filtering database used for this VLAN. Possible values are 1..64.	ieee8021QBridgeVlanFdbId (1.3.111.2.802.1.1.4.1.4.2.1.4)	RC	1

Attribute (CLI Attribute Name)	Description	CLI Object ID	Access	Default
Per-VLAN Incoming Packets (in-pkts)	The number of valid frames received by this port from its segment that were classified as belonging to this VLAN. Note: A frame received on this port is counted by this object only if it is for a protocol being processed by the local forwarding process for this VLAN. This object includes received bridge management frames that are classified as belonging to this VLAN (e.g., MMRP, but not MVRP or STP).	ieee8021QBridgeTpVlanPortInFrames (1.3.111.2.802.1.1.4.1.4.6.1.1)	RO	n/a
Per-VLAN Outgoing Packets (out-pkts)	The number of valid frames transmitted by this port to its segment from the local forwarding process for this VLAN. This object includes bridge management frames originated by this device that are classified as belonging to this VLAN (e.g., MMRP, but not MVRP or STP). Possible values are 0..264.	ieee8021QBridgeTpVlanPortOutFrames (1.3.111.2.802.1.1.4.1.4.6.1.2)	RO	n/a
Per-VLAN Dropped Packets (drop-pkts)	The number of valid frames received by this port from its segment that were classified as belonging to this VLAN and that were discarded due to VLAN-related reasons. This object refers specifically to the IEEE 802.1Q counters for Discard Inbound and Discard on Ingress Filtering. Possible values are 0..264.	ieee8021QBridgeTpVlanPortInDiscards (1.3.111.2.802.1.1.4.1.4.6.1.3)	RO	n/a

11.12.10C-LAN Registration Table Attributes

Table 11-29 C-LAN Registration Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port	The bridge port for the C-VLAN Registration entry. The bridge port specified in the command must match the Component ID in the VLAN Table (*Table 11-28*). For example, if the Component ID is c4 then the port must be external port 4).	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	<ext-bridge-port-list>	N/A	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
C-VID	The C-VID of this C-VLAN Registration entry. The VID must be defined in the VLAN Table (*Table 11-28*). The bridge component port specified in the command must match the Component ID in the VLAN Table. For example, if the Component ID is c4 then the port must be external4.	ieee8021PbCVidRegistrationCVid (1.3.111.2.802.1.1.5.1.2.1.1)	1..4094	N/A	N/A
S-VID (svlan)	The S-VID of this C-VLAN Registration entry. This value will be added to the C-tagged frames of the C-VID. The VID must be defined in the VLAN Table (*Table 11-28*) for an S-component.	ieee8021PbCVidRegistrationSVid (1.3.111.2.802.1.1.5.1.2.1.2)	1..4094	RC	N/A
Untagged CEP (untag-cep)	A flag indicating whether this C-VID should be carried untagged at the CEP.	ieee8021PbCVidRegistrationUntaggedCep (1.3.111.2.802.1.1.5.1.2.1.4)	Yes = The C-VID will be untagged No = The C-VID will be tagged	RC	No
Untagged PEP (untag-pep)	A flag indicating if this C-VID should be carried untagged at the PEP.	ieee8021PbCVidRegistrationUntaggedPep (1.3.111.2.802.1.1.5.1.2.1.3)	Yes = The C-VID will be untagged No = The C-VID will be tagged	RC	No

