



Siklu

EtherHaul™

Gigabit Ethernet Wireless Solution

Operation, Administration and Maintenance Manual



EH-OPER-01, Issue 7

Apr 2016

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

Copyright © 2016 Siklu Communication Ltd. All rights reserved.

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of Siklu.

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 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 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
 E-Band FCC part 101; V-Band FCC Part 15.255
- 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

FCC/IC Regulatory Statements

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules and IC RSS standards. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference

will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note:



Changes or modifications to this equipment not expressly approved by Siklu LTD or the party responsible for compliance could void the user's authority to operate the equipment.

Caution:



Outdoor units and antennas should be installed **ONLY** by experienced installation professionals who are familiar with local building and safety codes and, wherever applicable, are licensed by the appropriate government regulatory authorities. Failure to do so may void the product warranty and may expose the end user or the service provider to legal and financial liabilities. Siklu LTD and its resellers or distributors are not liable for injury, damage or violation of regulations associated with the installation of outdoor units or antennas.

Prudence: Les unités extérieures et les antennes doivent être installés que par des professionnels expérimentés d'installation qui sont familiers avec les norms locales et les codes de sécurité et, si applicable, sont agréées par les autorités gouvernementales de réglementation compétents. Ne pas le faire peut annuler la garantie du produit et peuvent exposer l'utilisateur final ou le fournisseur de services d'obligations juridiques et financiers. Revendeurs ou distributeurs de ces équipements ne sont pas responsables des blessures, des dommages ou violation des règlements liés à l'installation des unités extérieures ou des antennes. L'installateur doit configurer le niveau de puissance de sortie des antennes conformément aux réglementations nationales et le type d'antenne.

About this Document

This document is the EtherHaul Operation, Administration and Maintenance manual for Siklu's EtherHaul wireless link product line.

For the installation and radio link setup instructions, please refer to the individual product's Installation Manual.

Note:



Features and functionality described in this document may be available for specific product models or starting from specific SW version.

Please review the individual product's release notes to verify if a specific feature is supported in the product you use.

Applicable Products and Releases

- E-Band
 - EH-1200, minimum SW release 3.5.0
 - EH-1200TL, minimum SW release 3.5.0 (note that the EH-1200TL has limited functionality and capabilities so options may not be available)
 - EH-1200T, minimum SW release 7.0.0
 - EH-1200TL/TX, minimum SW release 7.0.0 (note that the EH-1200TX has limited functionality and capabilities so options may not be available)
 - EH-1200F, minimum SW release 7.0.0
 - EH-1200FX, minimum SW release 7.0.0 (note that the EH-1200FX has limited functionality and capabilities so options may not be available)
 - EH-2200/2500F, minimum SW release 7.0.0 (note that the EH-2200FX has limited functionality and capabilities so options may not be available)
 - EH-2200FX/2500FX, minimum SW release 7.0.0 (note that the EH-2200FX/2500FX has limited functionality and capabilities so options may not be available)
- V-Band
 - EH-600T, minimum SW release 7.0.0
 - EH-600TL/TX, minimum SW release 7.0.0 (note that the EH-600TL has limited functionality and capabilities so options may not be available)

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

1	Introduction to the EtherHaul System.....	15
1.1	Main Features	16
1.2	Functional Description	18
2	Installing the EtherHaul System	21
3	Managing the EtherHaul.....	22
3.1	Connecting to System Using the Web-Based Management	23
3.2	Connecting to System Using the Command Line Interface	24
3.3	Web-Based Management Main Page	25
3.4	Quick Configuration Wizard	27
3.5	General Configuration Commands	27
3.5.1	Apply	27
3.5.2	Save Configuration.....	27
3.5.3	Rollback.....	28
3.5.4	Reboot.....	28
3.6	Copy To Remote.....	28
4	Radio Configuration and Monitoring.....	29
4.1	Settings	29
4.2	Advanced Settings	31
4.3	Maintenance	33
4.4	Modulation Table	34
4.5	Spectrum Analyzer	35
4.6	Statistics.....	35
4.7	CLI Commands	36
5	Ethernet Ports Configuration and Monitoring.....	37
5.1	Settings	37
5.2	Advanced Settings	38
5.3	Maintenance	38
5.4	Statistics.....	39
5.5	CLI Commands	39
6	System Configuration and Monitoring.....	40
6.1	Settings	40
6.2	Advanced Settings	41
6.3	Maintenance	43

6.3.1	File Transfer	43
6.3.2	SW Upgrade	44
6.3.3	Licensing	45
6.3.4	Scripts	47
6.3.5	Configuration Management	49
6.4	Event Configuration	50
6.5	CLI Commands	51
7	Network Configuration and Monitoring	53
7.1	General	53
7.1.1	IP Address	53
7.1.2	Default Gateway and Static Routes	54
7.1.3	SNMP Managers.....	54
7.1.4	NTP.....	55
7.2	Advanced Settings	56
7.2.1	Management Access List.....	56
7.2.2	SNMP Agent	56
7.2.3	Syslog Server.....	57
7.3	Maintenance	57
7.3.1	Iperf Test	57
7.3.2	Connectivity	58
7.3.3	ARP Table	58
7.4	Users Administration.....	59
7.4.1	Users.....	59
7.4.2	Password Strength	59
7.5	LLDP	60
7.5.1	LLDP Configuration.....	60
7.5.2	LLDP Status	61
7.6	CLI Commands	62
8	Ethernet Services Configuration and Monitoring	65
8.1	Bridge Mode.....	65
8.2	Link Aggregation.....	66
8.3	Bridge Architecture	68
8.4	Default Bridge Configuration.....	70
8.5	Services Configuration Overview	70
8.5.1	VLAN Configuration.....	72
8.5.2	Port Network Type Configuration.....	74
8.5.3	Bridge Port (PVID) Configuration	75
8.5.4	Configuration Examples	76
8.6	Maintenance	78
8.7	Statistics.....	78

8.8	Advanced Ethernet Networking Configurations	78
8.8.1	C-VLAN Registration.....	79
8.8.2	PEP Virtual Ports.....	80
8.8.3	S-VID Translation	80
8.8.4	Forwarding Data Base (FDB).....	81
8.8.5	Default C-VLAN EtherType	82
8.8.6	Bridge VLAN EtherType	82
8.8.7	MAC Learning.....	82
9	Quality of Service	83
9.1	QoS Configuration Using the Web-based Management GUI	84
9.2	Default QoS Configuration.....	85
9.3	QoS Classification	85
9.3.1	Port Priority	85
9.3.2	Classification Criteria.....	85
9.3.3	Classifiers	86
9.4	Scheduling	87
9.4.1	Scheduling Mode: Strict Priority	87
9.4.2	Scheduling Mode: Weighted Fair Queue (WFQ).....	87
9.4.3	Scheduling Mode: Priority-Shaper	88
9.4.4	Scheduling Mode: WFQ-Shaper	89
9.5	QoS Configuration Commands	89
9.6	QoS Statistics.....	89
9.7	QoS CLI Commands – Classification and Scheduling.....	90
9.8	Advanced QoS Configuration	91
9.8.1	Advanced Classification.....	91
9.8.2	Metering and Coloring.....	92
9.8.3	PCP Rewrite	94
9.8.4	PFC - Priority-based flow control.....	95
9.8.5	Queue Management.....	96
9.8.6	Weighted Random Early Detection (WRED).....	96
10	Synchronization.....	100
10.1	Synchronous Ethernet (SyncE).....	100
10.1.1	SyncE Configuration	101
10.1.2	Typical SyncE Scenario.....	102
10.1.3	Port Clock.....	105
10.1.4	SyncE Alarms	106
10.2	IEEE 1588v2	106
10.2.1	IEEE 1588 Configuration	106

11	ExtendMM™	109
11.1	ExtendMM™ Description	109
11.2	ExtendMM™ Requirements.....	110
11.3	ExtendMM™ Configuration	110
12	Ethernet Ring Protection (ERP)	112
12.1	Ethernet Ring Protection Description.....	112
12.2	Supported ERP Features	113
12.3	ERP Ring Commands.....	113
12.4	ERP Administrative Commands.....	114
12.5	ERP Timers	116
12.6	Sample ERP Configuration	116
13	Operation, Administration and Maintenance (OAM)	118
13.1	CFM (Connectivity Fault Management)	118
13.1.1	CFM Overview	118
13.1.2	Working with Maintenance Domains.....	120
13.1.3	Working with Maintenance Associations	120
13.1.4	Working with Component Maintenance Associations	121
13.1.5	Working with Maintenance End Points (MEPS).....	121
13.1.6	Working with Peer MEPs	122
13.1.7	Working with CCM Messages	123
13.1.8	Working with Linktrace Messages	124
13.1.9	Sample CFM Configuration	124
13.2	Performance Monitoring (ITU-T Y.1731).....	131
13.3	Link OAM	132
13.3.1	Link OAM Configuration.....	132
13.3.2	Link OAM Discovery	133
13.3.3	Link OAM Loopback	134
14	Administration	135
14.1	TACACS+/RADIUS Users Administration	135
14.1.1	AAA Description.....	135
14.1.2	Authentication Modes.....	136
14.1.3	TACACS Authentication Mode	136
14.1.4	Radius Authentication Mode	138
14.2	CLI Commands	139
14.3	SNMPv3 Users Configuration.....	140
14.4	Zero-Touch Configuration.....	141
14.4.1	Requirements	141
14.4.2	Zero Touch System Process	141
14.4.3	CLI Configuration for Zero Touch using the CLI	142

14.5	Monitoring CLI Sessions.....	143
14.6	DHCP Relay (Option 82)	144
15	Diagnostics	146
15.1	Troubleshooting Process.....	146
15.2	System LEDs	148
15.3	Alarms	148
15.4	Performance Statistics	153
15.5	Loopbacks.....	153
15.5.1	Loopbacks Diagram.....	154
15.5.2	Ethernet Line Loopbacks.....	154
15.5.3	Radio (RF) Loopback.....	155
15.5.4	Loopbacks CLI Commands	155
16	Statistics.....	157
16.1	Radio (RF) Statistics Monitoring	157
16.1.1	RF Statistics Summary	157
16.1.2	RF Statistics Summary – 30 days	158
16.1.3	RF Statistics.....	158
16.2	Bandwidth Utilization Statistics	160
16.3	Ethernet Statistics	161
16.4	VLAN Statistics.....	162
16.5	Queues Statistics.....	162
16.5.1	Out-Queue Statistics	162
16.5.2	In-Queue Statistics.....	163
16.6	CLI Commands	163

TABLE OF FIGURES

Figure 1-1 Hitless Adaptive Bandwidth, Coding and Modulation	18
Figure 1-2 EH-600T (TDD) Functional Block Diagram	19
Figure 1-3 EH-1200 (TDD) Functional Block Diagram.....	19
Figure 1-4 EH-1200F (FDD) Functional Block Diagram.....	19
Figure 1-5 EH-2200F/FX/EH-2500F/FX (FDD) Functional Block Diagram	20
Figure 3-1 Launching the Web-Based Management	23
Figure 3-2 Entering Username and Password.....	23
Figure 3-3 Web-Based Management Main Page	24
Figure 3-4 Launching CLI	24
Figure 3-5 Copy To-Remote icon.....	28
Figure 4-1 Radio Page: Settings	29
Figure 4-2 Radio Page: Advanced Settings	31
Figure 4-3 Radio Page: Maintenance.....	33
Figure 4-4 Radio Page: Modulation Table – EH-600 and EH-1200 product lines.....	34
Figure 4-5 Radio Page: Modulation Table – EH-2200 product line.....	34
Figure 4-6 Radio Page: Spectrum Analyzer	35
Figure 4-7 Radio Page: Statistics.....	35
Figure 5-1 Eth Ports Page: Settings	37
Figure 5-2 Eth Ports Page: Advanced Settings	38
Figure 5-3 Eth Ports Page: Maintenance	38
Figure 5-4 Eth Ports Page: Statistics.....	39
Figure 6-1 System Page: Settings	40
Figure 6-2 System Page: Advanced Settings	41
Figure 6-3 System Page: Maintenance – File Transfer.....	43
Figure 6-4 System Page: Maintenance – SW Upgrade.....	44
Figure 6-5 System Page: Maintenance – Licensing.....	45
Figure 6-6 System Page: Maintenance – Scripts	47
Figure 6-7 System Page: Maintenance – Configuration Management	49
Figure 6-8 Network Page: Event Configuration	50
Figure 7-1 Network Page: General – IP Address.....	53
Figure 7-2 Network Page: General – Default Gateway	54
Figure 7-3 Network Page: General – SNMP Managers.....	54
Figure 7-4 Network Page: General – NTP.....	55
Figure 7-5 Network Page: Advanced Settings – Management Access List.....	56
Figure 7-6 Network Page: Advanced Settings – SNMP Agent	56

Figure 7-7 Network Page: Advanced Settings – Syslog Server.....	57
Figure 7-8 Network Page: Maintenance – Iperf Test.....	57
Figure 7-9 Network Page: Maintenance – Connectivity.....	58
Figure 7-10 Network Page: Maintenance – ARP Table	58
Figure 7-11 Network Page: Users Administration – Local Authentication.....	59
Figure 7-12 Network Page: Advanced Settings – Password Strength.....	59
Figure 7-13 Network Page: LLDP Configuration.....	60
Figure 7-14 Network Page: LLDP Status	61
Figure 8-1 Services Page: General – Bridge Mode.....	65
Figure 8-2 LAG Configuration and Monitoring	67
Figure 8-3 EtherHaul Bridge Architecture	69
Figure 8-4 Single Component Bridge Model (Provider NNI ports)	70
Figure 8-5 Multiple Components Bridge Model (Customer UNI ports)	70
Figure 8-6 Services Page: General - VLAN	72
Figure 8-7 Services Page: General – VLAN (Add VLAN).....	73
Figure 8-8 Services Page: General – Port Network Type.....	74
Figure 8-9 Services Page: General – Bridge Port	75
Figure 8-10 Services Page: Transparent Pipe	77
Figure 8-11 Services Page: Maintenance.....	78
Figure 9-1 Classification and Policing.....	83
Figure 9-2 Egress Queues Scheduling	84
Figure 9-3 Advanced Config Page: Quality of Service – Port Priority	85
Figure 9-4 Advanced Config Page: Quality of Service – Classification Criteria	85
Figure 9-5 Advanced Config Page: Quality of Service – Classifiers	86
Figure 9-6 Advanced Config Page: Quality of Service – Scheduler Mode Strict Priority	87
Figure 9-7 Advanced Config Page: Quality of Service – Scheduler Mode WFQ	87
Figure 9-8 Advanced Config Page: Quality of Service – Scheduler Mode Priority-Shaper	88
Figure 9-9 Advanced Config Page: Quality of Service – Scheduler Mode WFQ-Shaper.....	89
Figure 9-10 TCP Performance	97
Figure 9-11 TCP Performance without WRED	98
Figure 9-12 TCP Performance with WRED	99
Figure 10-1 SyncE Functional Diagram	100
Figure 10-2 Advanced Config Page: Synchronization – SyncE	101
Figure 10-3 Typical SyncE Scenario – Normal Operation.....	102
Figure 10-4 Typical SyncE Scenario – Radio Failure	103
Figure 10-5 Typical SyncE Scenario – Line Failure.....	104
Figure 10-6 Advanced Config Page: Synchronization – SyncE Port Clock.....	105
Figure 10-7 Advanced Config Page: Synchronization – IEEE 1588.....	106
Figure 11-1 ExtendMM™ in normal operation (sub-6 GHz in stand-by mode) Criteria.....	109

Figure 11-2 Advanced Config Page: ExtendMM™	110
Figure 12-1 Basic ERP Protection Mechanism	113
Figure 13-1 CFM Network	119
Figure 14-1 Network Page: Users Administration – TACACS	136
Figure 14-2 Network Page: Users Administration – Radius.....	138
Figure 15-1 System Loopback Points	154
Figure 15-2 Ethernet Line Loopback.....	154
Figure 15-3 RF Loopback.....	155
Figure 16-1 Statistics Page: RF Statistics Summary.....	157
Figure 16-2 Statistics Page: RF Statistics Summary – 30 days	158
Figure 16-3 Statistics Page: RF Statistics	158
Figure 16-4 Statistics Page: Bandwidth Utilization Statistics	160
Figure 16-5 Statistics Page: Ethernet Statistics	161
Figure 16-6 Statistics Page: VLAN Statistics.....	162
Figure 16-7 Statistics Page: Out-Queue Statistics	163
Figure 16-8 Statistics Page: In-Queue Statistics.....	163

1 Introduction to the EtherHaul System

This chapter provides a brief overview of the EtherHaul product line.

The EtherHaul radio delivers carrier-grade wireless point-to-point gigabit Ethernet services utilizing the 57-66GHz unlicensed V-band and the light-licensed 71-76/81-86GHz E-band spectrum.

The EtherHaul is based on Siklu's revolutionary integrated-silicon technology, which results in a highly reliable, zero footprint, and low-cost radio.

The EtherHaul offers Gigabit throughput, MEF-compliant networking, 8 levels of QoS, enhanced Hitless Adaptive Bandwidth, Coding and Modulation for maximum spectral efficiency, and services availability. It supports network synchronization, advanced OAM&PM tools and ring protection optimized for both small cell and mobile backhaul. It features multiple GbE interfaces, including optical, supporting complex network topologies, such as daisy chain, ring, and mesh. The multiple ports enable also colocation installation and leveraging the infrastructure for additional fixed services delivery. The EtherHaul is fast, simple and inexpensive to deploy.

EtherHaul as the ideal solution for mobile backhaul and business services delivery features:

- Field proven technology
- Reduced TCO and fast ROI
- All-outdoor invisible footprint
 - Small and light
 - Quick and easy to install
- Spectral efficient
 - Wide range of frequencies
 - TDD modulation with seamless delay and jitter
 - Hitless Adaptive Bandwidth Coding and Modulation for high availability
- Advanced layer-2 features:
 - MEF-compliant services and QoS
 - VLAN & Provider Bridge with 16K jumbo frames support
 - Clear separation between multiple services with QoS
 - Enables QoS aware MPLS services delivery
 - SLA assurance
- Advanced AES encryption for secured street level deployments

Highly-scalable, the EtherHaul products are software-upgradable to support future Layer 2.5/3 networking and routing capabilities as networks evolve to flat-IP topologies.

The EtherHaul products features advanced adaptive modulation, bandwidth and coding - allowing operators to maintain, prioritize, and verify QoS in all weather conditions, while achieving maximum (up to 99.999%) link availability for prioritized services such as voice signaling and Sync.

Offering easy and low cost all-outdoor installation and a small form factor, the EtherHaul products are also environmentally-friendly - boasting a small system and antenna footprint with especially low power consumption.

The EtherHaul systems are High-capacity Gigabit Ethernet backhaul, with advanced networking capabilities, at the lowest TCO in the industry. EtherHaul enables mobile operators to profitably and reliably provide data intensive services. Provided by Siklu, the pioneer in silicon based mm-waves backhaul systems, EtherHaul systems are the perfect choice for future proof investment.

1.1 Main Features

Siklu's EtherHaul wireless backhaul radio link operates in the new V-band and E-band spectrum, which provides clear technological and economic advantages over the existing lower frequency bands. Taking advantage of the new spectrum, the EtherHaul 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 (availability of features depends on platform):

All-Outdoor Packet Radio

- Operates in the unlicensed 57-64 GHz V-band and light-licensed 71-76/81-86 GHz E-Band
- Up to 1 Gbps throughput
- Asymmetric capacity configuration
- High gain narrow beam-width directional antenna
- Low latency

Highest Spectral Efficiency

- 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
- MEF compliant services and QoS
- Advanced service management, OAM and SLA assurance support
- SyncE, IEEE 1588TC and optimized transport of IEEE 1588
- Ring, mesh and daisy chain topologies for carrier grade availability and resiliency
- Standard-based for seamless integration into existing networks and multi-vendor interoperability
- Multi-vendor interoperability approved

Carrier Grade:

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

Green Design:

- Zero footprint, all-outdoor, extremely light weight
- low power consumption
- IEEE 802.3at+ compliant Power over Ethernet

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

Adaptive Bandwidth, Coding and Modulation

The EtherHaul family implements hitless/errorless adaptive bandwidth, coding and modulation adjustment to optimize the over-the-air transmission and prevent weather-related fading from disrupting traffic on the link. The EtherHaul can gain up to 21 dB in link budget by dynamically adapting: Modulation, FEC coding rates, and channel bandwidth maintaining the high priority traffic using quality of service advanced mechanism and dropping the traffic according to the QoS priority defined by the user.

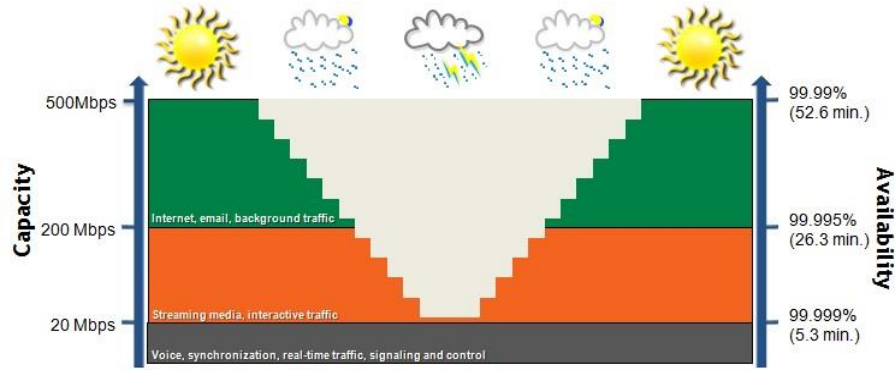


Figure 1-1 Hitless Adaptive Bandwidth, Coding and Modulation

1.2 Functional Description

The EtherHaul is an all-outdoor system comprised of the following functional blocks:

- RFIC: Siklu's integrated Silicon Germanium (SiGe) transceiver operating at 57-66GHz (EH-600T), 71-76GHz (EH-1200/TL) or 71-76/81-86GHz (EH-1200F/FX).
- Modem/Baseband ASIC: Siklu's modem/baseband ASIC includes the modem, FEC engines, and Synchronous Ethernet support.
- Network Processor: the networking engine is the heart of the high speed bridge/router function. The engine receives packets from Ethernet interfaces the modem and CPU. It is responsible for proper forwarding between these all interfaces.
- Interfaces: The network interface consists of 2-4 integrated 100/1000 Ethernet ports, depends on the product type.
- Host processor (CPU) the host processor controls the system responsible for the control plane, and the antenna alignment.
- Antenna: Siklu's self-designed 1ft innovative antenna, as well as 2ft antenna option for longer range higher availability.

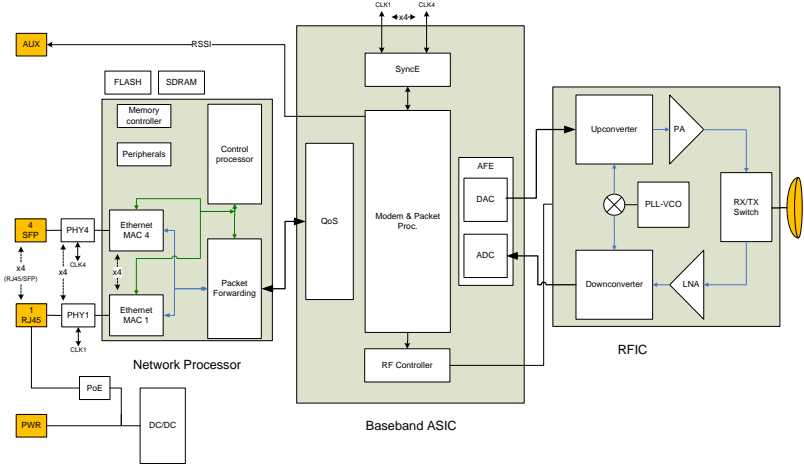


Figure 1-2 EH-600T (TDD) Functional Block Diagram

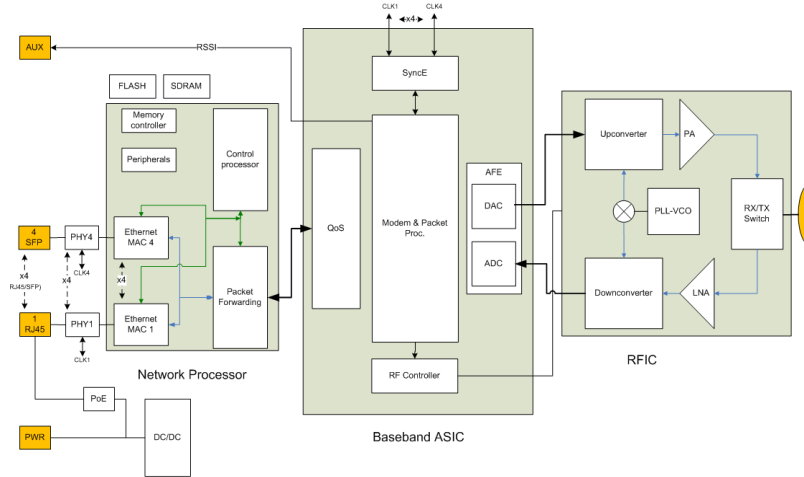


Figure 1-3 EH-1200 (TDD) Functional Block Diagram

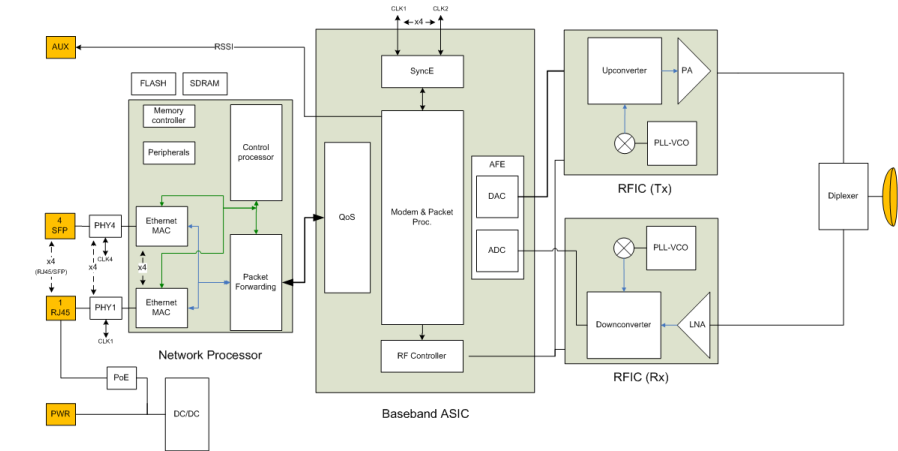


Figure 1-4 EH-1200F (FDD) Functional Block Diagram

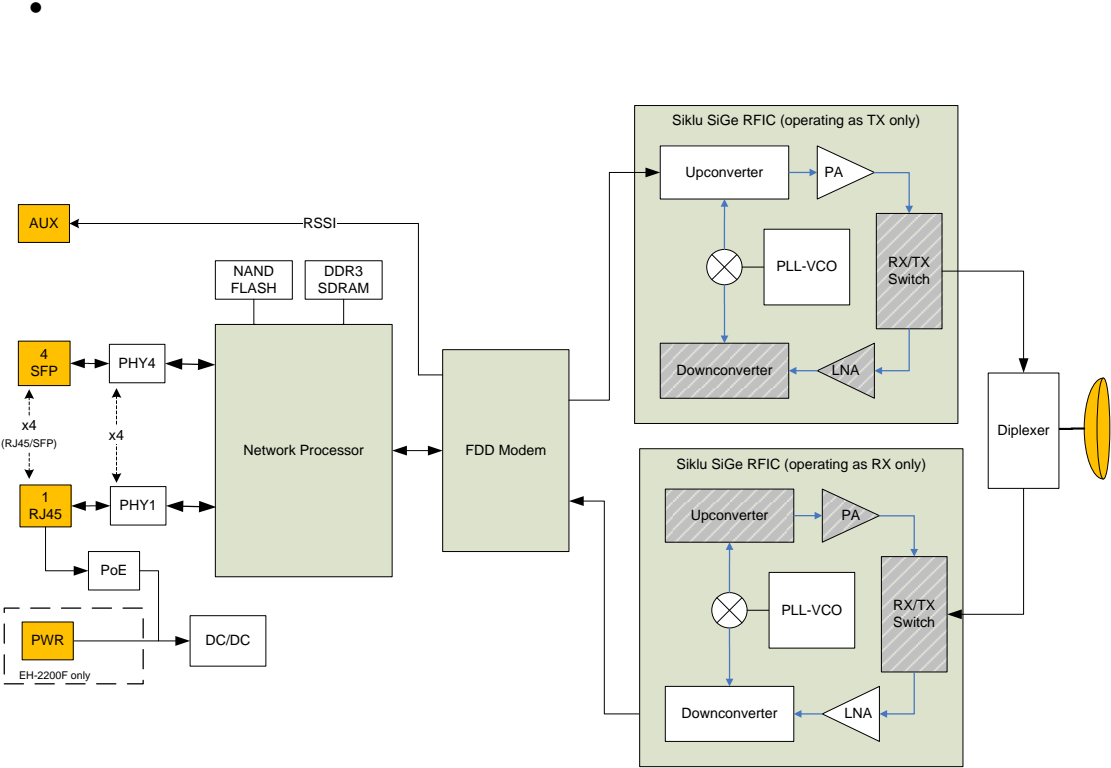


Figure 1-5 EH-2200F/FX/EH-2500F/FX (FDD) Functional Block Diagram

2 Installing the EtherHaul System

For installation and setup of the EtherHaul system, please refer to the individual product's Installation Manual.

The scope of this document is to describe the Web-Based Management (HTML) and Command Line Interface (CLI) configuration and monitoring options.

The Web-Based Management and Command Line Interface (CLI) should be used after successful installation and the commissioning of the radio link.

3 Managing the EtherHaul

In order to carry configuration, monitoring or maintenance tasks, connect your station to any one of the system's Ethernet ports and launch the chosen management option.

There are 2 options to connect and manage the EtherHaul:

- 1) Embedded HTML Web-Based Management.

EtherHaul's recommended management option and the use of this option is described in details in this document.

Provides self-explanatory graphical user interface for managing both ends of the link.

Note: HTML Web-Based Management availability depends on product's specs.



It is available for specific products and starting from specific SW version. Refer to the EtherHaul Release Notes for details.

- 2) Command Line Interface (CLI).

Provides command line interface for configuration and monitoring. Includes the entire configuration options of the system.

- General format of CLI command:

```
command object <object-id(s)> [attribute-name <attribute-value>]
```

for example:

```
set eth eth1 eth-type 100FD
show vlan all all statistics
```

- Typical commands:

`Set, show, clear, reset, run, copy`

- General CLI conventions:

- Confirmation after each command correctly entered.
- Error-message with hint in case of wrong command
- Use Tab for Auto-complete
- Use Up Arrow and Down Arrow to display command history
- Use ? for help on possible configuration options and for exact command syntax.

This chapter includes the following topics:

- Connecting to system using the Web-Based Management
- Connecting to system using the Command Line Interface
- Web-Based Management Main Page
- Quick Configuration Wizard
- General Configuration Commands

3.1 Connecting to System Using the Web-Based Management

1. Launch an Internet Browser and enter **https://** followed by the system's IP address. The system's default IP address is **192.168.0.1**.



Figure 3-1 Launching the Web-Based Management

2. When prompted, enter the username and password. Default: **admin** and **admin**.



Figure 3-2 Entering Username and Password

3. Once loaded, the Web-Based Management Main page is displayed.

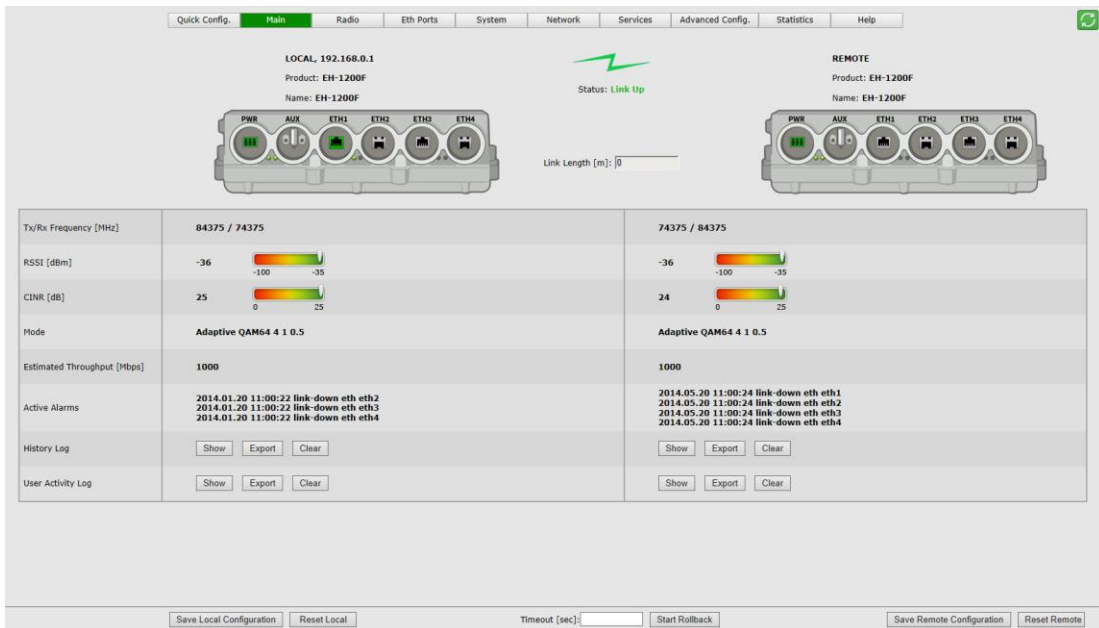


Figure 3-3 Web-Based Management Main Page

3.2 Connecting to System Using the Command Line Interface

1. Launch standard SSH client. You can use any common, open source SSH client program, such as PuTTY, available for download from the web.

Open an SSH session to the system's IP address. The system's default IP address is **192.168.0.1**.

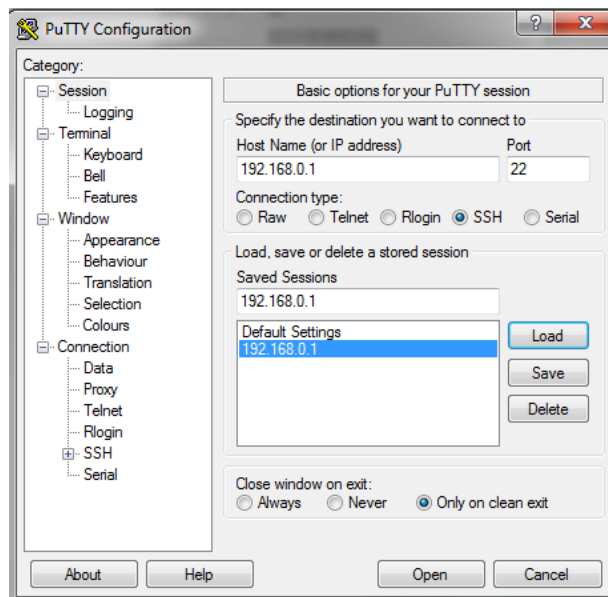


Figure 3-4 Launching CLI

2. PuTTY configuration (Recommended):
 - a. Go to category: Terminal -> Keyboard
Set Backspace key = Control-H
Set The function keys and keypad = Linux
 - b. Go to category: Window
Set Lines of Scrollback = 100000
 - c. Save the session and configuration. Give it a name and Click Save. The session will be stored under the Saved Sessions.
4. When prompted, enter the username and password. Default: **admin** and **admin**.

```
login as: admin
EH-1200F, S/N: F323036112, Ver: 6.0.0 11309
Using keyboard-interactive authentication.
Password:
EH-1200F>
```

3.3 Web-Based Management Main Page

The Web-Based Management provides link view, presenting both local and remote configuration and monitoring.

Although the local and remote systems IP address is identical (default IP address 192.168.0.1), the remote will be available as well as the EtherHaul uses dedicated communication channel for local-remote communication that is not IP-based.

It is recommended, however, to assign dedicated IP address for local and remote systems.

Note: Depending on your station's screen size and resolution, you may need to scroll the screen vertically or horizontally in order to view all options for local + remote.



Alternatively, you may change the change the Internet's Browser display distance (Zoom out, using Ctrl+Minus).

The Web-Based Management Main page is a read-only page and displays the following information:

- Link Status – Link up or down (with visual indication)
- Link Length [m] – link calculated distance between the local and remote systems (air distance) based on propagation time.

Note that Link Length reading supported on EH-600T and EH-1200F/FX platforms only.

- Tx/Rx frequency [MHz].
- RSSI [dBm] – Receiver Signal Strength Indicator. Current receive level.

- CINR [dB] – Carrier to Interference + Noise ratio. Indicates the current radio link's signal quality. In normal conditions, $CINR \geq 19$ indicates a good signal quality.
- Mode – Current operational mode of the link:
 - Alignment – Carrier Wave transmission. Used for antenna alignment. No data over the radio link.
 - Static – Fixed modulation profile. If you select Static, you must select from a list of pre-configured modulation profiles in the Modulation field.
 - Adaptive – Adaptive Bandwidth, Code, and Modulation. The system will work on the highest modulation profile based on the CINR values of the both sides and will present the current modulation profile.
- Estimated Throughput [Mbps] – based on the current modulation profile.
 - For FDD systems – value is Full-Duplex.
 - For TDD systems – value is aggregated (Half-Duplex).

Note:



Actual Layer 1 throughput depends on product's specs. Refer to the EtherHaul Release Notes for exact specifications.

- Current Alarms – list of currently active alarms and date&time raised.
- History Log – System alarms and events history log.
- User Activity Log – All configuration changes are logged, including user and date&time (presented in the form of CLI commands).

Note:



To view logs, pop-ups must be enabled and allowed on your Internet Browser.

3.4 Quick Configuration Wizard

Use the Quick Configuration wizard to configure the basic system parameters for both local and remote systems. It holds the basic minimal configuration required to start using the link.

The Quick Configuration wizard should be used for the initial system setup after installation. For monitoring and advanced configuration, please refer to the dedicated configuration pages of the Web-Based Management.

The Quick Configuration wizard is described in the individual product's Installation Manual.

3.5 General Configuration Commands

3.5.1 Apply

Any configuration change is executed upon clicking **Apply**.

The Local-Remote concept of the Web-Based Management allows configuring both local and remote systems of the link.

The **Apply** button is available at the bottom of each configuration page (one button for both local and remote systems).

When clicking **Apply**, the configuration changes will be sent to remote system first and then to the local system. If multiple parameters changed on the page before clicking **Apply**, all parameters are sent in bulk to the system and then executed locally in order to avoid losing management connection.

3.5.2 Save Configuration

Any configuration change applied should be saved using the **Save Configuration** button.

The system has two configuration banks:

1. Running Configuration – the currently active configuration. Every time **Apply** is clicked, the Running Configuration is updated.
2. Startup Configuration – the configuration the system will come up with after the next reboot. This configuration may be different than the currently active configuration (Running Configuration).

In order to save the applied configuration changes, click **Save Configuration** so changes will be saved to the startup configuration. If changes are not saved to the startup configuration, they will be lost the next time the system reboots.

Save Configuration buttons are available for local and remote systems.

3.5.3 Rollback

A safety measure that allows recovering from system configuration changes that caused loss of communication.

When Rollback is used, a timer runs (and restarts) whenever a management (or CLI) command is entered. In the event that no command is entered within the timeout period, the system automatically reboots and comes up with the saved startup configuration.

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

Rollback is activated for both local and remote systems.

3.5.4 Reboot

Separate buttons for local and remote reboot. The system will power off and then on and come up after initialization (~120 seconds).

Note that any unsaved changes will be lost.

3.6 Copy To Remote

You can find the **Copy To Remote** button next to some configuration parameters or sections. This function copies configuration to remote system based on the changes on the local system.

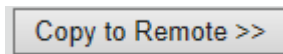


Figure 3-5 Copy To-Remote icon

Matching configuration may be of two types:

- Identical configuration – exactly same configuration will be copied from the local to remote system. It can be found for parameters that normally requires identical configuration for both local and remote units.

For example, Encryption configuration.

- Matching configuration – for parameters that require matching but opposite configuration.

For example (FDD systems): transmit frequency where Tx(local)=Rx(remote) and Rx(local)=Tx(remote).

4 Radio Configuration and Monitoring

The radio link parameters and radio link monitoring are managed in the **Radio** page.

This chapter includes the following topics:

- Settings
- Advanced Settings
- Maintenance
- Modulation Table
- Spectrum Analyzer
- Statistics
- CLI commands

4.1 Settings

Settings	Channel Bandwidth [MHz]	500	500
Advanced Settings	Tx Frequency [MHz]	58375	58375
Maintenance	Tx Power [dBm]	5	5
Modulation Table	RSSI [dBm]	-41	-39
Statistics	CINR [dB]	23	23
	Alignment Status	Inactive	Inactive
	Alignment Probe	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Mode	QAM64 4 1 0.5	QAM64 4 1 0.5
	Transmit Asymmetry	50TX-50RX	50TX-50RX

Figure 4-1 Radio Page: Settings

This section allows configuring the following parameters:

- Channel Bandwidth [MHz] – 250 or 500MHz (default is 500MHz).
Note that 250MHz support depends on product’s specs.
- Tx Frequency [MHz] – transmit frequency.
- Rx Frequency [MHz] – R/O field, updated based on Tx frequency.
 - For FDD systems – fixed 10GHz spacing between Tx and Rx frequencies.
 - For TDD systems – identical Tx and Rx frequencies.
- Tx Power [dBm] – ODU’s transmit power. Default is the max power, based on product’s specs. Minimum configurable Tx power is -35dBm (note that actual minimum Tx power is based on product’s specs).

Note:



Adjust Tx Power so the RSSI at the remote end will not exceed -35dBm (overload threshold).

The Tx power value sets the transmit power for the highest modulation profile. In case lower modulation profile(s) has higher max Tx power (based on product's specs), the Tx power will be increased automatically without indication in RF configuration menu.

- Mode – operational mode of the link:
 - Alignment – Carrier Wave transmission. Used for antenna alignment. No data over the radio link.

Note:



When exiting Alignment mode, perform system reboot to allow proper operation of the radio link.

- Static – Fixed modulation profile. If you select Static, you must select from a list of pre-configured modulation profiles in the Modulation field.
- Adaptive – Adaptive Bandwidth, Code, and Modulation.

The ODU will work on the highest modulation profile based on the CINR values of the both sides and will present the current modulation profile.

Adaptive mode is the normal and recommended mode of the radio link.

- Alignment Status – R/O field, indicating that the ODU is currently in Alignment mode (by configuration or by inserting DVM probes).
- Alignment Probe (EH-600T systems only) – when checked, the ODU will use the Alignment Cap Screw status as alignment indication: when removing the screw, the ODU will switch to Alignment.

When unchecked, the ODU will not switch to alignment mode is the screw is removed.

Note:




It is recommended to disable the Alignment Probe indication after EH-600T link is installed to avoid false identification and switch to Alignment mode.

- Transmit Asymmetry – Default value is symmetric configuration: 50% for Tx and Rx (50tx-50rx). For an asymmetric configuration (75%/25%), Role has to be set: the Master unit transmits the higher rate (75tx-25rx) and the Slave unit the lower rate (25tx-75rx).

When selecting asymmetric configuration, Role will be set automatically (refer to Radio Advanced Settings).

Note that Asymmetric configuration depends on product’s specs and is relevant only for TDD systems).

Note:  When changing Radio parameters of the link (like Mode, Asymmetry, frequency...) the link will go down and come up within couple of minutes.

4.2 Advanced Settings

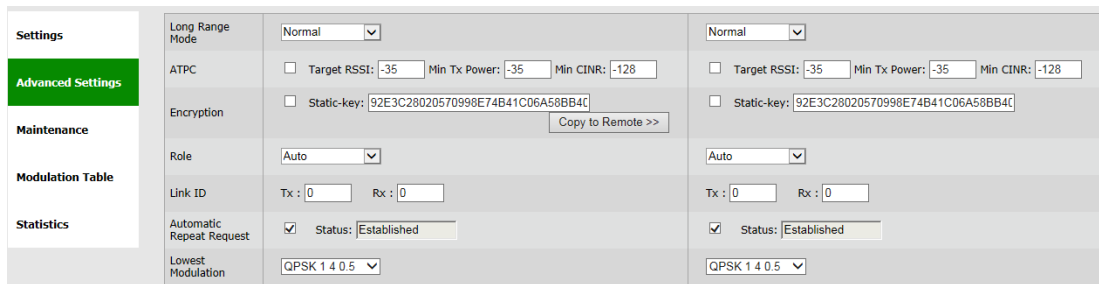


Figure 4-2 Radio Page: Advanced Settings

This section allows configuring the following parameters:

- Long Range Mode – checkbox to enable extended range mode (feature is license dependent).

V-band radios:

- Normal – links up to 4.5Km (systems with HW Rev prior to C0 are limited to 1000m)

E-band radios:

- Normal – links from 0 to 5Km
- Long – links from 5 to 10Km
- Extra-Long – links from 10 to 15Km
 - Note that EH-2200/EH-2500 product line has no limitation of the link distance and no config is required
- ATPC – Automatic Transmit Power Control adjusts transmitter output power of the local system based on the varying signal level at the remote receiver.

Note that ATPC support depends on product’s specs.

ATPC allows the transmitter to operate at less than maximum power for most of the time and when fading conditions occur, transmit power will be increased as needed until the maximum configured value is reached. ATPC messages are carried over the radio over radio communication channel.

The purpose of ATPC is a) to reduce interference to other radios operation in the same channel/band and to allow better frequency reuse; and b) to reduce transmitter power consumption and prolong system's components life.

ATPC is supplementary to adaptive modulation and works before adaptive modulation changes modulation profiles.

Interference avoidance algorithm is implemented in order to overcome the main drawback of use of ATPC: interference from other links that may degrade the radio link performance. Besides setting the Target RSSI, the user can also set the Target CINR that will notify the remote transmitter to increase its Tx power to maintain CINR is above the threshold set.

Mode of operation: the local system compares the actual received RSSI to the ATPC Target RSSI. If the difference in values is 2dB or higher ($\Delta \geq 2\text{dB}$), a message to remote transmitter will be sent, asking to change its Tx power.

The Tx power can be changed the system's configured Tx power down to the ATPC Min Tx Power that was configured.

Configuration options:

- Checkbox to enable the ATPC operation.
- ATPC Target RSSI – allowed values -35 to -70 dBm (default -35 dBm).
- ATPC Min Tx Power – allowed values -35 to 0 dBm (default -35 dBm).
- Min CINR – allowed values -128 to 128 dB (default -128 dB).
- Encryption – checkbox to enable Encryption and field to enter the static key.

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

Encryption is a licensed feature that requires license for operation. Before configuring it, verify that license is available and enable the **encryption** license component.

- 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 is set automatically by the link.

Manually setting the Role is necessary only for asymmetric configurations.

Link ID – unique Tx and Rx Link IDs for links installed on the same site to avoid locking on the wrong transmitter. Link IDs must be identical on both ends for the link to be operational.

Link ID not available for EH-2200 product line.

- ARQ - checkbox to enable the mode and field to view the current status.

The ARQ (Automatic Repeat Request) is an algorithm that uses selective repeat (retransmission) to eliminate radio BER. The default mode is **Enabled**. When both sides are enabled and radio link is up, ARQ status will be **Established**.

Disabling the ARQ mode is not recommended as it may result in radio BER.