11.12.11PEP Virtual Port Table Attributes

Table 11-30 PEP Virtual Port Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port (bridge-port)	The bridge port for the PEP Virtual Port entry. The Bridge Port specified in the command must be an internal port (PEP) that belongs to the corresponding C-component.	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	s1	N/A	N/A
PEP S-VID (s-vid)	The 12-bit S-VID that is associated with the PEP.	ieee8021PbEdgePortSVid (1.3.111.2.802.1.1.5.1.3.1.1)	1..4094	N/A	N/A
PEP C-PVID (cpvid)	The 12-bit C-VID that will be used for untagged frames received at the PEP. The VID must be defined in the VLAN Table for the port's C-component (*Table 11-28*).	ieee8021PbEdgePortPVID (1.3.111.2.802.1.1.5.1.3.1.2)	1..4094	RC	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
PEP Default User Priority (prio)	An integer range 0-7 to be used for untagged frames received at the Provider Edge Port.	ieee8021PbEdgePortDefaultUserPriority (1.3.111.2.802.1.1.5.1.3.1.3)	0..7	RC	None
PEP Acceptable Frame Types (admit)	The frame types that will be accepted upon receipt at the PEP.	ieee8021PbEdgePortAcceptableFrameTypes (1.3.111.2.802.1.1.5.1.3.1.4)	All= Admit all untagged and priority-tagged frames. Untagged= Admit untagged frames only. Tagged= Admit tagged frames only.	RC	All
PEP Ingress Filtering (filter)	The ingress filtering state of the PEP. When enabled, the device discards incoming frames for VLANs that do not include the port in its Member Set. When disabled, the device accepts all incoming frames to the port.	ieee8021PbEdgePortEnableIngressFiltering (1.3.111.2.802.1.1.5.1.3.1.5)	Enabled, Disabled	RC	Disabled

11.12.12S-VID Translation Table Attributes

Table 11-31 S-VID Translation Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Port	The bridge port for the VID Translation Table entry.	ieee8021BridgeBasePort (1.3.111.2.802.1.1.2.1.1.4.1.2)	host, eth0, eth1, eth2	N/A	N/A
Local S-VID (local-svid)	The internal S-VID on received (transmitted) at the ISS of a CNP or PNP. The VID must be defined in the VLAN Table (Table 11-28) and the Bridge Port specified in the command must belong to the S-component. Because VID translation is bidirectional, two entries cannot use the same Local S-VID for the same port. Figure 11-3 shows the bidirectional relationships for Local S-VID.	ieee8021PbVidTranslationLocalVid (1.3.111.2.802.1.1.5.1.1.1.1)	1..4094	N/A	N/A

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Relay S-VID (relay-svid)	The translated S-VID delivered (received) over the EISS from a CNP or PNP. The VID must be defined in the VLAN Table (Table 11-28) and the Bridge Port specified in the command must belong to the S-component. Because VID translation is bidirectional, two entries cannot use the same Relay S-VID for the same port. Figure 11-3 shows the bidirectional relationships for Relay S-VID.	ieee8021PbVidTranslationRelayVid (1.3.111.2.802.1.1.5.1.1.1.2)	1..4094	RC	N/A

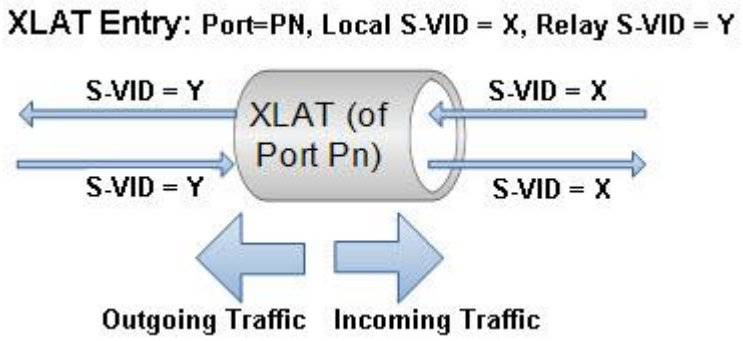


Figure 11-3 Bidirectional Definitions of S-VID Translation

11.12.13SNMP ifTable Attributes

Table 11-32 SNMP ifTable Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
Description	A text string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the interface hardware/software.	ifDescr (1.3.6.1.2.1.2.2.1.2)	RO	ASCII representation of the VLAN ID
Type	The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANA ifType textual convention.	ifType (1.3.6.1.2.1.2.2.1.3)	RO	l2vlan (135)