- Lowest Modulation – Lowest modulation profile. When modulation drops below this threshold, radio link will be down. It is used to limit the minimal modulation profile of the link. Default is QPSK 1 4 0.5 (lowest available).

4.3 Maintenance

Figure 4-3 Radio Page: Maintenance

This section allows configuring the following parameters:

- RF Loopback – checkbox to enable the internal RF loopback, set the timeout for clearing the loopback in seconds and select the modulation the ODU will be tested at.

Note that it will take the ODU to stabilize after loopback up to 3 minutes so set the loopback timeout accordingly (recommended 600 seconds).

Mute remote transmitter first to avoid interference with the loopback operation.

Loopback is done with MAC addresses swap.

Refer to the *Diagnostics* chapter of this manual for detailed description of the system’s loopbacks.

- Mute – checkbox to mute the transmitter with timeout in seconds. When muted, the ODU will not transmit.

4.4 Modulation Table

Settings Advanced Settings Maintenance Modulation Table Spectrum Analyzer Statistics	Modulation Table	Channel-width	Name	CINR Low	CINR High	Backoff	Capacity
		250Mhz	QPSK1	-128	11	5	20
		250Mhz	QPSK2	10	15	8	42
		250Mhz	QPSK3	11	17	8	175
		250Mhz	QAM16	16	20	8	350
		250Mhz	QAM64	19	127	8	500
		500Mhz	QPSK1	-128	14	5	20
		500Mhz	QPSK2	10	15	8	85
		500Mhz	QPSK3	11	17	8	350
		500Mhz	QAM16	16	20	8	700
500Mhz	QAM64	19	127	8	1000		

Figure 4-4 Radio Page: Modulation Table – EH-600 and EH-1200 product lines

Settings Advanced Settings Maintenance Modulation Table Statistics	Modulation Table	Channel-width	Name	CINR Low	CINR High	Backoff	Capacity
		250Mhz	BPSK1	-128	13	7	40
		250Mhz	BPSK2	9	16	7	100
		250Mhz	QPSK1	12	21	7	400
		250Mhz	QAM16	18	22.5	9	750
		250Mhz	QAM32	21.5	127	9	1000
		500Mhz	BPSK1	-128	13	7	80
		500Mhz	BPSK2	9	16	7	200
		500Mhz	QPSK1	12	21	7	800
		500Mhz	QAM16	18	22.5	9	1500
500Mhz	QAM32	21.5	127	9	2000		

Figure 4-5 Radio Page: Modulation Table – EH-2200 product line

The modulation table presents the available modulation profiles. The radio can be configured only to one of the profiles available in the table.

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

Note that different modulation tables may apply according to product used, the frequency channel used and ARQ status.

The modulation profiles and thresholds are optimized and should not be modified (can be configured via CLI only after consulting Siklu support).

4.5 Spectrum Analyzer

Site survey option to allocate free and un-interfered channels.

Radio link will go down and the ODU will scan all selected channels (about 1 minute per channel) and display a report of the spectrum scan.

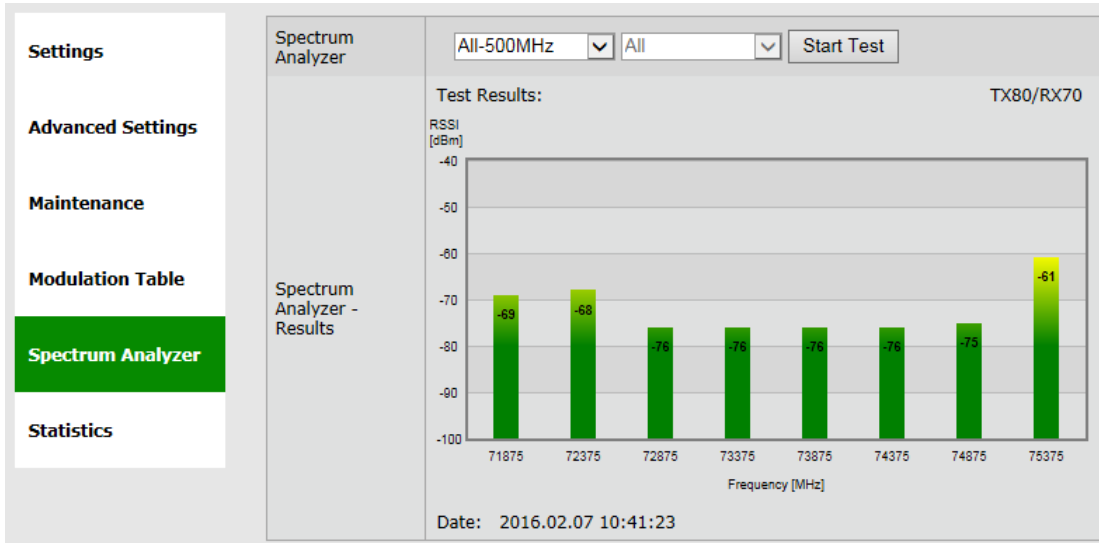


Figure 4-6 Radio Page: Spectrum Analyzer

Recorded values of ~-70dBm should be regarded as free from interference. In this example, 58375 channel is not free from interference and should not be used.

Note that Spectrum Analyzer feature availability depends of product used.

4.6 Statistics

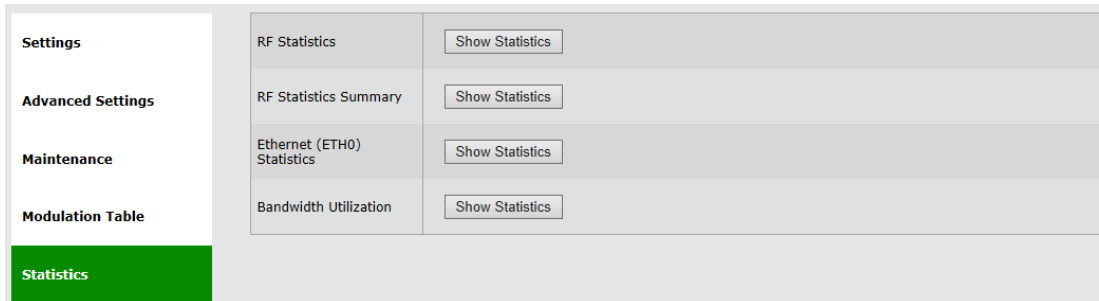


Figure 4-7 Radio Page: Statistics

Radio link's performance can be monitored using the advanced statistics counters.

Click **View Statistics** to review the local and remote RF Performance Monitoring statistics. Clicking **View Statistics** will open the **Statistics** page where all system's statistics can be reviewed.

Refer to the *Statistics* chapter of this manual for detailed description of the system's statistics.

4.7 CLI Commands

- Monitoring the RF configuration and status:

```
Show rf
```

- Encryption configuration:

```
Show encryption
```

- Alignment Probe configuration:

```
Show rf-debug probe-alignment-disable
```

- Viewing the modulation table (when ARQ is enabled):

```
Show modulation-arq
```

- Viewing the modulation table (when ARQ is disabled):

```
Show modulation
```

5 Ethernet Ports Configuration and Monitoring

The Ethernet ports parameters and monitoring are managed in the **Eth Ports** page.

The EtherHaul system has the following Ethernet interfaces:

- Host – Management interface
- Eth0 – Radio interface (RF)
- Eth1 – Line interface, port 1
- Eth2 – Line interface, port 2
- Eth3 – Line interface, port 3
- Eth4 – Line interface, port 4

The number of line interfaces and their type (RJ45 or SFP) depend on the product used.

This chapter includes the following topics:

- Settings
- Advanced Settings
- Maintenance
- Statistics
- CLI commands

5.1 Settings

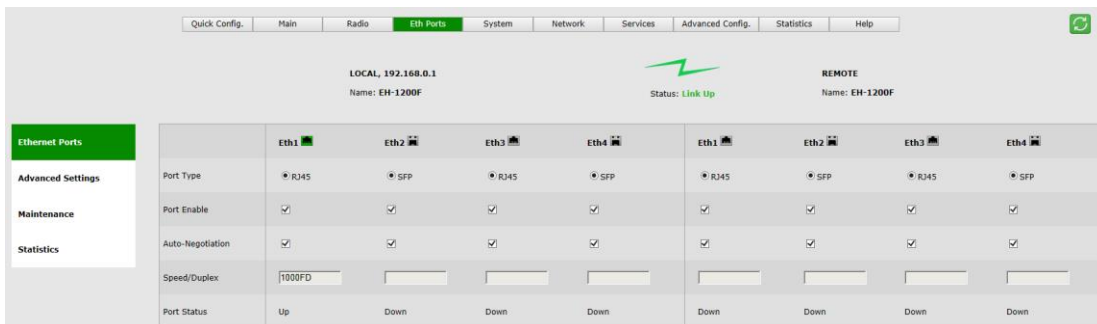


Figure 5-1 Eth Ports Page: Settings

This section allows configuring the following parameters:

- Port Type – RJ45 or SFP based on the physical port.
For EH-1200/TL systems with configurable port type, a radio-button allows selecting RJ45 or SFP.
- Port Enable – checkbox to enable the port.
Disable ports that are not in use so alarm will not be active (link down alarm).

- Auto Negotiation – checkbox to enable auto-neg.
- Speed/Duplex – speed (10/100/1000) and duplex (half/full) setting:
 - When Auto Negotiation Enabled – R/O field indicating the current speed/duplex.
 - When Auto Negotiation Disabled – manual configuration of the speed and duplex (for RJ45 ports: 10HD, 10FD, 100HD, 100FD, 1000HD or 1000FD; for SFP ports: 1000XHD or 1000XFD).
- Port status – Up or Down.

5.2 Advanced Settings

Ethernet Ports	Eth1	Eth2	Eth3	Eth4
Advanced Settings				
Suppress Alarm	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MTU	16384	16384	16384	16384
Alias				

Figure 5-2 Eth Ports Page: Advanced Settings

This section allows configuring the following parameters:

- Suppress Alarm – checkbox to enable alarm suppression (supported in EH-1200F/FX and EH-600T systems).
When enabled, ports in Status: Down will not generate an alarm.
- MTU – R/O field to indicate the Maximum Transmission Unit of the port.
- Alias – text field

5.3 Maintenance

Ethernet Ports	Eth1	Eth2	Eth3	Eth4
Maintenance				
Line Loopback	internal-mac-swap	disabled	disabled	disabled
Loopback Timeout	60	60	60	60

Figure 5-3 Eth Ports Page: Maintenance

This section allows configuring the following parameters:

- Line Loopback – checkbox to enable loopback on the port. External (towards the line side) or Internal (towards the radio side) loopback are available, with or without MAC addresses swap.

Refer to the *Diagnostics* chapter of this manual for detailed description of the system's loopbacks.

- Loopback Timeout – in seconds. Loopback will clear when timeout expires.

5.4 Statistics



Figure 5-4 Eth Ports Page: Statistics

Ethernet performance can be monitored using the advanced statistics counters.

Click **View Statistics** to review the local and remote Ethernet Performance Monitoring statistics. Clicking **View Statistics** will open the **Statistics** page where all system's statistics can be reviewed.

Refer to the *Statistics* chapter of this manual for detailed description of the system's statistics.

5.5 CLI Commands

- Monitoring the Ethernet ports configuration and status:

```
Show eth
```

- Changing Ethernet port type from RJ45 to SFP on EH-1200/EH-1200TL systems:

```
Set eth eth1 ether-type 1000xfd
```

6 System Configuration and Monitoring

The system general parameters and monitoring is managed in the **System** page.

This chapter includes the following topics:

- Settings
- Advanced Settings
- Maintenance
- Event Configuration
- CLI commands

The **Maintenance** section consists of the system's configuration files and file-system management, including:

- File Transfer
- SW Upgrade
- Licensing
- Scripts
- Configuration Management

6.1 Settings

	LOCAL, 192.168.0.1 Name: EH-1200F	REMOTE Name: EH-1200F
Model Name	EH-1200F-ODU-H-EXT	EH-1200F-ODU-L-EXT
Product Name	EH-1200F	EH-1200F
Date & Time	Date: 2014.01.20 Time: 11:29:03	Date: 2014.05.20 Time: 11:29:05
Inventory	Serial No. F410060501 SW Version: 6.0.0.11606	Serial No. F405057167 SW Version: 6.0.0.11606
Host	00:24:a4:01:e5:98 Eth0 (RF) 00:24:a4:01:e5:99	00:24:a4:01:d3:c8 Eth0 (RF) 00:24:a4:01:d3:c9
MAC Address	Eth1 00:24:a4:01:e5:9a Eth2 00:24:a4:01:e5:9b	Eth1 00:24:a4:01:d3:ca Eth2 00:24:a4:01:d3:cb
	Eth3 00:24:a4:01:e5:9c Eth4 00:24:a4:01:e5:9d	Eth3 00:24:a4:01:d3:cc Eth4 00:24:a4:01:d3:cd

Figure 6-1 System Page: Settings

This section allows configuring the following parameters:

- Model – R/O field.
- Name
- Date & Time – Date [YYYY.MM.DD], Time [HH:MM:SS]

Note:



Full inventory information of the system is stored as a file (inventory.ini) in the File System and can be retrieved by the user.

- Inventory – R/O fields. Serial Number and active SW version.
- MAC Address – R/O fields for each port.

6.2 Advanced Settings

General	System Uptime	<input type="text" value="0000:00:12:34"/>
Advanced Settings	Voltage	<input type="text" value="51 DC"/>
Maintenance	HW Version	<input type="text" value="A0"/>
Event Configuration	Max Rate [Mbps]	<input type="text" value="2000"/>
	Contact	<input type="text" value="undefined"/>
	Location	<input type="text" value="undefined"/>
	Loopback Permission	<input type="text" value="Enabled"/> ▼
	Control Packets CoS	<input type="text" value="Disabled"/> ▼
	Queue Length Optimization	<input type="text" value="msec"/> ▼ <input type="text" value="2"/>
	PSE (PoE Out)	<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>ETH2 Enable <input type="checkbox"/></p> <p>Status: <input type="text" value="Off"/> V-out: <input type="text" value="0.0 V"/> I-out: <input type="text" value="0.0 mA"/></p> </div> <div style="border: 1px solid #ccc; padding: 2px 5px;">PSE Reset</div> </div>

Figure 6-2 System Page: Advanced Settings

This section allows configuring the following parameters:

- System Uptime – R/O field. Time elapsed from last power on.
- Voltage – R/O field. Input voltage and indication DC or PoE.
- Contact.
- Location.
- HW Version – R/O field.
- Loopback Permission – control the permission to perform system loopbacks
 - Enabled (default): all loops allowed.
 - Disabled: no loops allowed.
 - MAC-SWAP: only loops with MAC-SWAP allowed.

- CoS Control Packets – Allows sending Ethernet control packets to a specific queue for prioritization. Enter the queue number (0..7, where 7 is the highest queue).

If disabled, the control packets will be prioritized based on the QoS policy in effect (pBits, VIDs, DSCP...).

The prioritized control packets:

- MPLS, LACP, and OSPF PDUs
- Spanning Tree Protocol (bridges, provider bridges)
- Link Layer Discovery Protocol
- Ethernet flow control (Pause frame)
- Ethernet OAM Protocol
- Ethernet CFM Protocol
- Precision Time Protocol (PTP) version 2 over Ethernet (Layer-2)
- Queue Length Optimization – for supporting models only.

Buffer length and size optimization (default is 2mSec). You may want to optimize the buffers length (in mSec) or size (in Kbps) when transferring high bandwidth video streaming.

- PSE (PoE Out) – for supporting models only.

13W/53W on EH-600T and EH-2200F (Port #3), 26W on EH-1200TX (Port #2).

- Enable – checkbox to enable the PSE.
- Status – On, Off, Auto-Off (system will switch to Auto-off after several attempts to power up external device (typically when external device power is higher than PSE max output).
- V-Out, I-Out – Voltage and Current monitored output levels.
- PSE Reset – reinitialize the attempts to power up external device

6.3 Maintenance

6.3.1 File Transfer

Figure 6-3 System Page: Maintenance – File Transfer

The administration of the file system is controlled by the **File Transfer** session. It includes the configuration files, SW version, licenses, scripts, inventory and more.

File transfer is available over HTTP when using the web-GUI. In this case, no external FTP, TFTP or SFTP server is required for file transfer.

In order to transfer files over FTP/TFTP/SFTP, FTP/TFTP/SFTP server must be running and the file transfer attributes must be configured.

This section allows configuring the following parameters:

- Protocol – HTTP, FTP, TFTP or SFTP.
- Server IP – the IP address of the server where the FTP/TFTP/SFTP server is running on.
- Path – the path of the stored file (or target destination) relative to the directory used for file transfers as configured in the server. If left blank, file transfer will be from/to the server's Root (or Home) directory.
- User – user name, as defined in the server. Leave blank if anonymous user defined.
- Password – password, as defined in the server. Leave blank if a anonymous user

The most simple and recommended way to transfer files is using HTTP file transfer (supported starting 6.9.x SW release).

Note:



For prior versions, or when using the CLI, use FTP (make sure that the FTP service is free and not blocked by Firewall/Antivirus or occupied by other software or services) or TFTP (often not blocked or used by other software services).

defined.

6.3.2 SW Upgrade

SW Upgrade	1.Version: <input type="text" value="7.0.0.16648"/>	Status: <input type="text" value="Active"/>
	2.Version: <input type="text" value="6.9.0.16215"/>	Status: <input type="text" value="Offline"/>
	SW File Name: <input type="text"/>	<input type="button" value="Browse"/> <input type="button" value="Download"/>
	Accept Timeout [Sec]: <input type="text"/>	<input type="button" value="Run"/> <input type="button" value="Accept"/>

Figure 6-4 System Page: Maintenance – SW Upgrade

The EtherHaul system supports two software version, maintaining an Active (running) and an Offline (standby) software versions (banks) that allow software upgrade with minimum service interruption.

The software upgrade process consists of 3 steps:

- 1) Download. Transferring the new software file to the system (to the offline software bank).
- 2) Upgrade. Switching the active status between the banks so the downloaded software becomes active.
- 3) Accept. Use timeout to verify that the new active software performs as expected and accept the upgrade to make it permanent.

The **SW Upgrade** section displays the software versions currently resides in the banks and their status (Active or Offline).

The software download is done using HTTP or an external FTP/TFTP/SFTP server. Refer to server's configuration as defined in the **File Transfer** section.

This section allows configuring the following parameters:

- SW File Name – The name of the software file to download.
- Accept Timeout [Sec] – time out in seconds in which the new software should be accepted. If the new software is not accepted within the timeout period, the system will reboot and rollback to the previously active software. It is recommended to use 600 seconds timeout whenever upgrading a software.

Click **Download** to start the software download from the server to the system.

Click **Upgrade** to activate the downloaded software. This action will result in system reboot.

Click **Accept** to accept the new SW.

Always upgrade both sides!

Note:



When upgrading an operational link, upgrade the remote system first and then the local system. Accept the software at both ends after verifying that the link performs as expected.

6.3.3 Licensing

Licensing	Data-Rate	<input type="text" value="1000"/>	Max Data-Rate: 1000
	Encryption	<input checked="" type="checkbox"/>	License Available
	L2 (OAM)	<input checked="" type="checkbox"/>	License Available
	L2 (Resiliency)	<input checked="" type="checkbox"/>	License Available
	SyncE	<input checked="" type="checkbox"/>	License Available
	ExtendMM™	<input checked="" type="checkbox"/>	License Available
	Extra-range	<input type="checkbox"/>	License Not Available
	PSE (PoE Out)	<input type="checkbox"/>	License Not Available
	License File Name:	<input type="text" value="F415062864.lic"/>	<input type="button" value="Download"/>

Figure 6-5 System Page: Maintenance – Licensing

The EtherHaul provides easy migration to support Gigabit throughput and advanced features, 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.

The following EtherHaul licenses can be purchased:

- Data rate (capacity) – from 100 up to 1000Mbps (or 2000Mbps for EH-2200 product line)
- Encryption – AES encryption
- L2 – Layer 2 networking capabilities
 - L2 (OAM) – Operation, Administration and Maintenance
 - L2 (Resiliency) – Ethernet Ring Protection
- SyncE – Synchronization (SyncE and IEEE1588)
- ExtendMM – Extending link range using Sub-6GHz radio link backup
- Extra-range – long range links (up to up to 15Km for EH-1200/1200F product line)
No limitation of link distance on EH-2200/2500 product line.
EH-600 product line systems prior to HW Rev C0 are limited to 1000m.
- PSE – PoE out (13W, 26 or 53W, according to product specs).

The data rate license active on the system dictates the highest modulation profile the link will reach:

Note:



- Data rate of 100 or 200 Mbps – max modulation profile QPSK 3.
- Data rate of 500 Mbps – max modulation profile QAM16.
- Data rate of 1000 Mbps – max modulation profile QAM64.

License upgrade key is a signature file containing the license configuration that is based on the system's serial number. License file will be provided by Siklu as a text file that can be opened with any text editor. The license file name will always be *<system_serial_number>.lic*.

The license upgrade is done using HTTP or an external FTP/TFTP/SFTP server. Refer to server's configuration as defined in the **File Transfer** section.

The license upgrade process consists of 2 steps:

- 1) Download. Transferring the new license file to the system.
- 2) Enable. Enabling the license components. Note that if you restore factory default configuration, the system will come up with the available license components enabled.

The **Licensing** section displays the current configuration of the license components (data-rate and features enable/disable) and states if license component is available (permission).

The **License File Name** is an R/O field that will always be according to the system's serial number (<system_serial_number>.lic).

Click **Load** to load a new license file. As the license file name is always <system_serial_number>.lic, it will be displayed as the License File Name.

Use the checkboxes to enable/disable license components.

Note:



Enabling license components will introduce a momentary service disruption.

6.3.4 Scripts

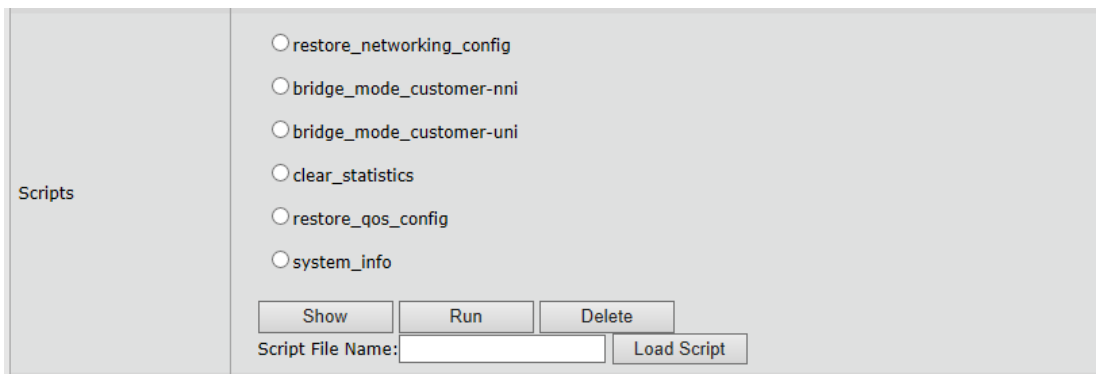


Figure 6-6 System Page: Maintenance – Scripts

The EtherHaul supports the use of pre-composed, multiple-line command scripts.

A script is simply a list of CLI commands, saved as a text file that runs locally on the system. Script output is displayed on a script output screen and can be copied and saved.

The **Scripts** section displays the scripts that were loaded to the system.

There are useful scripts that are pre-loaded to the system in the factory:

- 1) **clear_statistics** – this script clears all the statistics counters of the system, including RF statistics, Ethernet statistics, VLAN statistics and Queue statistics.
- 2) **System_info** – this script collects all the relevant system status, logs, configurations and statistics.
- 3) **Restore_networking_config** – restore all Ethernet networking configuration (VLANs) to default. Refer to the *Ethernet Services Configuration and Monitoring* chapter for description.
- 4) **Restore_qos_config** – restore all Quality of Service configuration to default. Refer to the *Quality of Service* chapter for description.