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
MTU Size	The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.	ifMtu (1.3.6.1.2.1.2.2.1.4)	RO	9216
MAC Address	The interface's address at its protocol sub-layer.	ifPhysAddress (1.3.6.1.2.1.2.2.1.6)	RO	The MAC address of the corresponding Eth.
Administrative Status	The desired state of the interface.	ifAdminStatus (1.3.6.1.2.1.2.2.1.7)	RW (Only a single value is allowed)	Up (1)
Operational Status	The current operational state of the interface. The Down state of ifOperStatus has two meanings, depending on the value of ifAdminStatus: If ifAdminStatus is not Down and ifOperStatus is Down then a fault condition is presumed to exist on the interface. If ifAdminStatus is Down, then ifOperStatus will normally also be Down i.e., there is not necessarily a fault condition on the interface.	ifOperStatus (1.3.6.1.2.1.2.2.1.8)	RO	Up (1) = Ready to pass packets
Last Change Time (lastchange)	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network management subsystem, then this object contains a zero value.	ifLastChange (1.3.6.1.2.1.2.2.1.9)	RO	0
Name	The textual name of the interface.	ifName (1.3.6.1.2.1.31.1.1.1.1)	RO	ASCII representation of the VLAN ID
State Trap	Indicates whether linkUp/linkDown traps should be generated for this interface.	ifLinkDownTrapEnable (1.3.6.1.2.1.31.1.1.1.14)	RW (only a single value is allowed.)	Disabled (2)
High Speed Indication	An estimate of the interface's current bandwidth in units of 1,000,000 bits per second.	ifHighSpeed (1.3.6.1.2.1.31.1.1.1.15)	RO	1000

Attribute (CLI Attribute Name)	Description	SNMP Object ID	SNMP Access	Value
Promiscuous Mode	This object has a value of False (2) if this interface only accepts packets/frames that are addressed to this station. This object has a value of True (1) when the station accepts all packets/frames transmitted on the media.	ifPromiscuousMode (1.3.6.1.2.1.31.1.1.1.16)	RO	False (0)
Connector	This object has the value True (1) if the interface sublayer has a physical connector. Otherwise, this object has the value False(2).	ifConnectorPresent (1.3.6.1.2.1.31.1.1.1.17)	RO	False (2)
Alias	This object is an alias name for the interface as specified by a network manager, and provides a non-volatile handle for the interface.	ifAlias (1.3.6.1.2.1.31.1.1.1.18)	RW	Zero-length string

11.12.14Forwarding Data Base (FDB) Object Attributes

Table 11-33 FDB Object Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PBB. In the current product version, the value of this object is equal to s1.	ieee8021QBridgeFdbComponentId (1.3.111.2.802.1.1.2.1.2.1.1.1). It is an index to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	s1 (forced)	N/A	s1
FDB ID (fdb-id)	The identity of this Forwarding Database. The system maintains 64 permanent instances of the FDB object.	ieee8021QBridgeFdbId (1.3.111.2.802.1.1.2.1.2.1.1.2) It is an index to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	1..64	N/A	1
Aging Time (aging)	The timeout period in seconds for aging out dynamically-learned forwarding information.	ieee8021QBridgeFdbAgingTime (1.3.111.2.802.1.1.2.1.2.1.1.5) It belongs to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	10..1000000	RW	172800

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Learned Entry Discards (full-table-counter)	The total number of Forwarding Database entries that have been or would have been learned, but have been discarded due to a lack of storage space in the Forwarding Database. When this counter is increasing, it indicates that the FDB is regularly becoming full, a condition which generally has adverse performance effects on the subnetwork. When this counter has a large value but is not currently increasing, it indicates that entry discards have been occurring but are not persistent. View the value of this object using the show command together with the **`statistics`** qualifier	ieee8021QBridgeFdbLearnedEntryDiscards (1.3.111.2.802.1.1.2.1.2.1.1.4) It belongs to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	Varies	RO	N/A
Dynamic Count (num-of-dynamic)	The current number of dynamic entries in this Forwarding Database. The value of this object is incremented each time an entry is created or deleted View the value of this object using the show command together with the **`statistics`** qualifier.	ieee8021QBridgeFdbDynamicCount (1.3.111.2.802.1.1.2.1.2.1.1.3) It belongs to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	Varies	RO	N/A

11.12.15FDB Address Table Attributes

Table 11-34 FDB Address Table Attributes

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
Bridge Component ID	The component identifier is used to distinguish between the multiple virtual bridge instances within a PBB. In the current product version, the value of this object is equal to s1.	ieee8021QBridgeFdbComponentId (1.3.111.2.802.1.1.2.1.2.1.1.1) It is an index to ieee8021QBridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2) and also to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	s1 (forced)	N/A	s1

Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
FDB ID (fdb-id-list)	The identity of this Forwarding Database. The system maintains 64 permanent instances of the FDB Address Table object.	ieee8021QBridgeFdbId (1.3.111.2.802.1.1.2.1.2.1.1.2) It is an index to ieee8021QBridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2) and also to ieee8021QBridgeFdbTable (1.3.111.2.802.1.1.2.1.2.1)	1..64	N/A	1
FDB MAC Address (addr)	The unicast MAC address for which the device has forwarding and/or filtering information.	ieee8021QBridgeTpFdbAddress (1.3.111.2.802.1.1.4.1.2.2.1.1) It is an index to ieee8021QBridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2)	NN-NN-NN-NN-NN-NN *where* NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	N/A	N/A
FDB Port (port)	The bridge port from which the MAC address has been learned.	ieee8021QBridgeTpFdbPort (1.3.111.2.802.1.1.4.1.2.2.1.2) It belongs to ieee8021QBridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2)	host, eth0, eth1, eth2, c1, c2, c3, c4, s1	RC	N/A
Address Entry Status (status)	The status of this FDB Address Table entry.	ieee8021QBridgeTpFdbStatus (1.3.111.2.802.1.1.4.1.2.2.1.3) It belongs to ieee8021QBridgeTpFdbTable (1.3.111.2.802.1.1.4.1.2.2)	Learned= The port was learned and is being used. Self= The port indicates which of the device's ports has this address. Mgmt= The entry has been assigned by management.	RO	N/A

11.12.16ARP Table Attributes

Table 11-35 ARP Table Attributes

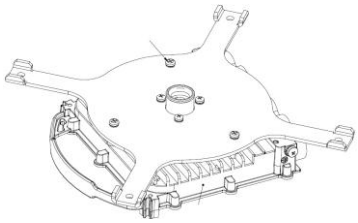
Attribute (CLI Attribute Name)	Description	SNMP Object ID	Value	Access	Default
ARP Interface (interface)	The index value that uniquely identifies the interface for this entry. The interface identified here is identical to that of the MIB's ifIndex.	ipNetToPhysicalIfIndex (1.3.6.1.2.1.4.35.1.1)	1..4	N/A	1
ARP IP Address	The IP Address that corresponds to the media-dependent physical address.	ipNetToPhysicalNetAddress (1.3.6.1.2.1.4.35.1.3)	X.X.X.X , where: X is a decimal number from 0 to 255 (for example 10.0.15.74)	RC	None
ARP MAC Address (mac-addr)	The media-dependent physical address.	ipNetToPhysicalPhysAddress (1.3.6.1.2.1.4.35.1.4)	NN-NN-NN-NN-NN-NN, where: NN is a hexadecimal number (for example 00-AF-DD-1E-2D-A3)	RC	None

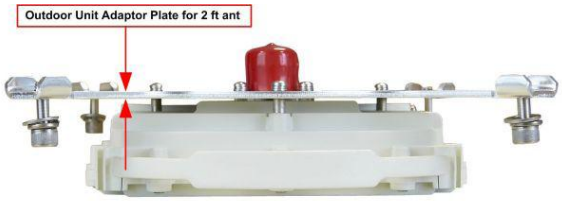
Appendix A: Installing the ODU with a Two Foot Antenna

This appendix presents the installation instructions of EH1200 ODU with two foot antenna.