For EH-1200F/FX and EH-600T systems, additional scripts are available:

- 5) **Bridge_mode_customer-nni** – change bridge configuration. Refer to the *Ethernet Services Configuration and Monitoring* chapter for description.
- 6) **bridge_mode_customer-uni** – change bridge configuration. Refer to the *Ethernet Services Configuration and Monitoring* chapter for description.



Whenever contacting Siklu for support, send the output of this script from both systems for efficient service (copy the output to a text file).

Select a script from the list and click **Show** to view (pop-up screen) list of commands composing this script.

Click **Run** to run the selected script. The commands in the script will be executed one after the other. Pop-up screen will display the progress and outcome of the script.

Click **Delete** to delete the selected script.

Enter a file name and click **Load Script** to load a new script file.

When clicking **Load Script**, the system will look for the file at the FTP directory and will store it in the file system as a new script (under directory *scripts/*).

6.3.5 Configuration Management

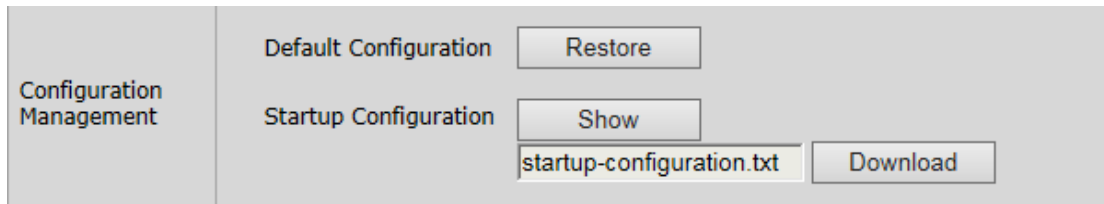


Figure 6-7 System Page: Maintenance – Configuration Management

This section allows configuring the following parameters:

- **Default Configuration** – Click **Restore** to delete current *startup-configuration.txt* file. After reboot, the system will come up with the factory default configuration (unless *customer_default_config.txt* file is present).
- **Startup Configuration** – Click **Show** to view (pop-up screen) the *startup-configuration.txt* file. The startup-configuration file lists the commands that build the configuration the system will come up with after reboot.

Click **Load** to load a new startup-configuration file that will replace the current file and will be used after next system reboot.

When clicking **Load**, the system will look for a file named *startup-configuration.txt* at the FTP directory and will store it in the file system (*flash:*) as the new startup-configuration file. After next reboot, the system will come up with the new configuration.

6.4 Event Configuration

Event	Trap	Alarm	Threshold
Temperature High	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Low: <input type="text" value="-40"/> High: <input type="text" value="80"/> Hysteresis: <input type="text" value="1"/>
CINR Out Of Range	<input type="checkbox"/>	<input type="checkbox"/>	Low: <input type="text"/> Hysteresis: <input type="text"/>
RSSI Out Of Range	<input type="checkbox"/>	<input type="checkbox"/>	Low: <input type="text"/> Hysteresis: <input type="text"/>
Lowest Modulation	<input type="checkbox"/>	<input type="checkbox"/>	
Link Down	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Loopback Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Tx Mute Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
CFM Fault Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
QL EEC1 Or Worse	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Ref Clock Switch	<input checked="" type="checkbox"/>		
SFP In	<input checked="" type="checkbox"/>		
Modulation Change	<input checked="" type="checkbox"/>		
Cold Start	<input checked="" type="checkbox"/>		

Figure 6-8 Network Page: Event Configuration

The EtherHaul supports masking of individual/group alarms and events. In case alarm is masked, it is not displayed in the Active Alarms and Event Log and no trap is sent.

By default, none of the alarms are masked but the RSSI, CINR and Lowest Modulation threshold-crossing alarms. In addition, some alarms have configurable thresholds to raise and clear alarm.

This section allows configuring the following parameters:

- Event – the event/group of events to be configured
- Trap – checkbox to enable sending SNMP trap for this event.
- Alarm – checkbox to enable raising an alarm for this event (meaning, showing it in the active Alarms list and in the log file). Note that not all events can be configured as Alarms.
- Threshold – the following events have configurable thresholds for alarm raise/clear and for sending traps. The threshold hysteresis can be defined (to avoid toggling alarms).

- Temperature – when system temperature exceeds the High or Low thresholds. Note that system temperature is typically 15-25°C higher than ambient temperature.
- CINR – when radio CINR drops below the Low threshold.
- RSSI – when radio RSSI drops below the Low threshold.
- Lowest Modulation – the threshold is configured in the Radio Configuration section.

Threshold-crossing alarms are supported for EH-1200F/FX and EH-600T systems only.

Refer to the *Alarms* section under *Diagnostics* chapter of this manual for detailed description of the system's alarms.

6.5 CLI Commands

- Restoring factory default configuration:

```
clear startup-configuration
reset system
```

- Viewing the startup configuration

```
copy startup-configuration display
```

- Viewing the currently running configuration

```
copy running-configuration display
```

- Loading new startup configuration (for example, using FTP):

```
copy ftp://<ftp_user>:<ftp_password>@<ftp_server_ip>/startup-configuration.txt flash:startup-configuration.txt
```

- Downloading SW (for example, using FTP):

```
copy sw ftp://<ftp_user>:<ftp_password>@<ftp_server_ip>/<sw_file_name>
```

- Upgrading and accepting SW:

```
run sw immediately 600

accept sw
```

- Viewing list of scripts:

```
show script
```

- Deleting script:

```
clear script <script_name>
```

- Loading a new script (for example, using FTP):

```
copy ftp://<ftp_user>:<ftp_password>@<ftp_server_ip>/<script_file_name>
flash:scripts/<script_file_name>
```

- Viewing list of files in the File System:

```
dir flash:
```

- Event Configuration:

Viewing event configuration (masking and thresholds):

```
show event-cfg
```

Configuring events:

```
set event-cfg rssi-out-of-range trap-mask no alarm-mask no threshold-low
-50
```

Customer Default Config

You can use the file system to copy to the system *customer_default_config.txt* file.

The Customer Default Config allows loading a specific default config for customers. Customers may create their own specific default configuration file that will be used after restoring default configuration. In case *customer_default_config.txt* is present in the file system, after restoring default configuration the system will come up with this configuration.

- Loading new customer default configuration (for example, using FTP):

```
copy ftp://<ftp_user>:<ftp_password>@<ftp_server_ip>/customer-default-
config.txt flash: customer-default-config.txt
```

7 Network Configuration and Monitoring

General parameters regarding communication and network connectivity are managed in the **Network** page.

This chapter includes the following topics:

- General Settings
- Advanced Settings
- Maintenance
- Users Administration
- LLDP
- CLI Commands

7.1 General

7.1.1 IP Address

The screenshot shows the 'Network' configuration page for a device named 'EH-1200F'. The 'LOCAL' interface (192.168.0.1) and 'REMOTE' interface (EH-1200F) are both 'Link Up'. The 'IP Address' section is active, showing two columns of configuration tables. The left column is for the LOCAL interface and the right column is for the REMOTE interface. Each table has columns for '#', 'Type', 'IP Address', 'Prefix-length', and 'VLAN'. The LOCAL interface has two entries: #1 with Type 'Static', IP Address '192.168.0.1', Prefix-length '24', and VLAN '0'; and #2 with Type 'Static', IP Address '10.10.10.1', Prefix-length '24', and VLAN '0'. The REMOTE interface has two entries: #1 with Type 'Static', IP Address '192.168.0.1', Prefix-length '24', and VLAN '0'; and #2 with Type 'Static', IP Address '10.10.10.2', Prefix-length '24', and VLAN '0'. There are 'Add IPv4' and 'Add IPv6' buttons at the bottom of each table.

Figure 7-1 Network Page: General – IP Address

The EtherHaul supports up to four IP addresses that can be associated with different VLANs. IPv4 or IPv6 can be configured. IP addresses may also be acquired by DHCP.

This section allows configuring the following parameters:

- # - Index (1-4)
- Type – Static or DHCP
- IP Address – Default is 192.168.0.1
- IP Prefix Length – Default is 24 (equivalent to Mask of 255.255.255.0)
- VLAN – 0 (not defined, meaning the IP is not associated with specific VLAN)

Click the **Add IPv4** or **Add IPv6** to add an IP address.

Click the **Trash** icon to clear an IP. Note you cannot clear the IP address you used to log in to the system.

Note: It is recommended to leave the default IP address (#1) and add the unique IP address as #2. This will allow users to login to the system when on site even if they do not know the configured IP of the system.



7.1.2 Default Gateway and Static Routes

Default Gateway

IP Address : 10.10.10.250

IPv6 Address :

Figure 7-2 Network Page: General – Default Gateway

This section allows configuring a single default gateway for IPv4 and IPv6.

The EtherHaul allows defining up to 10 static routes, in which you can define the network (Destination + Prefix-length) and the Next-Hop.

When entering default gateway, it is translated to a static route (#1).

Setting and viewing static routes is available via the CLI only.

7.1.3 SNMP Managers

SNMP Managers

#	IP Address	UDP-Port	Security Name	SNMP Ver	Engin ID
1	10.10.10.200	162	public	v2c	local

Add

Figure 7-3 Network Page: General – SNMP Managers

The EtherHaul allows defining up to five managers that will receive SNMP traps. Traps can be sent using SNMPv2c or SNMPv3.

This section allows configuring the following parameters:

- # - Index (1-5).
- IP Address – Destination IP Address.
- UDP Port – port number for sending traps (default is 162).
- Security Name (community) – same as the trap community name in SNMPv2c and as the user name in SNMPv3 (default is public).
- SNMP Ver – SNMP version: SNMPv2c or SNMPv3 (default is SNMPv2c).
- Engine ID – Used for SNMPv3.

For SNMPv3 configuration, refer to the *SNMPv3 Users Configuration* section under *System Administration* chapter of this manual.

Click the **Add** to add SNMP manager.

Click the **Trash** icon to clear SNMP manager.

7.1.4 NTP

The screenshot shows a configuration window titled "NTP". It contains three input fields: "Server IP" with the value "192.168.44.250", "Sec. Server IP" with the value "0.0.0.0", and "TMZ" with the value "-4". Each field has a small 'x' icon to its right for clearing the input.

Figure 7-4 Network Page: General – NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of network elements over packet-switched, variable-latency data networks.

NTP provides a connectionless service (UDP in the Transport Layer).

The EtherHaul has an embedded NTP client. It can synchronize the host clock to any NTP server in the LAN/Internet to deliver accurate and reliable time.

Primary and secondary servers can be defined.

This section allows configuring the following parameters:

- Server IP – primary NTP server IP Address
- Secondary Server IP – secondary NTP server IP Address
- TMZ – time zone shift in hours (-12 to 14). Note that changing the TMZ value will change the time entered.

7.2 Advanced Settings

7.2.1 Management Access List

#	IP/IPv6 Address	Prefix Length	
1	0.0.0.0	0	
2	0000:0000:0000:0000:0000:0000:0000:00	0	

Add

Figure 7-5 Network Page: Advanced Settings – Management Access List

List of authorized IPv4/IPv6 IP addresses (or IP address ranges) that are permitted to access the Host (management).

The default configuration allows all IP address to access the Host.

This section allows configuring the following parameters:

- # - Index (1-8)
- IP Address
- Prefix-Length – together with the IP address determine IP address range

7.2.2 SNMP Agent

SNMP Agent

Read Community: Write Community: SNMP-Version:

Figure 7-6 Network Page: Advanced Settings – SNMP Agent

SNMP Agent properties (SNMP passwords).

This section allows configuring the following parameters:

- Read Community – default is **public**. Used for Read access (SNMP Get).
- Write Community – default is **private**. Used for Read/Write access (SNMP Set).
- SNMP-Version – SNMPv2c or SNMPv3. Default is v2c.

7.2.3 Syslog Server

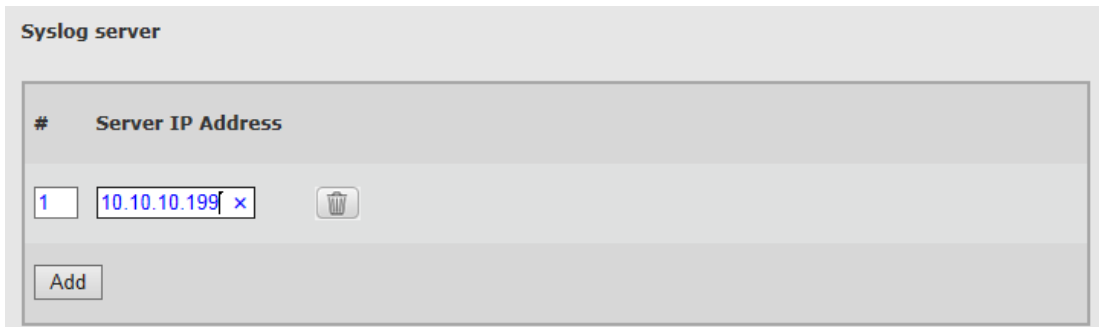


Figure 7-7 Network Page: Advanced Settings – Syslog Server

When set, all system's event and alarms will be sent to servers. Up to 5 different Syslog servers can be configured.

Syslog servers listen to Port 514.

7.3 Maintenance

7.3.1 Iperf Test

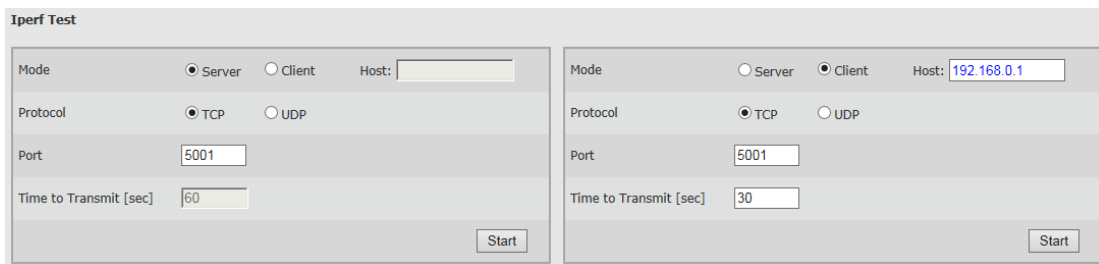


Figure 7-8 Network Page: Maintenance – Iperf Test

Built-in Iperf client/server for over the link TCP/UDP test.

Configure one side as Server and run it (click Start) and remote end as Client (and enter the server IP address).

Note that Iperf test run in parallel to traffic over the link.

Iperf output:

```

-----
Client connecting to 192.168.0.1, TCP port 5001
-----
[SUM] 0.0- 3.0 sec 148 MBytes 413 Mb/s/sec
[SUM] 3.0- 6.0 sec 150 MBytes 418 Mb/s/sec
[SUM] 6.0- 9.0 sec 148 MBytes 415 Mb/s/sec
[SUM] 9.0-12.0 sec 148 MBytes 415 Mb/s/sec
[SUM] 12.0-15.0 sec 149 MBytes 416 Mb/s/sec
    
```

[SUM] 15.0-18.0 sec 147 MBytes 412 Mb/s/sec
[SUM] 18.0-21.0 sec 148 MBytes 412 Mb/s/sec
[SUM] 21.0-24.0 sec 148 MBytes 415 Mb/s/sec
[SUM] 24.0-27.0 sec 150 MBytes 420 Mb/s/sec
[SUM] 27.0-30.0 sec 146 MBytes 409 Mb/s/sec
[SUM] 0.0-30.1 sec 1.45 GBytes 414 Mb/s/sec

Note: Iperf Test results are typically ~90% of the expected TCP/UDP when using external laptops, up to ~600Mbps.



For TDD systems – expected TCP rate is ~415-430Mbps

For FDD systems – expected TCP rate is ~500-600Mbps

7.3.2 Connectivity

The screenshot shows a section titled "Connectivity". It contains two rows of input fields and buttons. The first row has an "IP Address" label followed by a text input field, a "Ping" button, and a "Trace Route" button. The second row has an "IPv6 Address:" label followed by a text input field, a "Ping6" button, and a "Trace Route6" button.

Figure 7-9 Network Page: Maintenance – Connectivity

Enter target IP address (IPv4 or IPv6) and click **Ping** or **Trace Route** to test connectivity. Pop-up screen will display the results.

7.3.3 ARP Table

The screenshot shows a section titled "ARP Table". It contains a table with three columns: "IP Address", "MAC Address", and "Status". The table has one row with the following values: "192.168.0.199", "f0:de:f1:6a:11:6a", and "dynamic". To the right of the "dynamic" status is a trash can icon. Below the table is an "Add" button.

Figure 7-10 Network Page: Maintenance – ARP Table

The ARP table is used to map between IP addresses and physical addresses. You can map specific IP address to specific MAC address and create or modify entries in the ARP table.

7.4 Users Administration

7.4.1 Users

The screenshot shows the 'Users Administration' page. On the left is a sidebar with navigation links: General, Advanced Settings, Maintenance, **Users Administration** (highlighted in green), and LLDP. The main content area is titled 'Authentication Mode' and features three radio buttons: Local, Radius, and Tacacs. To the right of these is a 'Shared Secret' field containing the text 'none'. Below this is a table with columns 'Name', 'Type', and 'Password'. The table contains one row with 'admin' in the Name field, 'admin' in the Type field, and '*****' in the Password field. An 'Add' button is located below the table.

Figure 7-11 Network Page: Users Administration – Local Authentication

Internal user management and external Radius or TACACS server are supported.

The Users administration page will be updated based on the selected **Authentication Mode**.

For internal user management (standard user/passwords that are configured in the device), select **Local** as the **Authentication Mode**.

The EtherHaul supports 4 types of users that can be defined locally:

- **User** – Read-only access. Cannot view user names, passwords, and other security settings.
- **Tech** – Read-only access for all configuration settings. Can clear statistics, alarms, and log lists, and run diagnostics.
- **Super** – Read-write access for all configuration settings but user names, passwords, and other security settings.
- **Admin** – Full read-write.

A single default admin user is defined with user name **admin** and password **admin**.

Up to 32 different users can be defined of different types. Note that only one admin type user can be defined and the user name **admin** cannot be changed (only the password can be changed).

For Radius or TACACS AAA configuration, refer to the *TACACS+/RADIUS Users Administration* section under *System Administration* chapter of this manual.

7.4.2 Password Strength

The screenshot shows the 'Password Strength' settings. There are two input fields: 'Password Min Length' with the value '8' and 'Password Min Difference' with the value '1'.

Figure 7-12 Network Page: Advanced Settings – Password Strength

For password strength enforcement.

This section allows configuring the following parameters:

- Password Min Length - minimum password length (0 to 16 characters). Default is 8.
- Password Min Difference - minimum password difference between characters (0 to 5). Default is 1.

7.5 LLDP

The Link Layer Discovery Protocol (LLDP) is a unidirectional neighbor discovery protocol (as per IEEE 802.1AB).

LLDP performs periodic transmissions of the system's capabilities to the connected stations. LLDP frames are not forwarded, but are constrained to a single link. The information distributed by the protocol is stored in a topology data base. This information can be retrieved by the user in order to easily resolve the network's physical topology and its associated stations.

LLDP enables the discovery of accurate physical network topologies, meaning which devices are neighbors and through which ports they connect. It enables the EtherHaul to discover other network elements that are connected to it, including the discovery of third-party network elements, and enables easier integration of EtherHaul links in an LLDP supported networks.

7.5.1 LLDP Configuration

Port	State	VID	IP Index
Eth0 (RF)	rx-tx	none	lowest
Eth1	disabled	none	lowest
Eth2	disabled	none	lowest
Eth3	disabled	none	lowest
Eth4	disabled	none	lowest

Figure 7-13 Network Page: LLDP Configuration

LLDP can be configured for each one of the Ethernet ports, including the radio port (Eth0). LLDP information may be sent over VLAN or without VLAN (untagged).

This section allows configuring the following parameters:

- Port – Eth0, Eth1-Eth4

- Config – enabling LLDP on the port. Select **rx-tx** to enable LLDP. Note that you may work with uni-directional LLDP by selecting **rx** or **tx** only.

Note: By default LLDP is enabled on the radio port (Eth0) and disabled on all line Ethernet ports).



Disabling LLDP on all ports including the radio, will pass LLDP packets transparently over the radio.

- VID – VLAN ID that LLDP messages will be sent on. Default is **none** (untagged).
- IP Index – Lowest, Highest or IP index (1-4). The IP address the system will respond with in the LLDP information reply. Default is **Lowest**.

7.5.2 LLDP Status

LLDP Port Status	
Port:	Eth0
Chassis ID	192.168.0.2
Chassis ID Subtype	network-addr
Port ID	00:24:a4:01:d3:c9
Port ID Subtype	mac-addr
Port Description	Eth0
System Name	EH-1200F
System Description	EH-1200F
Mng. Address	ip 192.168.0.2 1

Figure 7-14 Network Page: LLDP Status

This section displays the information received from the peer device:

- Chassis ID – displays the IP address (network address, typically refer to IP #1) of remote device
- Chassis ID Subtype – will be 'network-addr'
- Port ID – displays the received MAC address

- Port ID Subtype – will be 'mac-addr'
- Port Description – The port connected at the peer device
- System Name – of peer device
- System Description – of peer device
- Mng. Address – IP address that peer device reports. As there can be multiple IP addresses, the device reports the IP address according to **LLDP**
Configuration: IP Index configured above.

7.6 CLI Commands

- IP Addresses (IPv4):

Viewing IP addresses:

```
show ip
```

Setting IP address (static IP example):

```
set ip 2 ip-addr static 10.10.10.1 prefix-len 23 vlan 12
```

Setting IP address (DHCP example):

```
set ip 2 ip-addr dhcp
```

Deleting IP address:

```
clear ip 2
```

- IPv6 IP Addresses:

Viewing IPv6 addresses:

```
show ipv6
```

Setting IPv6 IP address (static IP example):

```
set ipv6 2 ipv6-addr static 0001:0001:0001:0001:0001:0001:0001:0001  
prefix-len 32 vlan 200
```

Deleting IPv6 address:

```
clear ipv6 2
```

- Default Gateway and Static Routes:

Viewing default gateway and routes (IPv4):

```
show route
```

Viewing default gateway and routes (IPv6):

```
show route6
```

Setting default gateway and routes (IPv4):

```
set route 1 dest 0.0.0.0 prefix-len 0 next-hop 82.166.81.138
```

Setting default gateway and routes (IPv6):

```
set route6 1 dest 0001:0001:0001:0001:0001:0001:0001:0001 prefix-len 0  
next-hop 0001:0001:0001:0001:0001:0001:0001:0002
```

- SNMP Managers:

Viewing SNMP managers:

```
show snmp-mng
```

Setting SNMP managers:

```
set snmp-mng 1 ip-addr 192.168.0.250 udp-port 162 snmp-version v2c  
security-name public
```

Deleting SNMP managers:

```
clear snmp-mng all
```

- NTP:

Viewing NTP configuration:

```
show ntp
```

Setting NTP servers:

```
set ntp 1 server 10.10.250.222 secondary-server 192.168.0.250 tmz 2
```

- Management Access List:

Viewing access list:

```
show access-list
```

Setting access list:

```
set access-list 1 ip-addr 192.168.0.0 prefix-len 24
```

Deleting access list:

```
clear access-list all
```

- SNMP Agent properties:

Viewing properties:

```
show snmp-agent
```

Setting SNMP communities:

```
set snmp-agent read-com public write-com private snmp-version v2c
```

- Users:

Viewing users list:

```
show user
```

Configuring users:

```
set user JohnS passw happy123 type super
```

Deleting user:

```
clear user JohnS
```

- Password Strength:

Viewing password strength properties:

```
show password-strength
```

Setting password strength:

```
set password-strength min-length 8 min-difference 0
```

- Syslog Server:

Viewing servers:

```
show syslog

Configuring server:
set syslog 2 server 192.168.0.222

Deleting user:
clear syslog all
```

- Connectivity:

```
Ping:
ping 192.168.0.222

ping configuration options:
ping [-c <num-packets 1..32000>] [-t] [-l <packet-length 0..5000>] <host>
-t - ping until stopped by ctrl/c

Trace Route:
tracert 192.168.0.222

tracert configuration options:
tracert [-h <maximum-hops 1..255>] [-w <timeout, sec, 1..86400>] <host>

Ping (IPv6):
Ping6 0001:0001:0001:0001:0001:0001:0001:0002

Trace Route (IPv6):
Tracert6 0001:0001:0001:0001:0001:0001:0001:0002
```

- ARP Table (Address Translation):

```
Viewing ARP Table:
show arp

Configuring entries in the ARP table:
Set arp 192.168.0.222 mac-addr 01:02:03:04:05:06

Deleting entries:
clear arp 192.168.0.222
```

- LLDP:

```
Viewing LLDP configuration:
show lldp

Configuring LLDP:
set lldp eth1 admin rx-tx vid 500 ip-index lowest

Viewing LLDP status:
show lldp-remote
```


8 Ethernet Services Configuration and Monitoring

The Ethernet services (VLAN) parameters and monitoring are managed in the **Services** page.

This chapter includes the following topics:

- Bridge Architecture
- Bridge Mode
- Link Aggregation (LAG)
- Default Bridge Configuration
- Services Setup
 - VLANs
 - Port Network Type
 - Bridge-Port (PVID)
- Maintenance
- Statistics
- CLI Commands
- Advanced Ethernet Networking Configurations

8.1 Bridge Mode

For supporting models only.

Bridge mode is used in order to minimize config by users when implementing common networking scenarios.

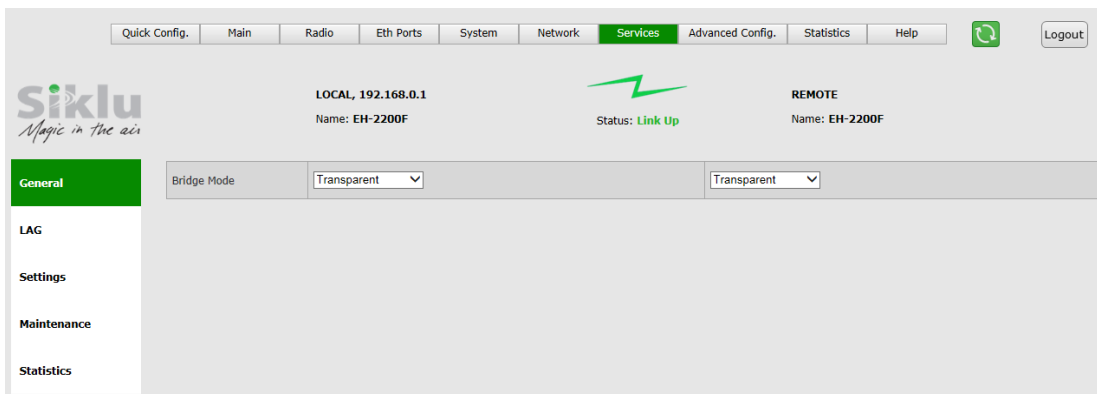


Figure 8-1 Services Page: General – Bridge Mode

Transparent – IEEE 802.1d Transparent Bridge. In this mode, all traffic (both tagged and untagged) is transparently forwarded between all ports and over the radio.

Pipe – traffic is forwarded over the radio separately for each port, providing pipe connection over the radio:

Port 1 ↔ Port 1

Port 2 ↔ Port 2

...

Pipe mode is implemented by internally tagging the traffic (C-Vlans) coming from each line port with dedicated S-Vlan (1001-1004). Each S-Vlan is connected to the port it came from, the radio and the Host (to allow management over each one of the line ports).

Pipe Unique FDB – Same as Pipe mode, but when each S-VLAN is learned and stored on separate FDB (forwarding database).

May be used for certain LAG connections between switches across the radio.

Port Isolation – allows defining an uplink port, where all traffic is sent to, while maintaining separation between other ports.

This mode allows aggregating traffic from different ports to other port (not the radio). Pipe mode is a specific case where the uplink port is the radio.

Out Of Band – allows local management only over the selected port. No management information will be carried over the radio.

Note that as no management over the radio, the Web-GUI communication channel will be down, hence no management of the remote will be available.

- CLI

```
Setting bridge mode:  
set system bridge-mode  
{transparent | pipe | pipe-unique-fdb | {port-isolation <uplink-eth-  
port>} | {out-of-band <management-eth-port>}}
```

8.2 Link Aggregation

Link aggregation combines multiple parallel network connections into one logical connection in order to increase throughput and allow redundancy in case one of the links fail.

LAG can be configured on 2 of the line ports. Up to 2 LAGs can be defined on a system with 4 ports (one LAG instance on systems with 2 or 3 ports).

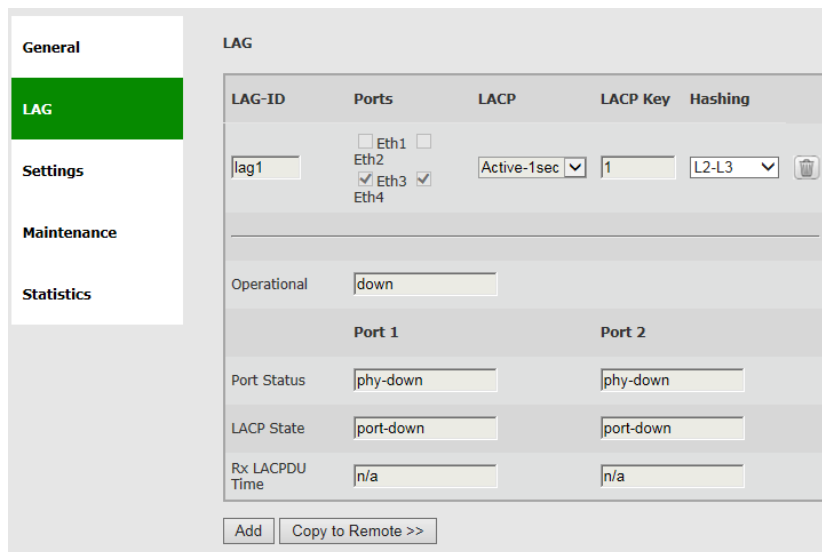


Figure 8-2 LAG Configuration and Monitoring

To configure LAG:

1. Make sure the bridge-mode=transparent
2. Select ports (exactly 2 ports)
3. LACP mode:
 - a. Disable: no LACP
 - b. Passive: ports send LACP packets only after receiving LACP packets from the partner port
 - c. Active: the ports send LACP packets at regular intervals to the partner ports (LACPDUs)
 - i. Active-1Sec: keep alive messages sent every 1 second
 - ii. Active-30Sec: keep alive messages sent every 30 seconds
 - d. LACP Key (1..128)
4. Hashing: L2, L2-L3, L2-L3-L4
5. Hashing (the algorithm for dividing the packets between the ports):
 - a. L2: based on source and destination MAC addresses (SA and DA)
 - b. L2-L3: based on SA and DA + source and destination IP address
 - c. L2-L3-L4: based on SA and DA + IP address + Port

To monitor LAG:

1. Operational – monitors the LAG status (up or down)

2. Port status – individual port’s status (actual phy status, LACP status and Rx time of the received LACP PDUs)

When LAG is created, a new interface is defined (lag1, lag2) that replaces the Eth ports:

- Vlan configuration
- Port network type
- Bridge-port
- Alarms

Link Aggregation + Out of Band management:

Allows out of band management, tagged or untagged, over selected port only (no management over the radio). Management traffic learned on the default FDB (FDB1). All other line ports are carried over the radio tagged with S-Vlan 1000 (FDB2), also LAG ports. No management over the radio so no Remote on management Web-GUI.

1. Make sure the bridge-mode=transparent
2. Configure LAG on selected ports
3. Set bridge-mode = Out-of-band with the selected management port

8.3 Bridge Architecture

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

Provider Bridge, commonly known as Q in Q, 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 (S-VLAN).

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 (C-VLAN).

The implementation of Provider Bridge is a network of up to seven virtual bridges connected in a “cross-like” fashion. 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. An internal port name uses the name of its peer component.

Bridge component types:

- S Component – an S component handles traffic tagged with S-VLANs.

A single S component (named S1) is the heart of the bridge and cannot be deleted. All packets passing through this bridge must be tagged with S-VLAN.

- C Component – a C component handles traffic tagged with C-VLANs.

On EH-1200F/FX and EH-600T systems: By default, no C components defined (“Single Component Bridge Model”). Up to 6 C components (named C1 to C6) can be defined.

On EH-1200/TL systems: By default, C components defined (“Single Component Bridge Model”). Up to 4 components (named C1 to C4) can be defined.

All packets passing through this bridge must be tagged with S-VLAN.

You can change the default bridge configuration to suit your network by removing or adding the desired bridge components.

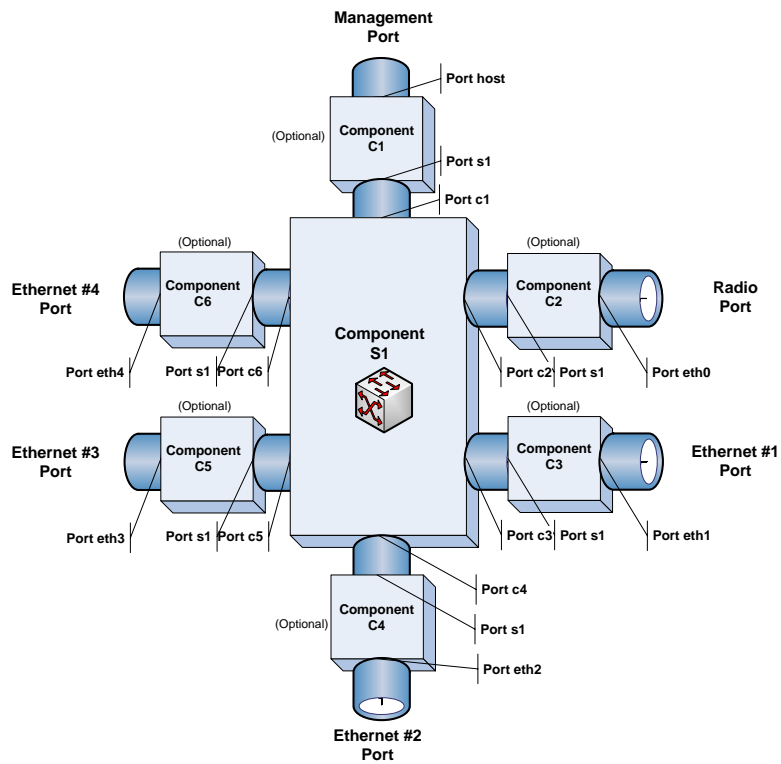


Figure 8-3 EtherHaul Bridge Architecture

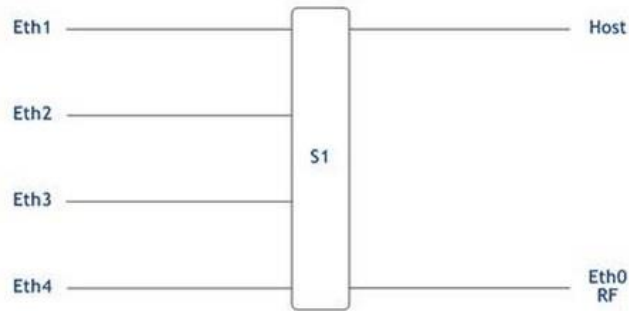


Figure 8-4 Single Component Bridge Model (Provider NNI ports)

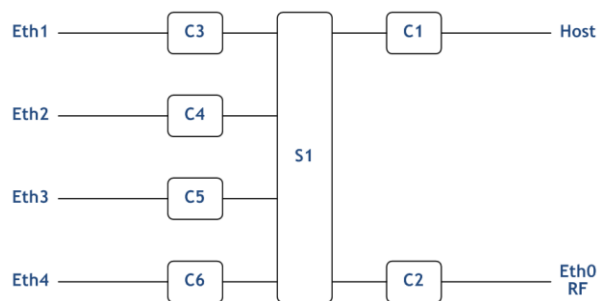


Figure 8-5 Multiple Components Bridge Model (Customer UNI ports)

8.4 Default Bridge Configuration

The default system's configuration is IEEE 802.1d Transparent Bridge. In this mode, all traffic (both tagged and untagged) is transparently forwarded between all ports and over the radio.

In addition, management VLAN can be used for out-of-band and in-band management.

The transparent bridge mode uses a simplified bridge configuration for simple and easy deployments. It is very useful in 2 cases:

- Simple LAN extension solution is required.
- First setup to enable links establishment including services flow.

For the EH-2200 product line, the default bridge mode is Pipe. This will allow easy integration to switches that implement LAG (Link Aggregation).

8.5 Services Configuration Overview

Configuring Ethernet services consists of 3 parts:

- VLAN configuration

Allow, block or add specific VLAN IDs on the system's ports.

- VLAN ID 1 – Default VLAN of the system. Used to carry untagged traffic (tagged internally using PVID 1).
- VLAN 'undef' – internal name that covers all VLAN IDs that were not configured specifically ('undefined VLANs'). For example, on the system's default configuration 'undef' is allowed on all ports, meaning that all VLAN IDs will be forwarded on all ports.

VLANs 1 and undef cannot be deleted.

- Port Network Type (EH-1200F/FX and EH-600T systems)

Each Ethernet port can be configured to one of the following Network Types to support forwarding of C-VLANs and S-VLANs:

- Provider NNI (PNP - Provider Network Port) – port that doesn't have a C component associated with it and is used for S-VLANs processing.

S-VLAN entering the provider-nni port will be processed based on the VLAN configuration of the port.

Untagged or C-VLAN entering a provider-nni port will be considered as untagged (as they have no S-VLANs) and will be tagged internally using S-VLAN PVID (default is S-VLAN ID 1).
- Customer UNI (CEP - Customer Edge Port): port that has a C component associated with it and is used for C-VLANs processing.

C-VLAN entering a customer-uni port will be processed based on the VLAN configuration on the ports.

Untagged or S-VLAN entering a customer-uni port will be considered as untagged (as they have no C-VLANs) and will be tagged internally using C-VLAN PVID (default is C-VLAN ID 1).
- Customer NNI (CNP - Customer Network Port): port that doesn't have a C component associated with it but presents a simplified model for C-VLANs processing and transparent bridge implementation.

As in provider-nni, untagged or C-VLAN entering a customer-nni port will be considered as untagged (as they have no S-VLANs) and will be tagged internally using S-VLAN PVID (default is S-VLAN ID 1).

Processing of specific C-VLANs is done by mapping them to specific S-VLAN IDs using C-VLANs Registration.

By default, all Ethernet ports are configured as Customer NNI ports. That means all untagged and C-VLANs are carried transparently to all ports.

- Bridge-Port (PVID)

A VLAN ID which will be assigned to an untagged frame or a priority-tagged frame, (the 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.

- The default PVID is 1 with priority 0:
- Untagged frame entering the S1 component (or provider-nni) will be tagged with S-VLAN ID 1.
- Untagged frame entering a C component (or customer-uni) will be tagged with C-VLAN ID 1.

8.5.1 VLAN Configuration

The system’s default configuration is transparent bridge, meaning all untagged, C-VLANs and S-VLANs can pass transparently to all ports.

The **VLAN** section displays the current processing of VLANs (C-VLANs and S-VLANs):

- Egress Ports: On what ports the VLAN ID is transmitted.
- Remove Tag: If a port is checked, the VLAN ID is removed (untagged) on egress (when it goes out of the port).

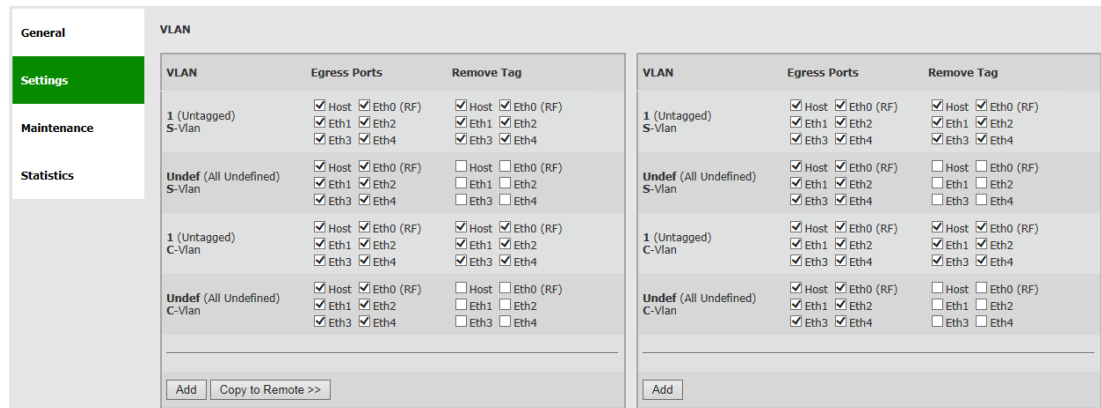


Figure 8-6 Services Page: General - VLAN

The default configuration above displays the VLAN processing:

- S-VLAN 1 (Untagged): all frames with no S-VLAN are tagged internally (using PVID) with S-VLAN ID 1 and can go out (egress) on all ports. On egress, the added S-VLAN ID 1 is removed, providing transparent connection.
- S-VLAN Undef (All Undefined): all frames with any S-VLAN (meaning, all S-VLANs) can go out (egress) on all ports. On egress, the S-VLAN they came in with is not removed, providing transparent connection.
- C-VLAN 1 (Untagged): all frames with no C-VLAN are tagged internally (using PVID) with S-VLAN ID 1 and can go out (egress) on all ports. On egress, the added S-VLAN ID 1 is removed, providing transparent connection.

- C-VLAN Undef (All Undefined): all frames with any C-VLAN (meaning, all C-VLANs) are tagged internally (using PVID) with S-VLAN ID 1 and can go out (egress) on all ports. On egress, the added S-VLAN ID 1 is removed, providing transparent connection for all C-VLANs.

To add a vlan:

Click **Add** and configure the VLAN you wish to add.

When adding a C-VLAN, the port Network Type would change to customer-uni to allow C-VLAN configuration.

When adding an S-VLAN, the port Network Type will not change and will remain provider-uni.

The screenshot shows a web-based configuration interface for VLANs. At the top, there is a title 'VLAN'. Below it is a table with three columns: 'VLAN', 'Egress Ports', and 'Remove Tag'. The table contains four rows of configurations for both S-VLAN and C-VLAN types, each with '1 (Untagged)' and 'Undef (All Undefined)' options. Below the table is a form for adding a new VLAN. The form includes a text input field with the value '12', radio buttons for 'C-Vlan' (selected) and 'S-Vlan', and checkboxes for egress ports (Host, Eth0 (RF), Eth1, Eth2, Eth3, Eth4) and 'Remove Tag' options. There are 'Add' and 'Copy to Remote >>' buttons at the bottom of the form.

VLAN	Egress Ports	Remove Tag
1 (Untagged) S-Vlan	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4
Undef (All Undefined) S-Vlan	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	<input type="checkbox"/> Host <input type="checkbox"/> Eth0 (RF) <input type="checkbox"/> Eth1 <input type="checkbox"/> Eth2 <input type="checkbox"/> Eth3 <input type="checkbox"/> Eth4
1 (Untagged) C-Vlan	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4
Undef (All Undefined) C-Vlan	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	<input type="checkbox"/> Host <input type="checkbox"/> Eth0 (RF) <input type="checkbox"/> Eth1 <input type="checkbox"/> Eth2 <input type="checkbox"/> Eth3 <input type="checkbox"/> Eth4

12 Host Eth0 (RF) Host Eth0 (RF)
 C-Vlan S-Vlan Eth1 Eth2 Eth3 Eth4 Eth1 Eth2 Eth3 Eth4

Add Copy to Remote >>

Figure 8-7 Services Page: General – VLAN (Add VLAN)

- CLI

```
Default VLAN configuration (all ports customer-nni):
set vlan s1 1 egress host,eth0,eth1,eth2,eth3,eth4 untagged host,eth0,eth1,eth2,eth3,eth4
history disable
set vlan s1 undef egress host,eth0,eth1,eth2,eth3,eth4 untagged none history disable

Default VLAN configuration (all ports customer-uni):
set vlan s1 1 egress c1,c2,c3,c4,c5,c6 untagged c1,c2,c3,c4,c5,c6 history disable
set vlan s1 undef egress c1,c2,c3,c4,c5,c6 untagged none history disable
set vlan c1 1 egress host,s1 untagged host history disable
set vlan c1 undef egress host,s1 untagged none history disable
set vlan c2 1 egress eth0,s1 untagged eth0 history disable
set vlan c2 undef egress eth0,s1 untagged none history disable
set vlan c3 1 egress eth1,s1 untagged eth1 history disable
set vlan c3 undef egress eth1,s1 untagged none history disable
```

```

set vlan c4 1 egress eth2,s1 untagged eth2 history disable
set vlan c4 undef egress eth2,s1 untagged none history disable
set vlan c5 1 egress eth3,s1 untagged eth3 history disable
set vlan c5 undef egress eth3,s1 untagged none history disable
set vlan c6 1 egress eth4,s1 untagged eth4 history disable
set vlan c6 undef egress eth4,s1 untagged none history disable

Viewing VLAN table:
show vlan

component-id  vid      fdb-id  egress                                untagged                                history
s1            1        1       host,eth0,eth1,eth2,eth3,eth4        host,eth0,eth1,eth2,eth3,eth4        disable
s1            undef    1       host,eth0,eth1,eth2,eth3,eth4        none                                  disable

Adding VLAN:
set vlan <component-id> <vid-list> [fdb-id <value>] [egress <value>]
[untagged <value>] [history <value>]
    <component-id>          : c1 | c2 | c3 | c4 | c5 | c6 | s1
    <vid-list>              : undef | 1..4094
fdbid is used for s-vlans only
    
```

8.5.2 Port Network Type Configuration

Port Network Type

Host	<input type="text" value="Customer-NNI"/>	Eth0 (RF)	<input type="text" value="Customer-NNI"/>
Eth1	<input type="text" value="Customer-NNI"/>	Eth2	<input type="text" value="Customer-NNI"/>
Eth3	<input type="text" value="Provider-NNI"/>	Eth4	<input type="text" value="Customer-UNI"/>

Figure 8-8 Services Page: General – Port Network Type

The default port Network Type is Customer-NNI (for EH-1200F/FX and EH-600T systems).

You can change the Network Type manually or all the system to configure it automatically using the VLAN configuration.

In addition, the system has built-in scripts to change the Network Type between Customer NNI and Customer UNI. Refer to the *Scripts* section under the *System* chapter of this manual for details.

- CLI

```

Setting port network type:
set eth <eth> [network-type <value>]
    <eth>          : host | eth0 | eth1 | eth2 | eth3 | eth4
    <network-type value> : provider-nni | customer-uni | customer-nni
    
```

8.5.3 Bridge Port (PVID) Configuration

Port	C-Vlan		S-Vlan	
	PVID	P-Bit	PVID	P-Bit
Host	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
Eth0 (RF)	<input type="text" value="1"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
Eth1	<input type="text" value="12"/>	<input type="text" value="0"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
Eth2	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
Eth3	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="0"/>
Eth4	<input type="text"/>	<input type="text"/>	<input type="text" value="1"/>	<input type="text" value="0"/>

Figure 8-9 Services Page: General – Bridge Port

PVID is a VLAN ID which will be assigned to an untagged frame or a priority-tagged frame, (the 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.

- Untagged frame entering the S1 component (or provider-nni) will be tagged with S-VLAN ID 1 with P-Bit (prio) 0.
- Untagged frame entering a C component (or customer-uni) will be tagged with C-VLAN ID 1 with P-Bit (prio) 0.
- Configuring C-VLAN PVID is available only on ports with Network Type of customer-uni.