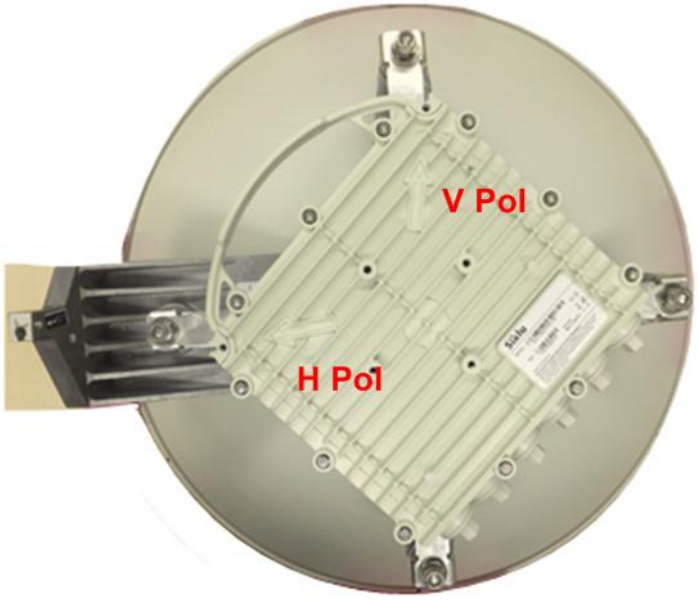
1. Install the two foot antenna according to the mounting diagram in the next page. Antenna mounting kit installation instructions are also available inside the mounting kit package.
2. Remove the protective tape on the antenna feed.

The 2ft ODU is shipped with External ODU adapter attached.

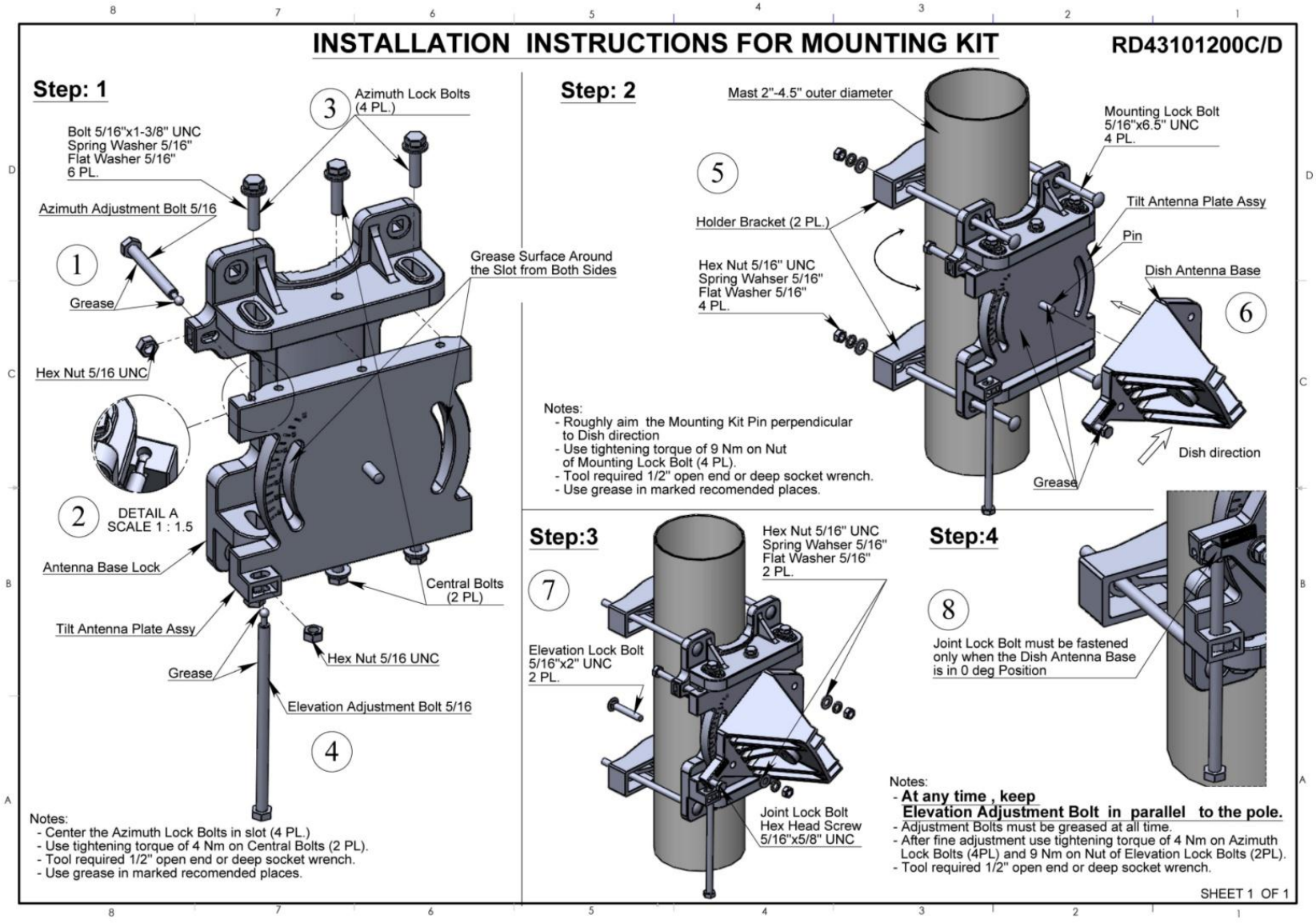




3. Unpack the 2ft ODU and remove the protective cap.
4. Attach the ODU to the antenna and tight the 4 locking bolts.
5. Make sure you install the ODU with the required polarization (note the polarization arrow on the back of the ODU).



6. Proceed with antenna alignment and ODU setup as described in Chapter 2.


INSTALLATION INSTRUCTIONS FOR MOUNTING KIT
RD43101200C/D
Step: 1
3
Azimuth Lock Bolts
(4 PL.)
Bolt 5/16"x1-3/8" UNC
Spring Washer 5/16"
Flat Washer 5/16"
6 PL.
Azimuth Adjustment Bolt 5/16
1
Grease
Grease Surface Around
the Slot from Both Sides
Hex Nut 5/16 UNC
2
DETAIL A
SCALE 1 : 1.5
Antenna Base Lock
Central Bolts
(2 PL)
Tilt Antenna Plate Assy
Grease
Hex Nut 5/16 UNC
Elevation Adjustment Bolt 5/16
4
Notes:
- Center the Azimuth Lock Bolts in slot (4 PL.)
- Use tightening torque of 4 Nm on Central Bolts (2 PL).
- Tool required 1/2" open end or deep socket wrench.
- Use grease in marked recomended places.
Step: 2
Mast 2"-4.5" outer diameter
Mounting Lock Bolt
5/16"x6.5" UNC
4 PL.
5
Holder Bracket (2 PL.)
Tilt Antenna Plate Assy
Pin
Hex Nut 5/16" UNC
Spring Wahser 5/16"
Flat Washer 5/16"
4 PL.
Dish Antenna Base
6
Dish direction
Grease
Notes:
- Roughly aim the Mounting Kit Pin perpendicular
to Dish direction
- Use tightening torque of 9 Nm on Nut
of Mounting Lock Bolt (4 PL).
- Tool required 1/2" open end or deep socket wrench.
- Use grease in marked recomended places.
Step:3
Hex Nut 5/16" UNC
Spring Wahser 5/16"
Flat Washer 5/16"
2 PL.
7
Elevation Lock Bolt
5/16"x2" UNC
2 PL.
Joint Lock Bolt
Hex Head Screw
5/16"x5/8" UNC
Step:4
8
Joint Lock Bolt must be fastened
only when the Dish Antenna Base
is in 0 deg Position
Notes:
- At any time , keep
Elevation Adjustment Bolt in parallel to the pole.
- Adjustment Bolts must be greased at all time.
- After fine adjustment use tightening torque of 4 Nm on Azimuth
Lock Bolts (4PL) and 9 Nm on Nut of Elevation Lock Bolts (2PL).
- Tool required 1/2" open end or deep socket wrench.
SHEET 1 OF 1