- CLI

```
Setting PVID:
set bridge-port <component-id-list> <bridge-port> [pvid <value>] [prio
<value>] [admit <value>] [filter <value>]
  <component-id-list>      : list: | c1 | c2 | c3 | c4 | c5 | c6 | s1
  <bridge-port>           : host | eth0 | eth1 | eth2 | eth3 | eth4 | s1
| c1 | c2 | c3 | c4 | c5 | c6
```

Admit: This attribute controls what kinds of frames are allowed into the bridge. If it is set to `untagged` then only untagged or priority tagged frames may enter. If it is set to `tagged` then only tagged frames (i.e. those with VID different from zero) may enter. If it is 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 through 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`.

8.5.4 Configuration Examples

8.5.4.1 Single Cable Connection

When single Ethernet cable is used, both customer traffic and management (either tagged or untagged) are running over the cable.

As a single port is connected, no meaning for traffic separation applies. For such a case, the default transparent configuration can be used (no configuration changes in the VLAN table).

8.5.4.2 Transparent Pipe for Customer Traffic + Separate Management

In case of a requirement to provide completely transparent (and isolated) “Pipe” for customer traffic, two Ethernet connections are used – one for customer traffic and second for management (either tagged or untagged).

Example: management on Eth1, customer traffic on Eth2. You are required to provide transparent isolated connection between Eth2 ports across the link.

To provide this traffic separation, all traffic coming from Eth2 will be tagged with S-VLAN (for example, S-VLAN 2). This S-VLAN will be allowed on Eth2 and Eth0 (RF).

Configuration steps using the GUI:

1. Add S-VLAN 2, Egress to ports Eth2 and Eth0, Remove tag when going out of Eth2.
2. Use PVID to tag the traffic port: set S-VLAN PVID 2 on Eth2.
3. Change the Network Port Type of Eth0 to Provider-NNI to allow S-VLAN egress on this port.

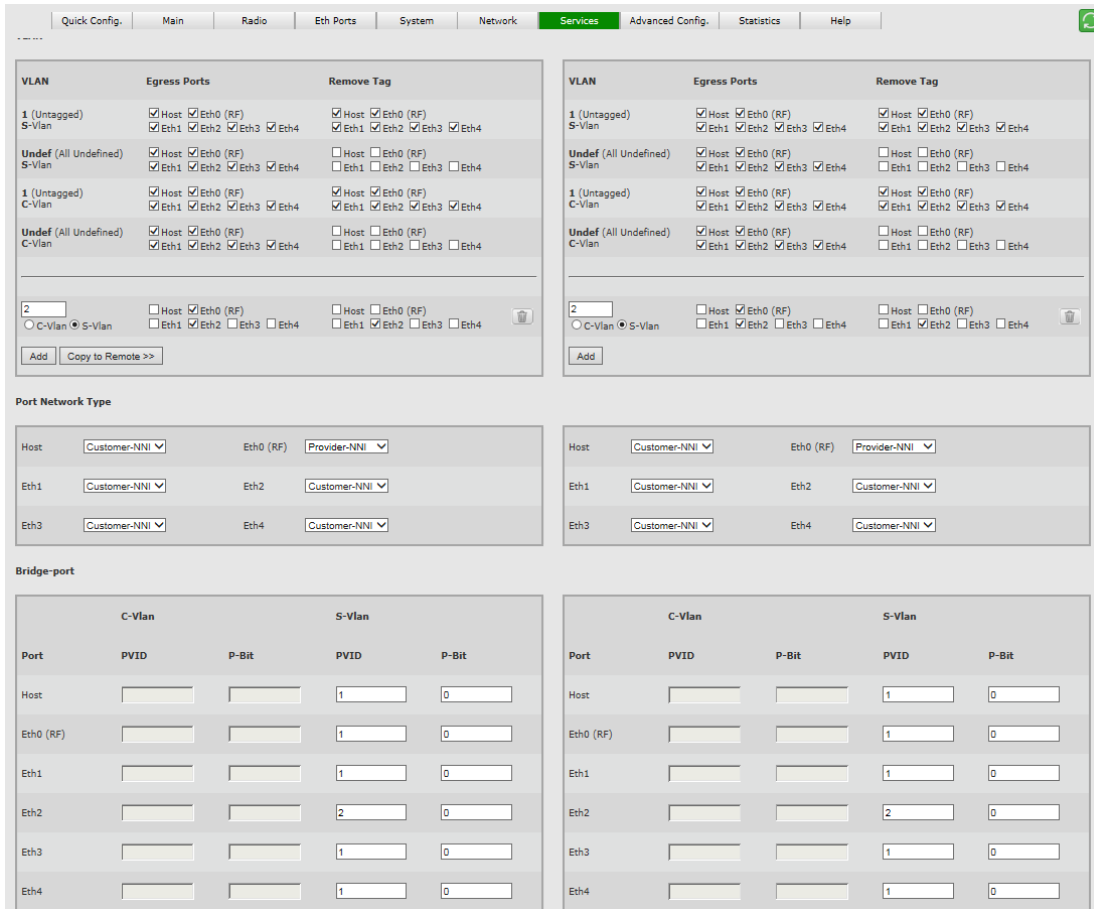


Figure 8-10 Services Page: Transparent Pipe

- CLI

```
VLAN Configuration:
set vlan s1 1 egress host,eth1,eth2,eth4,eth0,eth3 untagged
host,eth1,eth2,eth4,eth0,eth3
set vlan s1 2 egress eth2,eth0 untagged eth2
set vlan s1 undef egress host,eth1,eth2,eth4,eth0,eth3 untagged none
```

```
Bridge-Port (PVID) Configuration:
set bridge-port s1 eth2 pvid 2
```

```
Port Network Type Configuration:
set eth eth0 network-type provider-nni
```

8.6 Maintenance

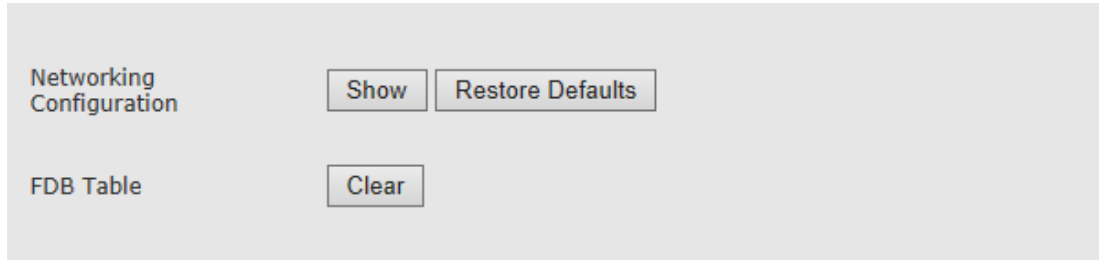


Figure 8-11 Services Page: Maintenance

In the Networking Configuration click **Show** to view (pop-up screen) the full networking services configuration in the form of CLI commands.

Click **Restore** to restore factory default networking services settings. The system will run the existing `restore_networking_config` script (from the list of scripts available) that will restore factory default networking services settings.

In the FDB Table click **Clear** to clear all MAC entries in the Forwarding Database table.

8.7 Statistics

VLAN statistics can be monitored using the advanced statistics counters.

Click **View Statistics** to review the local and remote VLAN statistics. Clicking **Show Statistics** will open the **Statistics** page where all system's statistics can be reviewed.

Refer to the *Statistics* chapter of this manual for detailed description of the system's statistics.

8.8 Advanced Ethernet Networking Configurations

Advanced QoS Configuration can be configured in CLI only and includes:

- C-VLAN Registration
- PEP Virtual Ports
- S-VID Translation
- Forwarding Database (FDB)
- Default C-VLAN EtherType
- Bridge VLAN EtherType
- MAC Learning

Note: When loading the **Services** page, the current system's networking services configuration will be evaluated. If advanced configuration that is not supported by the GUI is present, the services configuration will not be displayed and the following



message will be displayed:

“The Networking Services configuration cannot be displayed. Refer to the CLI for configuration or restore default networking services configuration.”

8.8.1 C-VLAN Registration

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 to eth4.
- The `set cvlan-reg` command fails if the port specified belongs to an 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}
```

8.8.2 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}
```

8.8.3 S-VID Translation

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 rebooted.

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 an 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]]]
```

8.8.4 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.

The system maintains 64 permanent instances of the FDB object that can be created on S1 (separate instances based on S-VLANs only).

By default, FDB #1 is used for all incoming packets.

The default aging time for all FDBs is 172800 seconds (48 hours).

Creating and modifying FDB aging:

```
set fdb <component-id> <fdb-id> [aging <value>]
    <component-id>          : s1
```

```

<fdb-id>          : set of 1..64
<aging value>    : 5..1000000

```

```

Creating and modifying entries in the FDB Address table:
set fdb-table <component-id> <fdb-id-list> <mac-addr> bridge-port
<value> [quota <value>]
  <component-id>      : c1 | c2 | c3 | c4 | c5 | c6 | s1
  <fdb-id-list>      : list: | integer 1..64
  <mac-addr>         : mac

```

```

Clearing FDB table:
clear fdb-table all all all

```

8.8.5 Default C-VLAN EtherType

By default the C-VLAN EtherType is 0x8100.

That means that unless specifically configured for a specific bridge, the C-VLAN EtherType will be set to 0x8100.

You can change the default EtherType using the CLI.

```

set bridge-common def-cvlan-etype
hex number 0x700..0xFFFF except 0x800, 0x806, 0x8809, 0x88CC, 0x8902

```

8.8.6 Bridge VLAN EtherType

By default the S-VLAN EtherType is 0x88a8 and the C-VLAN EtherType is 0x8100 (as the Default C-VLAN EtherType).

You can change the default EtherType using the CLI.

```

set bridge-common def-cvlan-etype
hex number 0x700..0xFFFF except 0x800, 0x806, 0x8809, 0x88CC, 0x8902
set bridge <component-id> [vlan-ethertype <value>]
  <component-id>      : c1 | c2 | c3 | c4 | c5 | c6 | s1
  <vlan-ethertype value> : hex number 0x700..0xFFFF except 0x800, 0x806,
0x8809, 0x88CC, 0x8902, 0x86DD

```

8.8.7 MAC Learning

By default the MAC Learning is enabled.

You can disable MAC Learning using the CLI. If disabled, all received frames will not be learned and will be broadcasted to all ports.

```

set bridge-common mac-learning
disable | enable

```

9 Quality of Service

The EtherHaul incorporates an advanced Quality of Service engine which complements the hitless adaptive bandwidth, coding and modulation mechanism.

Quality of Service (QoS) mechanism enables service providers to offer different classes of service for different types of traffic or customers and is 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.

The EtherHaul QoS engine classifies the incoming packets onto streams using any combination of VID, PCP, DSCP (or alternatively MPLS EXP bit) fields. Each stream may be assigned a bandwidth profile with CIR (committed rate), CBS (committed burst size), EIR (excess rate), EBS (excess burst size) and color-mode.

The implemented mechanism supports 3 colors and 2 rates. The frames that fit into CIR/CBS profile marked drop ineligible and colored “green”. The traffic which is within excess profile but exceeds committed profile is marked drop eligible (“yellow”). Upon congestion at egress interface the yellow packets are dropped first. The rest, which are out of profile, are colored “red” and discarded. The “red” frames are dropped using a head drop algorithm and “green” frames take precedence of “yellow”.

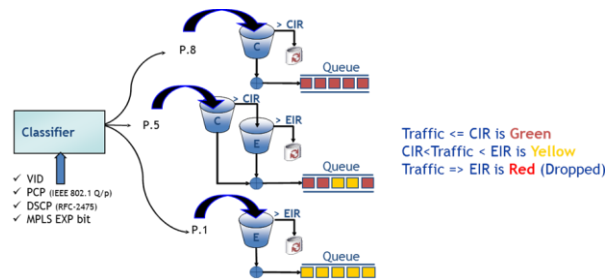


Figure 9-1 Classification and Policing

These packets are then mapped to 1 of the 8 priority queues (per interface). These queues are accessed by the scheduling mechanism.

The priority queues of the EtherHaul are accessed using the following scheduling mechanisms:

- Strict Priority: lower priority packets are served only if all higher priority queues are empty.
- Weighted Fair Queuing (WFQ): data packet scheduling technique maintaining fairness by applying weights to the queues. Each queue is serviced in the order of its weighted proportion to the available resources.
- Shaper: 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.

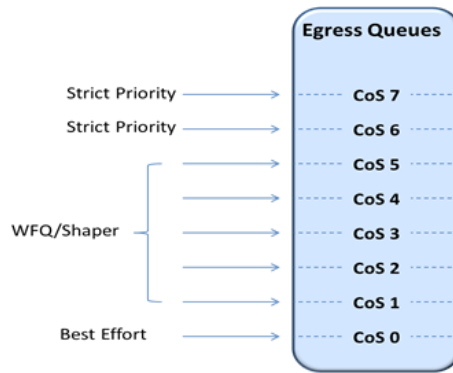


Figure 9-2 Egress Queues Scheduling

QoS functions:

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

9.1 QoS Configuration Using the Web-based Management GUI

The Web-Based Management Graphical User Interface (GUI) supports the commonly-used classification options.

Advanced QoS Configuration can be configured in CLI only and includes:

- Advanced classification
- Metering (CIR/EIR/CBS/EBS) and Coloring (Ingress QoS color Marking)

For EH-1200F/FX and EH-600T systems, additionally supported:

- PCP Rewrite
- PFC – Priority-based flow control
- Queue Management
- WRED

Note:



When loading the **Advanced Config** page (that includes the **Quality of Service** section), the current system's QoS configuration will be evaluated. If advanced configuration that is not supported by the GUI is present, the QoS configuration will not be displayed and the following message will be displayed:

"The QoS configuration cannot be displayed. Refer to the CLI for configuration or restore default QoS configuration."

9.2 Default QoS Configuration

The default QoS configuration is classification of traffic coming from all ports based on Priority Code Point (PCP, or pBit).

Any traffic coming with pBit 0 will be classified to queue number 0 (CoS 0, lowest priority), traffic coming with pBit 1 will be classified to queue number 1 (CoS 1) and so on till CoS 7 (highest priority).

9.3 QoS Classification

The EtherHaul 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), packet type (unicast, non-unicast or all) 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 the marker.

9.3.1 Port Priority

Port priority means that all traffic of the selected ports will be assigned with highest priority (CoS 7), regardless of other classification rules.

When configuring port priority for specific ports, classifier rule is created with the highest precedence (precedence 1).

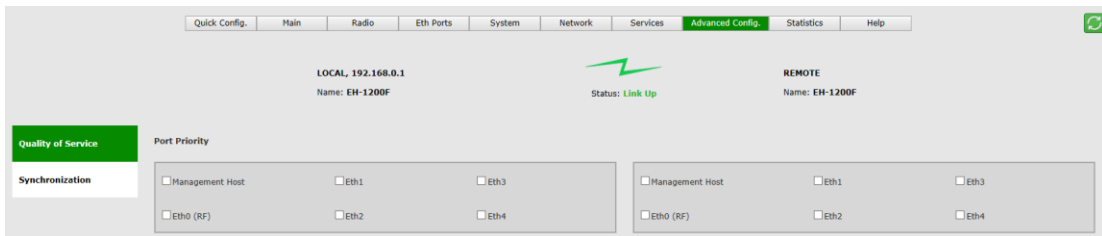


Figure 9-3 Advanced Config Page: Quality of Service – Port Priority

9.3.2 Classification Criteria

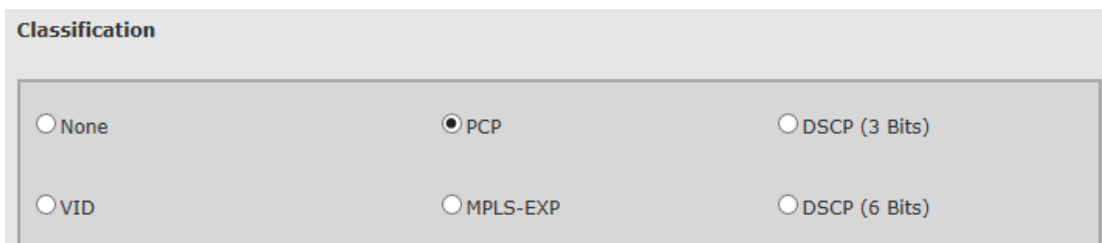


Figure 9-4 Advanced Config Page: Quality of Service – Classification Criteria

Classification Criteria options have lower priority than configured **Port Priority**.

Classification based on one of the following options:

- None – no classification, hence no classifiers (all previously configured classifiers will be deleted besides the Port Priority).
- VID – classification based on the incoming VLAN ID.
- PCP – classification based on the incoming Priority Code Point (PCP, or pBit) of the incoming frame.
- MPLS-EXP – classification based on the incoming MPLS Experimental bit.
- DSCP (3 Bits) – classification based on the incoming Differentiated Services Code Point 3 MSB (most-significant-bits). If selected, the system will accept values 0÷7 (3 bits).
- DSCP (6 Bits) – classification based on the incoming Differentiated Services Code Point full 6 bits. If selected, the system will accept values 0÷63 (6 bits).

9.3.3 Classifiers

Classifiers				
ID #	Classification Value	Ports	CoS(Queue#)	
1	0	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	0	
2	1	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	1	
3	2	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	2	
4	3	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	3	
5	4	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	4	
6	5	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	5	
7	6	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	6	
8	7	<input checked="" type="checkbox"/> Host <input checked="" type="checkbox"/> Eth0 (RF) <input checked="" type="checkbox"/> Eth1 <input checked="" type="checkbox"/> Eth2 <input checked="" type="checkbox"/> Eth3 <input checked="" type="checkbox"/> Eth4	7	
<input type="button" value="Add"/>				

Figure 9-5 Advanced Config Page: Quality of Service – Classifiers

Classification rules are based on the selected classification criteria.

If Port Priority was configured, it will be displayed as Read Only entry.

9.4 Scheduling

Scheduler Mode options:

- **Strict Priority** – Lower priority packets are served only if all higher priority queues are empty. This is the default scheduler mode.
- **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.

Weights (for WFQ configuration) or CIR values (for Shaper configuration) can be configured for queues #1 to #5 (CoS 1 to 5).

9.4.1 Scheduling Mode: Strict Priority

The screenshot shows a configuration page titled "Scheduler Mode". Below the title is a dropdown menu with "Strict-Priority" selected and a downward arrow.

Figure 9-6 Advanced Config Page: Quality of Service – Scheduler Mode Strict Priority

Lower priority packets are served only if all higher priority queues are empty.

9.4.2 Scheduling Mode: Weighted Fair Queue (WFQ)

The screenshot shows a configuration page titled "Scheduler Mode" with "WFQ" selected in the dropdown menu. Below the dropdown is a table with five rows, each representing a queue configuration. The table has four columns: "Egress-qos", "CoS", "Weight", and "CIR".

Egress-qos	CoS	Weight	CIR
Eth0 (RF)	1	1	0
Eth0 (RF)	2	2	0
Eth0 (RF)	3	4	0
Eth0 (RF)	4	6	0
Eth0 (RF)	5	8	0

Figure 9-7 Advanced Config Page: Quality of Service – Scheduler Mode 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:

$$R * W_i / (W_1 + W_2 + \dots + W_n)$$

WFQ explicitly considers data queue, and by regulating the weights dynamically, you can utilize WFQ 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 on a best effort basis.

9.4.3 Scheduling Mode: Priority-Shaper

Scheduler Mode

Priority-Shaper ▾

Egress-qos	CoS	Weight	CIR
Eth0 (RF)	1	<input type="text" value="1"/>	<input type="text" value="50"/>
Eth0 (RF)	2	<input type="text" value="1"/>	<input type="text" value="100"/>
Eth0 (RF)	3	<input type="text" value="1"/>	<input type="text" value="100"/>
Eth0 (RF)	4	<input type="text" value="1"/>	<input type="text" value="150"/>
Eth0 (RF)	5	<input type="text" value="1"/>	<input type="text" value="100"/>

Figure 9-8 Advanced Config Page: Quality of Service – Scheduler Mode Priority-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.

Shaper 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 on a best effort basis.

You can set the Committed Information Rate (CIR) to a value between 1-1000 Mbps (the total of all CIR cannot exceed 1000 Mbps). The CIR value limits the maximum rate of the particular queue.

In Priority-Shaper scheduling, packets in the lower priority queues are served only if all higher priority queues are empty.

9.4.4 Scheduling Mode: WFQ-Shaper

Egress-qos	CoS	Weight	CIR
Eth0 (RF)	1	1	50
Eth0 (RF)	2	2	100
Eth0 (RF)	3	4	100
Eth0 (RF)	4	6	150
Eth0 (RF)	5	8	100

Figure 9-9 Advanced Config Page: Quality of Service – Scheduler Mode WFQ-Shaper

Combination of the Shaper and WFQ scheduling. Queues are served based on their weights and the CIR value limits the maximum rate of the particular queue.

9.5 QoS Configuration Commands

In the QoS Configuration click **Show** to view (pop-up screen) the full QoS configuration in the form of CLI commands.

Click **Restore** to restore factory default QoS settings. The system will run the existing restore_qos_config script (from the list of scripts available) that will restore factory default QoS settings.

9.6 QoS Statistics

Queues ingress (in-queue) and egress (out-queue) statistics can be monitored using the advanced statistics counters.

Click **View Statistics** to review the local and remote queue statistics. Clicking **Show Statistics** will open the **Statistics** page where all system's statistics can be reviewed.

Refer to the *Statistics* chapter of this manual for detailed description of the system's statistics.

9.7 QoS CLI Commands – Classification and Scheduling

- Default classification:

```
set classifier-cos 1 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 0 ip-cos dont-care packet-type all cos 0
set classifier-cos 2 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 1 ip-cos dont-care packet-type all cos 1
set classifier-cos 3 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 2 ip-cos dont-care packet-type all cos 2
set classifier-cos 4 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 3 ip-cos dont-care packet-type all cos 3
set classifier-cos 5 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 4 ip-cos dont-care packet-type all cos 4
set classifier-cos 6 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 5 ip-cos dont-care packet-type all cos 5
set classifier-cos 7 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 6 ip-cos dont-care packet-type all cos 6
set classifier-cos 8 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 7 ip-cos dont-care packet-type all cos 7
```

- Configuring classifier:

```
set classifier-cos <classifier-id: 1..248> [interface <host|eth0|
eth1|eth2|eth3|eth4>] [precedence <1..8>] [vid < list 0..4094>] [pcp <
list 0..7>] [ip-cos <{{dscp-cos | mpls-exp} <list of 0..7>}|dont-care>]
[packet-type < unicast | non-unicast | all>] [cos <0..7>]
```

- Configuring scheduling:

```
set scheduler mode <strict-priority | wfq | priority-shaper | wfq-shaper>

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

9.8 Advanced QoS Configuration

The Web-Based Management GUI supports the commonly used configuration options.

Advanced QoS Configuration can be configured in CLI only and includes:

- Advanced classification
- Metering (CIR/EIR/CBS/EBS) and Coloring (Ingress QoS color Marking)
- PCP Rewrite
- PFC – Priority-based flow control
- Queue Management
- WRED

9.8.1 Advanced Classification

Classification Criteria combinations:

The EtherHaul supports classification based on combination of the classification criteria options, such as VID and PCP (or any other combination).

Such combinations are supported on CLI only.

Example:

```
set classifier-cos 5 interface eth1,eth3,eth4 precedence 1 vid 4
pcp 3 ip-cos dont-care packet-type all cos 4
```

Classification based on DSCP:

The EtherHaul supports 2 modes of classification based on DSCP: 3 bits (MSB) or 6 bits (full DSCP). When selecting DSCP (3 Bits), you can combine it with PCP classification (in addition to VID and MPLS-EXP). When selecting DSCP (6 Bits), you do not have the option to combine it with PCP classification (in addition to VID and MPLS-EXP).

The availability of classification based on DSCP (3 Bits) or DSCP (6 Bits) is determined per port in the Eth port configuration in the CLI.

Example:

```
set eth eth1 classifier-mode
dscp | pcp-dscp
```

Classifiers Configuration:

Use the following command to configure classifiers (classifier-cos):

```
set classifier-cos <classifier-id: 1..248> [interface <host|eth0|
```

```
eth1|eth2|eth3|eth4>] [precedence <1..8>] [vid < list 0..4094>] [pcp <
list 0..7>] [ip-cos <{{dscp-cos | mpls-exp} <list of 0..7>}|dont-care>]
[packet-type < unicast | non-unicast | all] [cos <0..7>]
```

IP-COS: Priority based on IP header value – DSCP (differentiated services), MPLS-EXP (MPLS experimental bit), or Don't-Care (IP header values ignored).

Precedence: Priority between classifiers. Multiple and overlapping classifiers rules may be configured. In such case, the precedence value will determine the priority between the overlapping classifier rules. Precedence 1 is the lowest priority.

Default Classifiers Configuration:

```
set classifier-cos 1 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 0 ip-cos dont-care packet-type all cos 0

set classifier-cos 2 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 1 ip-cos dont-care packet-type all cos 1

set classifier-cos 3 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 2 ip-cos dont-care packet-type all cos 2

set classifier-cos 4 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 3 ip-cos dont-care packet-type all cos 3

set classifier-cos 5 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 4 ip-cos dont-care packet-type all cos 4

set classifier-cos 6 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 5 ip-cos dont-care packet-type all cos 5

set classifier-cos 7 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 6 ip-cos dont-care packet-type all cos 6

set classifier-cos 8 interface host,eth0,eth1,eth2,eth3,eth4 precedence 1
vid 0-4094 pcp 7 ip-cos dont-care packet-type all cos 7
```

9.8.2 Metering and Coloring

Classifier-evc configuration:

Frames on the ingress are classified onto CoS or EVC (optional)

If no EVC defined, the classifier-cos determines queue number on egress the frame is forwarded to (CoS)

If EVC is defined, the EVC and CoS represents the entry in the marking table (for metering and coloring)

```

classifier-cos configuring:
set classifier-cos <classifier-id {1..248}> [interface
<host|eth0|eth1|eth2|eth3|eth4>] [precedence <1..8>] [vid <0..4094>] [pcp
<0..7>] [ip-cos <{dscp-cos | mpls-exp} <0..7> | dont-care>] [packet-type
<unicast|non-unicast|all>] [cos <0..7>]

classifier-evc configuring:
set classifier-evc <classifier-id {1..248}> [interface
<host|eth0|eth1|eth2|eth3|eth4>] [precedence <1..8>] [vid <0..4094>] [pcp
<0..7>] [ip-cos <{dscp-cos | mpls-exp} <0..7> | dont-care>] [packet-type
<unicast|non-unicast|all>] [evc<0..31>]
    
```

Meter configuration:

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 a classifier, the packet is either dropped or internally colored: Green or Yellow.

BW profiles per EVC:

- CIR – Committed Information Rate.
- EIR – Excess Information Rate.
- CBS, EBS - size of burst window for allowed CIR / EIR rates.

Coloring:

- Green – traffic within CIR (and CBS) is colored green.
- Yellow – traffic exceeding CIR but within EIR (and EBS) is colored yellow.
- Traffic exceeding CIR+EIR rate is unconditionally discarded.

In case of congestion, when green packet arrives, the oldest yellow packet is discarded (head-drop).

```

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

binding meter and classifier:
set ingress-qos <evc-classifier-id {1..248}> <cos-id {0..7}> [meter
<0..248>] [marking <enable | disable>]
    
```

Color-Aware mode for S-VLANs

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

The DEI (Drop Eligible Indicator) bit in S-Tag is used for Color encoding:

- DEI = '0' → Green
- DEI = '1' → Yellow

For incoming colored S-VLAN packets, the drop precedence is determined by the DEI bit (and not according to the metering result).

Colored packets are transmitted with the color (DEI bit) they came in with.

9.8.3 PCP Rewrite

PCP Rewriting capability allows you to set the outer PCP value of an outgoing frame as a function of COS.

Note:



PCP Rewrite configuration supported in the CLI only.

The PC-Write-Profile table is a set of profiles where each profile is a single mapping between eight COS values to eight PCP values - so it can be represented by eight values in the range 0-7. Each profile is identified by a profile ID.

In addition, the rewrite-profile attribute is available for each eth. The attribute value can be set to NULL or a valid profile ID. A non-Null value causes a frame's PCP to be written accordingly prior to the frame being sent on an external port. When no value is set the default value is "no profiles defined". The maximum number of profiles is 128.

```

Rewrite PCP on frames going to eth1 with the cos value
set pcp-write-profile 1 0 1 2 3 4 5 6 7 // profile that maps each
cos to the pcp of same numerical value
set pcp-write-profile 1 XX 1 2 3 4 5 6 7 8
set eth eth1 pcp-write-profile-id 1 // let port 1 operate
with PCP rewrite.

To cancel PCP rewrite
set eth eth1 pcp-write-profile-id none
    
```

9.8.4 PFC - Priority-based flow control

Priority-based flow control (IEEE standard 802.1Qbb) prevents frame loss from congestion by pausing traffic based on the congested priority without affecting the traffic of uncongested priorities.

Instead of pausing all traffic on a link as in IEEE 802.3x Ethernet PAUSE (flow control), PFC allows you selectively pause traffic according to its class.

Standard Ethernet does not guarantee that a packet injected into the network will arrive at its intended destination. Reliability is provided by upper-layer protocols. A problem arises when transmitters send packets faster than receivers can accept them. When receivers run out of available buffer space to hold incoming flows, they silently drop additional incoming packets.

Applications that require reliability in Layer 2 must have flow control that includes feedback from a receiver to a sender regarding buffer availability. Using IEEE 802.3x Ethernet PAUSE control frames, a receiver can generate a MAC control frame and send a PAUSE request to a sender when a specified threshold of receiver buffer has been filled to prevent buffer overflow. Upon receiving a PAUSE request, the sender stops transmission of any new packets until the receiver notifies the sender that it has sufficient buffer space to accept them again. The disadvantage of using Ethernet PAUSE is that it operates on the entire link, which might be carrying multiple traffic flows. Some traffic flows do not need flow control in Layer 2, because they are carrying applications that rely on upper-layer protocols for reliability. PFC enables you to configure Layer 2 flow control selectively for the traffic that requires it.

Note:



PFC configuration supported in the CLI only.

Implementation concept:

- This feature should work only when the ODU is set as “pipe” i.e. as transparent bridge.
- PFC can be set towards one UNI port only (one of the 4 Eth ports), for traffic set between one of ETH ports and the radio port (Eth0/RF).
- Priorities should be set for the PFC for the RF port only (Eth0). It can be done for all 8 queues but the mandatory requirement is for the first 4 queues.
- Once the BW in the radio drops down, as a result of modulation change or manual change, if the out queues of ETH0/RF cross a maximum threshold a pause frame should be send to the UNI port.
- Min and max thresholds defined in Mb.

```

set eth <eth> [pfc-mode <value>]
  <eth>          : host | eth0 | eth1 | eth2 | eth3 | eth4
  <pfc-mode value> : rf | disable

set pfc <pfc-id-list> [min-threshold <0..100>] [max-threshold
<0..100>]
  <pfc-id-list>      : list: | integer 1..32

set egress-qos eth0 <cos-id-list> pfc <pfc-id-list>

```

9.8.5 Queue Management

The EtherHaul allows controlling the drop mode by setting it to one of the following options:

- Simple – set queue length in microseconds
- Length – set queue length us Kbytes
- WRED

The default queue mode and length is Simple with queue length of 2000 microseconds.

```

set egress-qos <eth> <cos-id-list> [drop-mode <value>]
  <eth>          : host | eth0 | eth1 | eth2 | eth3 | eth4
  <cos-id-list>  : list: | integer 0..7
  <drop-mode {simple <queue-length-microsec 1.. 1000000}> |
  {length <queue-length-in-kbytes 10..10000> } |{wred <wred-id>}

```

9.8.6 Weighted Random Early Detection (WRED)

Queues have several different queue thresholds, each queue threshold is associated to a particular traffic class.

Weighted random early detection (WRED) is a queue management algorithm with congestion avoidance capabilities. It is an extension of Random Early Detection (RED) in which a single queue may have several different queue thresholds. Each queue threshold is associated to a particular traffic class; a queue may have lower thresholds for lower priority packet.

A queue buildup will cause the lower priority packets to be dropped, hence protecting the higher priority packets in the same queue. In this way quality of service prioritization is made possible for important packets from a pool of packets using the same buffer a standard traffic will be dropped instead of higher prioritized traffic.

WRED is very useful in improving TCP performance.



Note: WRED configuration supported in the CLI only.

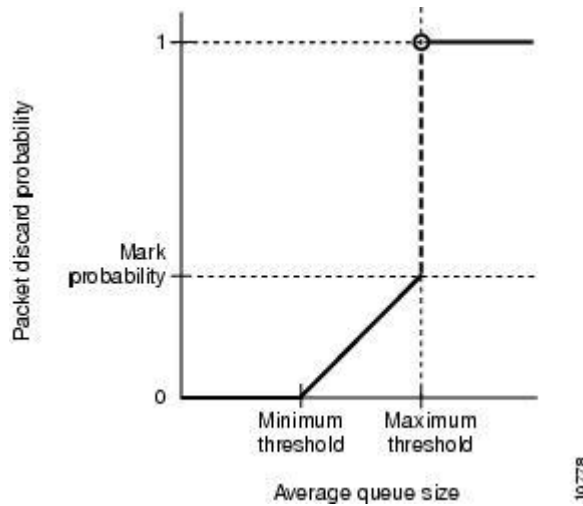


Figure 9-10 TCP Performance

9.8.6.1 WRED Functionality

When a packet arrives, WRED handles it according to the following process:

- 1) The average queue size is calculated using the following equation:

$$\text{Average} = (\text{old_average} * (1 - 1/2^n)) + (\text{current_queue_size} * 1/2^n).$$
- 2) The packet is filtered according to its size.
 - If the average queue size is below the minimum queue threshold, the packet is queued normally.
 - If the average queue size is greater than the maximum threshold, the packet is automatically dropped.
 - If the average queue size is between the minimum and maximum queue threshold, the packet is either dropped or queued depending on the packet's drop probability.

9.8.6.2 WRED Parameters

- **Minimum and Maximum Thresholds** - When the system uses color aware configuration, it requires the use of thresholds per color (green and yellow). When the system does not use color aware configuration (blind mode), it uses one set (the Green set) of thresholds.
 The difference between the maximum threshold and the minimum threshold should be large enough to avoid global synchronization of TCP hosts (which can

occur as multiple TCP hosts reduce their transmission rates). If the difference is too small, many packets may be dropped at the same time, resulting in global synchronization.

- “n” the average factor** - “n” is the user-configurable exponential weight factor. The previous average is more important for the higher n values. Peaks and Lows in queue length are smoothed by a high value. Lower n values allow the value of the average queue size to remain similar to the value of the close to the current queue size.

If the value of n is too high, WRED does not react to congestion. Packets are sent or dropped as if WRED is not enabled.
- Packet Drop Probability** - The mark probability denominator is the fraction of packets dropped when the average queue size reaches the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue reaches the maximum threshold.

9.8.6.3 TCP Performance Example

The following images display how the system behaves with and without WRED:

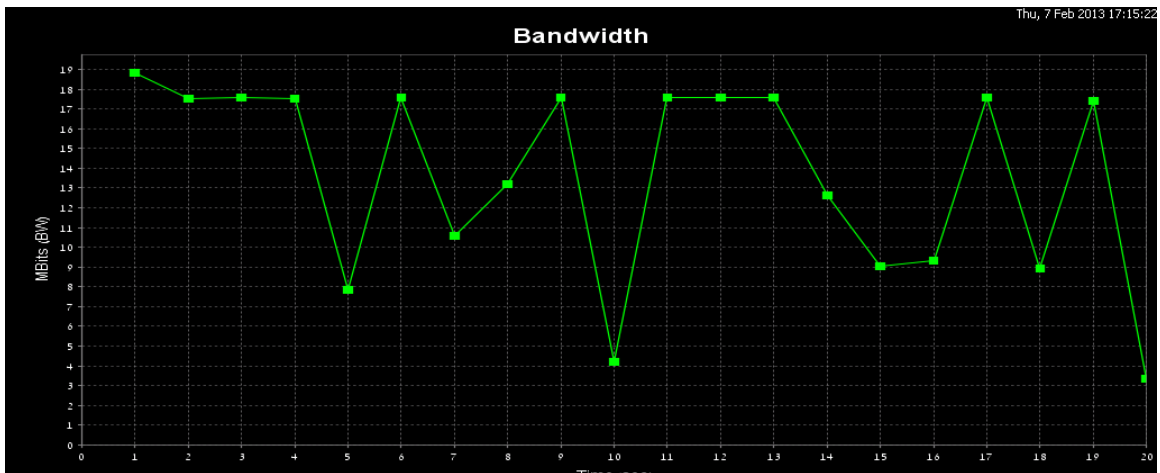


Figure 9-11 TCP Performance without WRED

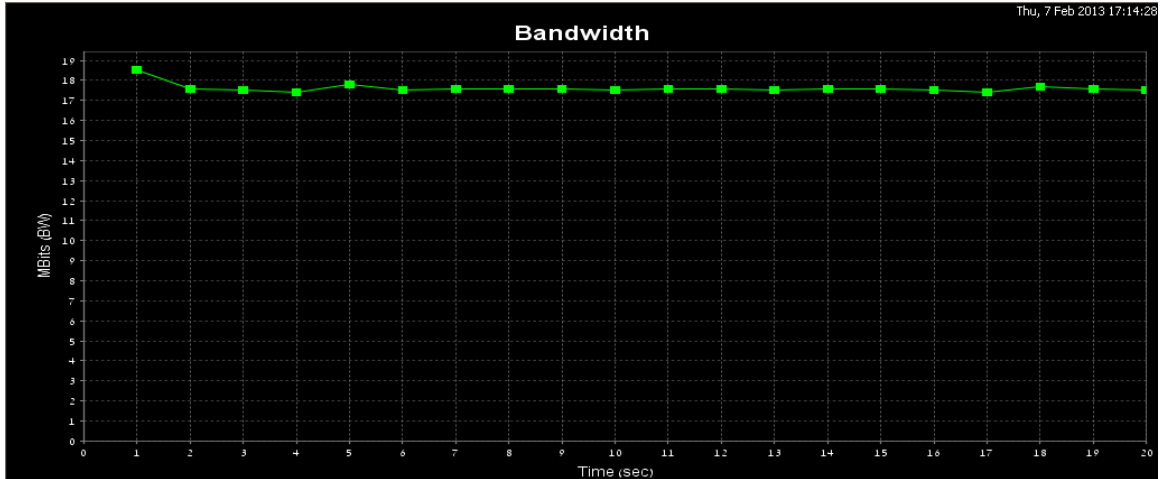


Figure 9-12 TCP Performance with WRED

9.8.6.4 WRED Configuration

```
wred:
set wred <wred-id-list> [n-factor <1..32>] [min-threshold
<10000..1000000>] [max-threshold <10000..1000000>] [drop-probab
<0..1000>] [min-threshold-yellow <10000..1000000>] [max-threshold-
yellow <10000..1000000>] [drop-probab-yellow <0..1000>]
    <wred-id-list>          : list: | integer 1..32

egress-qos:
egress-qos eth0 <queue> wred <wred-index> wred-green <wred-index>
wred-yellow <wred-index> wred-n <1-16>
```

10 Synchronization

This chapter describes the supported Ethernet synchronization standards by the EtherHaul.

- Synchronous Ethernet (SyncE) as per G.8261, G.8262 and G.8264
- IEEE 1588 (timing over packet) Transparent Clock (TC) as per IEEE 1588v.2.
IEEE 1588 is supported for EH-1200F/FX and EH-600T systems.

10.1 Synchronous Ethernet (SyncE)

The EtherHaul 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.

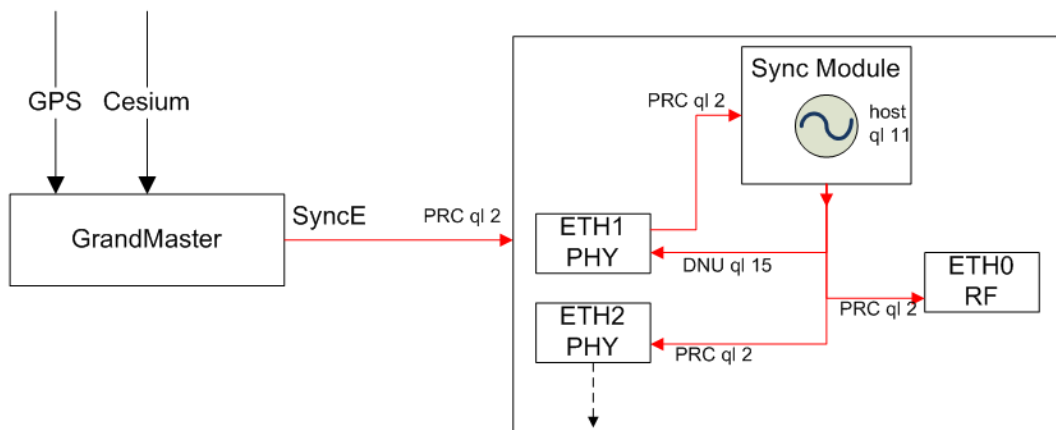


Figure 10-1 SyncE Functional Diagram

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 products 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 and hierarchy:

Table: Quality Levels (ql) and 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

SyncE is a licensed feature that requires license for operation. Before configuring it, verify that license is available and enable the **syncce** license.

10.1.1 SyncE Configuration

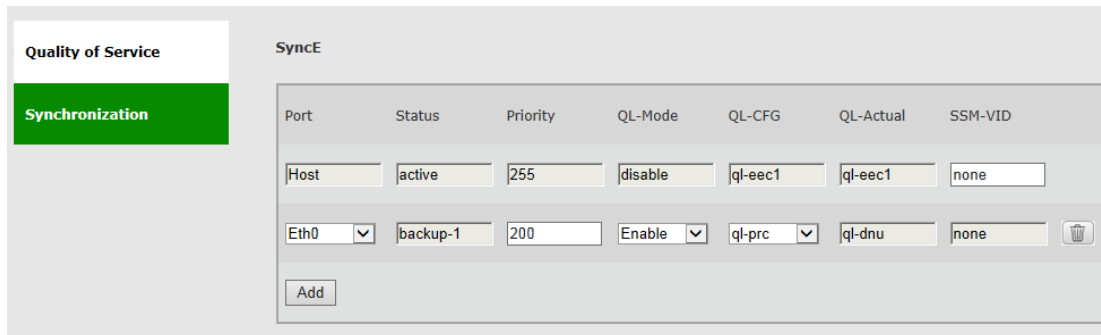


Figure 10-2 Advanced Config Page: Synchronization – SyncE

The reference clock (ref-clock) can be configured per interface.

This section allows configuring the following parameters:

- Port – the port the SyncE ref-clock is configured on: Host (internal clock, default settings cannot be changed), Eth0 (RF), Eth1 -4.
- Status – clock status: active, backup (and on what input), down.

- Priority – 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 254, where 1 is the highest priority.

One entry, for host, cannot be deleted and has the fixed priority of 255 (the lowest priority).

You cannot configure more than one interface with the same priority.

- QL-Mode – enable/disable. When ql-mode is disabled, ESMC messages are ignored and the status is determined by the **set ql-config** attribute.
- QL-CFG – ql config. Determines the quality level (ql) of the interface (values as in the ql table above).
- QL-Actual – R/O field. The quality level of the interface.
- SSM-VID – the VLAN ID ssm messages are sent over (default none=untagged).

Note:



It can take the system few minutes to lock on the new clock source after initial syncE setup.

10.1.2 Typical SyncE Scenario

Normal Operation

The local EtherHaul receives timing information on Eth1 from the network (source) with quality level PRC (2: ql-prc) and distributes it to all interfaces.

The remote EtherHaul receives timing information from the radio port (Eth0). Its quality level is PRC (2: ql-prc).

QL-Mode is enabled, meaning quality level is extracted from the ESMC messages.

DNU (15: ql-dnu, Do Not Use) is returned to the source in order to prevent timing loops.

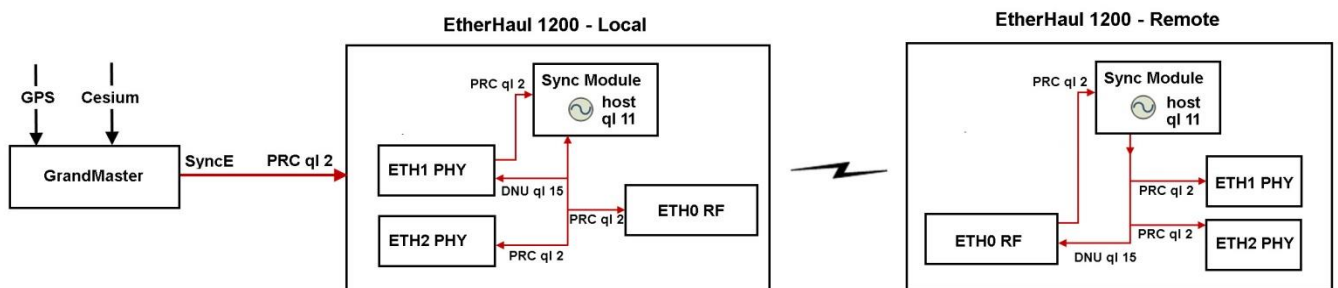


Figure 10-3 Typical SyncE Scenario – Normal Operation

The configuration for this scenario is:

```
Show ref-clock: Local EtherHaul Remote EtherHaul
```

<pre>ref-clock host prio ref-clock host status ref-clock host ql-actual ref-clock host ql-config ref-clock host ql-mode ref-clock host ssm-cvid</pre>	<pre>255 backup-1 ql-eecl ql-eecl disable none</pre>	<pre>255 backup-1 ql-eecl ql-eecl disable none</pre>
<pre>ref-clock eth1 prio ref-clock eth1 status ref-clock eth1 ql-actual ref-clock eth1 ql-config ref-clock eth1 ql-mode ref-clock eth1 ssm-cvid</pre>	<pre>200 active ql-prc ql-eecl enable none</pre>	
<pre>ref-clock eth0 prio ref-clock eth0 status ref-clock eth0 ql-actual ref-clock eth0 ql-config ref-clock eth0 ql-mode ref-clock eth0 ssm-cvid</pre>		<pre>200 active ql-prc ql-eecl enable none</pre>

Radio Failure

The local EtherHaul receives timing information on Eth1 from the network (source) with quality level PRC (2: ql-prc) and distributes it to all interfaces.

No incoming clock source on the remote EtherHaul as radio link is down.

The remote EtherHaul switches to holdover mode (internal clock) while maintaining the PRC clock accuracy it received previously and distributing it with its own quality level (11: ql-eecl).

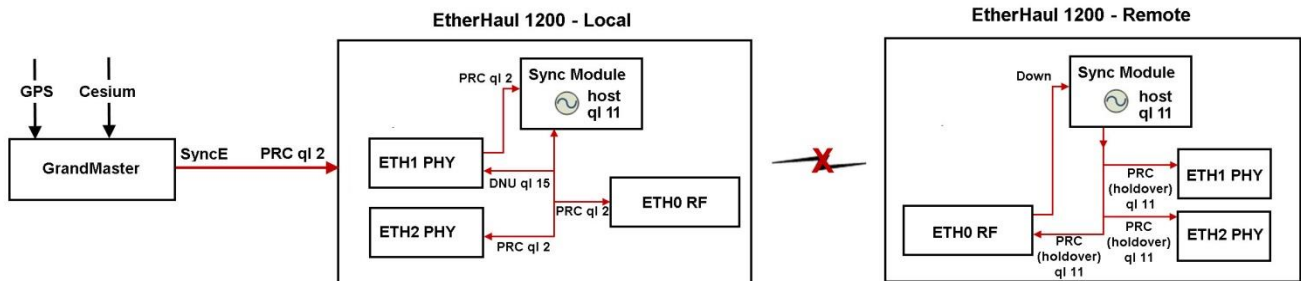


Figure 10-4 Typical SyncE Scenario – Radio Failure

The configuration for this scenario is:

Show ref-clock:	Local EtherHaul	Remote EtherHaul
<pre>ref-clock host prio ref-clock host status ref-clock host ql-actual ref-clock host ql-config ref-clock host ql-mode ref-clock host ssm-cvid</pre>	<pre>255 active ql-eecl ql-eecl disable none</pre>	<pre>255 active ql-eecl ql-eecl disable none</pre>

<pre>ref-clock eth1 prio ref-clock eth1 status ref-clock eth1 ql-actual ref-clock eth1 ql-config ref-clock eth1 ql-mode ref-clock eth1 ssm-cvid</pre>	<pre>200 down ql-dnu ql-eecl enable none</pre>	
<pre>ref-clock eth0 prio ref-clock eth0 status ref-clock eth0 ql-actual ref-clock eth0 ql-config ref-clock eth0 ql-mode ref-clock eth0 ssm-cvid</pre>		<pre>200 down ql-dnu ql-eecl enable none</pre>

Line Failure

No incoming clock source on the local EtherHaul as line link is down.

The local EtherHaul switches to holdover mode (internal clock) while maintaining the PRC clock accuracy it received previously and distributing it with its own quality level (11: ql-eecl1).

The remote EtherHaul receives and is locked on its Eth0 source and distributes timing information from this source to its interfaces.

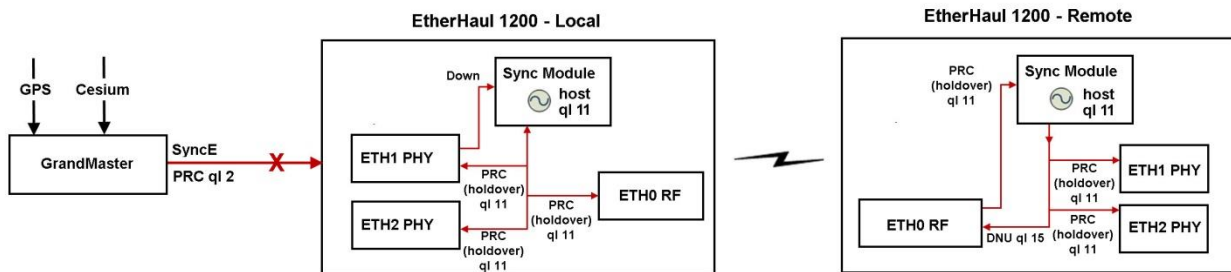


Figure 10-5 Typical SyncE Scenario – Line Failure

The configuration for this scenario is:

Show ref-clock:	Local EtherHaul	Remote EtherHaul
<pre>ref-clock host prio ref-clock host status ref-clock host ql-actual ref-clock host ql-config ref-clock host ql-mode ref-clock host ssm-cvid</pre>	<pre>255 backup-1 ql-eecl ql-eecl disable none</pre>	<pre>255 backup-1 ql-eecl ql-eecl disable none</pre>
<pre>ref-clock eth1 prio ref-clock eth1 status ref-clock eth1 ql-actual ref-clock eth1 ql-config ref-clock eth1 ql-mode ref-clock eth1 ssm-cvid</pre>	<pre>200 active ql-prc ql-eecl enable none</pre>	

<pre>ref-clock eth0 prio ref-clock eth0 status ref-clock eth0 ql-actual ref-clock eth0 ql-config ref-clock eth0 ql-mode ref-clock eth0 ssm-cvid</pre>		<pre>200 active ql-eecl ql-eecl enable none</pre>
---	--	---

10.1.3 Port Clock



Figure 10-6 Advanced Config Page: Synchronization – SyncE Port Clock

For Electrical 10/100/1000 ports (RJ45) the clock config can be set.

The port clock config is relevant only for SyncE configuration.

The Port Clock determines the clock flow direction (relevant only when carrying Sync E over 1000BaseT).

When using fibers (SFP), SFPs clock is carried independently and the clock configuration is not available.

The ports’ default is Auto (clock direction determined by the auto-neg protocol).

The relevant Ethernet standards define that two RJ45 ports connected between them MUST be configured to one of the automatic modes (auto or synce) or should be configured manually one to master and second to slave.

When using SyncE over RJ45, the Ethernet port’s Clock must be set manually as per one of the following options:

1. Option 1: Clock=synce. In this configuration, the clock direction is selected automatically by the SyncE SSMs.
2. Option 2: Clock=Master/Slave. Manually set Clock=Slave on the port that receives the SyncE clock and Clock=Master on the port that transmits the SyncE clock. This mode must be used when no SSMs are used on the network.

Configuring the port clock using the CLI:

```
set eth eth1 clock {auto | master | slave | synce}]
```

10.1.4 SyncE Alarms

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

10.2 IEEE 1588v2

The EtherHaul supports IEEE 1588v2 Transparent Clock (TC). The support is hardware based. The operator is required to have a software license to activate the capabilities. The EtherHaul complies with the mobile backhaul specifications for packet synchronization distribution backhaul architectures for mobile radio access networks.

1588 Transparent Clocks (TCs) used to overcome the 1588 synchronization performance issue due to packet delay variation over the network. In a wireless link the compensation of the PDV needs to be done for the entire link including the air interface and not only per node. The time stamping and the correction field update is HW based.

IEEE 1588 is supported for EH-1200F/FX and EH-600T systems.

10.2.1 IEEE 1588 Configuration

IEEE 1588

Operational Status	<input type="text" value="down"/>
PTP Encapsulation	<input type="text" value="ptp-over-ip"/>
Air-Delay Correction	<input type="text" value="0"/>
Air-Delay	<input type="text" value="636"/>
Link Length	<input type="text" value="0"/>
Modified Packets Counter	<input type="text" value="0"/>

Figure 10-7 Advanced Config Page: Synchronization – IEEE 1588

In wireless link the compensation of the PDV needs to be done for the entire link including the air interface and not only per node.

Siklu's 1588 Transparent Clock (TC) implements one step end to end HW time stamping and distributed TC algorithm to synchronize the two ends of the link. The accuracy level of the synchronization correction field between the two sides is <100ns and complies with the most stringent accuracy level required (accuracy class level 6) on all of the Ethernet ports.

IEEE 1588 is a licensed feature that requires license for operation. Before configuring it, verify that license is available and enable the **synce** license.

This section allows configuring the following parameters:

- Checkbox to enable /disable the feature (default disabled).
- Operational Status – Read Only field. Will be Up if the 1588 is configured correctly on both sides and both sides time stamp counter are in sync.

Note that it can take up to 5 minutes till sync is achieved and operational status will be Up.
- PTP Encapsulation – ptp-over-ip or ptp-over-Ethernet.
- Air Delay Correction – Manual correction of air delay (in nSec). Correction may positive or negative.
- Air Delay – Read Only field. Measured air delay (including modem delay) in nSec by the system. Takes in account air-delay-correction.
- Air Distance – Read Only field. Measured air distance in meters by the system. Takes in account air-delay-correction (manually changing the air-delay correction affects the air-distance).

Displayed as Link Length on the web-based management's **Main Page**.

- Modified Packets Counter – The number of 1588 packets which passed through the system and stamped. The counter is cleared upon reboot (no option to clear it manually).

Configuration and monitoring using the CLI:

```
Configuration:  
set ieee1588 admin up air-delay-correction 0  
  
Viewing status:  
show ieee1588
```

For 1588 phase locking, SyncE must be configured (for frequency locking) even in the absence of SyncE signal over the link. Basic SyncE configuration may be applied.

Local side (network side) – assuming local clock (Host) is used (no SyncE running):

```
set ieee1588 admin up
```

Remote side (BTS side):

```
set ref-clock eth0 prio 100 ql-config ql-eecl ql-mode disable  
set ieee1588 admin up
```

11 ExtendMM™

This chapter describes the ExtendMM feature – extended range solution that allows delivering Gigabit throughput over interference-free millimeter waves for long distances by using a Sub-6 GHz radio link backup.

How does it work? By combining any Siklu EtherHaul millimeter wave radio with 1ft. antenna, any sub-6 GHz radio and Siklu’s advanced networking capabilities. With a single click you can turn the two radios into an extended link solution that delivers the capacity you need over the distance you require.

11.1 ExtendMM™ Description

Siklu’s ExtendMM™ creates an always-on, all-weather, extended range connection by combining any Siklu EtherHaul-1200 millimeter wave radio (1ft. antenna) with any sub-6 GHz radio. With a single click you turn the two radios into a single high-performance long-distance link.

Most of the year you will benefit from 1 Gbps over the interference-free millimeter wave EtherHaul link. The sub-6 GHz link will be in stand-by mode.

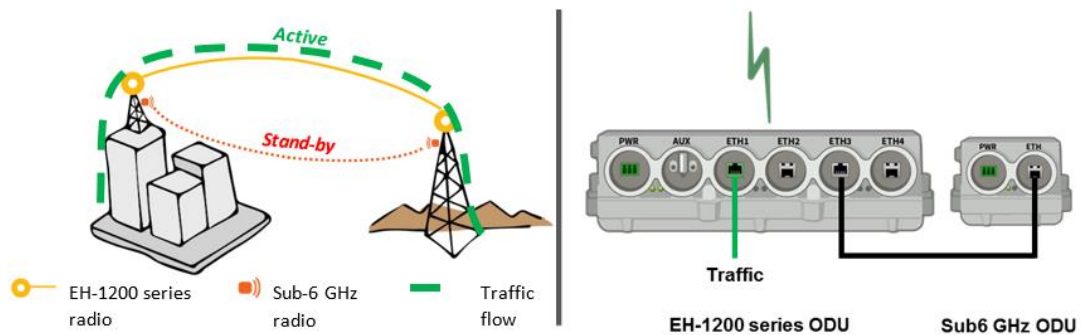


Figure 11-1 ExtendMM™ in normal operation (sub-6 GHz in stand-by mode) Criteria

When a significant rain event happens, the ExtendMM™ solution automatically switches the high priority traffic, hitlessly, from the primary EtherHaul path to the sub-6 GHz path. As the rain cell passes, the link immediately returns to Gigabit speed. No additional networking equipment is needed. The EtherHaul powerful, integrated networking engine does everything for you.

As the capacity of the sub-6 GHz link is lower than the 1 Gbps capacity of the EtherHaul, the ExtendMM allows to leverage the EtherHaul traffic prioritizing capabilities extending the availability of the high priority traffic. When the significant rain event happens activating the adaptive capabilities of the EtherHaul. When the EtherHaul capacity reaches the configured threshold, the high priority traffic is forwarded to the sub-6 GHz link. Switching the traffic routing to the sub-6 GHz link is done hitlessly by the EtherHaul

integrated, powerful networking engine. When the rain cell moves on and the EtherHaul can provide a capacity higher than the configured threshold, the traffic is routed hitlessly back to the EtherHaul.

11.2 ExtendMM™ Requirements

The ExtendMM solution is based on the ITU-T G.8032 Ethernet Ring Protection Switching standard. This standard uses advanced and fast networking capabilities to detect main link failure and route the traffic seamlessly to the backup path and back.

The ExtendMM solution will operate with any sub-6 GHz, Ethernet, transparent bridge which will transport any type of Layer 2 broadcast or multicast traffic.

Mount the EtherHaul and sub-6 GHz radios and establish reliable connectivity of both. Connect the traffic cable to the EtherHaul port (Eth1). Connect the sub-6 GHz radio to the EtherHaul port (Eth2 is the default).

11.3 ExtendMM™ Configuration

The ExtendMM will operate with the default parameters in the majority of the cases. If required the default parameters may be configured in the ExtendMM™ section under Advanced Config.

ExtendMM™	
ExtendMM™ Enable	<input type="checkbox"/> Copy to Remote >>
Role	master
Backup Port	eth2
VID	1
Capacity Threshold [Mbps]	20
Main Path	down
Backup Path	down

Figure 11-2 Advanced Config Page: ExtendMM™

This section allows configuring the following parameters:

- Role – the EtherHaul radio on one side of the link should be “master” while the other should be “slave”.
- Backup Port – the Ethernet port in the EtherHaul to which the sub-6 GHz radio is connected to. (Default: Eth2)
- VID – VLAN id used for the backup signaling (G.8032). (Default: 1)
- Capacity Threshold [Mbps] – the capacity for which below it the traffic is routed to the sub-6 GHz link. (Default: 80 Mbps).
- Main Path – status of the EtherHaul main path link.
- Backup Path – status of the sub-6 GHz backup path link.

Note:



As the ExtendMM solution is based on the ITU-T G.8032 Ethernet Ring Protection Switching standard, refer to the Ethernet Ring Protection (ERP) section of this document for in-depth description of the protection mechanism.

12 Ethernet Ring Protection (ERP)

This chapter describes the Ethernet Ring Protection functionality based on G.8032v2.

Note:



ERP configuration and monitoring supported in the CLI only.

ERP is a licensed feature that requires license for operation. Before configuring it, verify that license is available and enable the **L2 (resiliency)** license component.

12.1 Ethernet Ring Protection Description

Ethernet Ring Protection (ERP) is a network resiliency protocol defined in ITU-T G.8032. The EtherHaul 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 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 provides protection and recovery switching within 50 mSec for typical rings. The ERP mechanism uses a very small percentage of total available bandwidth.

The following figure 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.

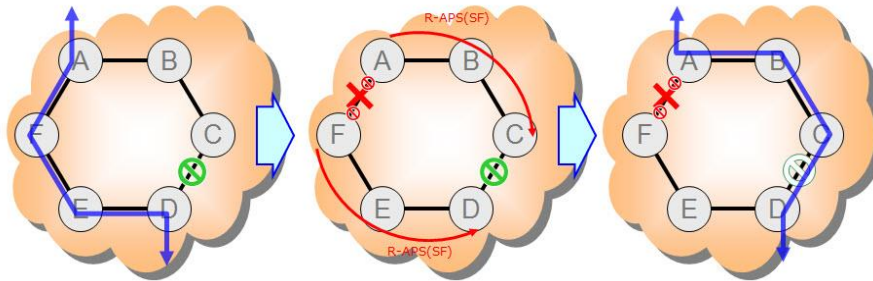


Figure 12-1 Basic ERP Protection Mechanism

12.2 Supported ERP Features

Among the ERP features supported by the EtherHaul 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
- Link failure detection can be based over CCM's or Physical link down.
- By default the failure detection based on link down detection.

Using CCM's for failure detection required MEP settings 300Hz (every 3.3 ms) for sub 50ms switchover.

12.3 ERP Ring Commands

To set a ring, use the following command:

```
CLI>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>
```

To display ring statistics, use the following command:

```
CLI>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:

```

CLI>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 lis ready Role none

```

CLI example for setting failure detection based on CCM's:

```

CLI>set ring 1 cw-mep ?
none | {<md-idx> <ma-idx> <mep-id> <peer-mep-id>}

```

12.4 ERP Administrative Commands

The EtherHaul 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.

```

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

```

```

CLI>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
```

```
CLI>show ring all state
```

```
ring 3 state           : fs
```

```
CLI>set ring 3 action clear
```

```
Set done: ring 3
```

```
CLI>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
```

```
CLI>set ring 3 action acw-ms
```

```
Set done: ring 3
```

```
CLI>show log
```

```
Aug  4 21:43:18 sw cad: local Manual switch at 200 CW unblocked  
ACW blocked
```

```
CLI>set ring 3 action clear
```

```
Set done: ring 3
```

```
CLI>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
```

12.5 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

12.6 Sample ERP Configuration

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
ring 1 cw-status-data : unblocked
ring 1 acw-status-data : unblocked
ring 1 cw-status-raps : unblocked

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 acw-status-data : blocked
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>

13 Operation, Administration and Maintenance (OAM)

This chapter describes the Operation, Administration and Maintenance (OAM) capabilities of the EtherHaul system and includes the following topics:

- Connectivity Fault Management (CFM) as per IEEE 802.1ag
- Link OAM as per IEEE 802.1ah
- Performance Monitoring as per Y.1731

Note:



OAM configuration and monitoring supported in the CLI only.

OAM is a licensed feature that requires license for operation. Before configuring it, verify that license is available and enable the **L2 (oam)** license component.

13.1 CFM (Connectivity Fault Management)

This section describes the CFM functionality and details the configuration and monitoring options and includes the following topics:

- CFM Overview
- Working with Maintenance Domains (MD)
- Working with Maintenance Associations (MA)
- Working with Component Maintenance Associations
- Working with Maintenance End Points (MEP)
- Working with Peer MEPs
- Working with CCM Messages
- Working with Link Trace Messages
- Sample CFM Configuration

13.1.1 CFM Overview

Connectivity Fault Management (CFM) is an Ethernet layer operation, administration, and management (OAM) protocol designed to monitor and troubleshoot networks. CFM enables 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.

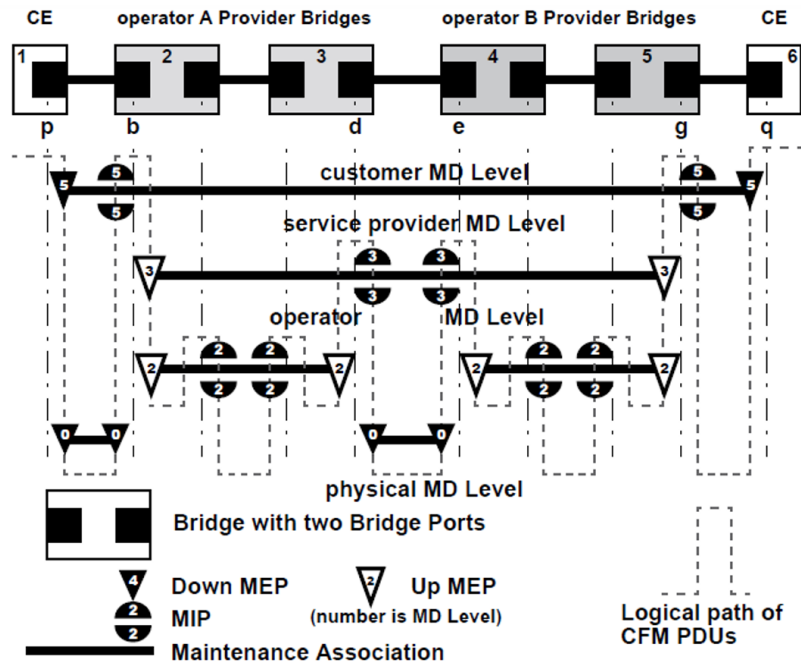
CFM is designed to be transparent to the customer data transported by the network and to provide maximum fault coverage. These capabilities are used in networks operated by multiple independent organizations, each with restricted management access to each other's equipment.

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.

The system allows to:

- Define Maintenance Domain (MD)
- Define Maintenance Association (MA)
- Define Maintenance Association End Points (MEPs) and Maintenance Association Intermediate Points (MIPs)



UP MEP – transmit CFM PDUs into the bridge
 Down MEP – transmit CFM PDUs out of the bridge

Figure 13-1 CFM Network

The system supports the following monitoring tools:

- CFM Continuity Check Message (CCM)
- CFM Linktrace
- CFM Loopback

13.1.2 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
```

13.1.3 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}
```

13.1.4 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}
```

13.1.5 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 | lbr-tx-sn | lbr-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.

13.1.6 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}
```

13.1.7 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
```

13.1.8 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.

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.

13.1.9 Sample CFM Configuration

This section provides a sample CFM configuration script.

Configuring the Local System

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 port (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 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 System

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 mhfc-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 System

The following set of commands sets up the Loopback on the local System. 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

```

13.2 Performance Monitoring (ITU-T Y.1731)

Performance monitoring provides monitoring functionality according to Y.1731 standard. The following measurements are supported:

- Frame delay measurements
- Frame jitter measurements
- Frame loss measurements

The Performance Monitoring is based on the CFM configuration.

The statistics are presented between the cfm-meps.

Loss and Delay measurements are given for the traffic on the CFM MA. Special 64 bytes packets are used for this purpose (DMM) in intervals of 10 seconds (configurable).

To enable and monitor Y.1731 measurement for MEPs based on the Sample CFM Configuration example above)

- Enable lm (loss measurement) and dm (delay measurement) on local (Link and Customer levels):

```

set cfm-mep 1 1 1 lm enabled
set cfm-mep 1 1 1 dm enabled
set cfm-mep 2 2 1 lm enabled
set cfm-mep 2 2 1 dm enabled

```

- Enable lm (loss measurement) and dm (delay measurement) on remote (Link and Customer levels):

```
set cfm-mep 1 1 2 lm enabled
```

```
set cfm-mep 1 1 2 dm enabled
```

```
set cfm-mep 2 2 2 lm enabled
```

```
set cfm-mep 2 2 2 dm enabled
```

- To monitor the loss and delay

```
show cfm-peer-mep 1 1 1 2 statistics <- to the peer
cfm-peer-mep 1 1 1 2 far-end-loss           : 0
cfm-peer-mep 1 1 1 2 near-end-loss         : 0
cfm-peer-mep 1 1 1 2 total-tx-far-end     : 3178
cfm-peer-mep 1 1 1 2 total-tx-near-end    : 3932
cfm-peer-mep 1 1 1 2 delay                : 745
cfm-peer-mep 1 1 1 2 delay-variation      : 320
cfm-peer-mep 1 1 1 2 elapsed-time         : 0000:00:48:42
```

13.3 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 to detect, verify, and isolate connectivity failures in point-to-point connections.

The following functionality is supported:

- Discovery
- Remote Loopback

13.3.1 Link OAM Configuration

Link OAM can be enabled on one of the link interfaces (Eth1, Eth2, Eth3 or Eth4) or the radio interface (Eth0).

To enable Link OAM:

```
set link-oam <eth-list> [admin <value>]
<eth-list>                : eth0 | eth1 | eth2 | eth3 | eth4
[admin <value: Enabled | disabled >]
```

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

To view Link OAM configuration and status:

```
CLI>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
```

13.3.2 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):

```
CLI>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
```

13.3.3 Link OAM Loopback

Link OAM loopback is supported and can be enabled on the Ethernet port. Once enabled, traffic received on the port is looped back to the port that 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**:

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

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

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

To view loopback settings:

```
CLI >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**;

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

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

14 Administration

This chapter describes the system's administration capabilities and procedures and includes the following topics:

- Users Administration
- SNMPv3 Users Configuration
- Zero-Touch Configuration
- Monitoring CLI Login Sessions
- DHCP Relay (Option 82)

14.1 TACACS+/RADIUS Users Administration

The EtherHaul supports both internal user management and external Radius or TACACS server.

To administrate users, refer to the **Users Administration** section in the **Network** Page.

The page will be updated based on the selected **Authentication Mode**.

For internal user management (standard user/passwords that are configured in the device), select **Local** as the **Authentication Mode**.

Local users administration (default mode) is described in the to the *Users Administration* section under *Network Configuration and Monitoring* chapter of this manual.

14.1.1 AAA Description

RADIUS (Remote Authentication Dial-In User Service) and **TACACS+** (Terminal Access Controller Access-Control System) are AAA mechanisms.

- **Authentication:** Identification of requester profile (username, password, and privilege level) on a per-request basis.
- **Authorization:** Permission/denial of access to a subset of commands subject to authentication success/failure. (The mechanisms of Authorization and authentication are independent of each other.)
- **Accounting:** Reporting of information on requesters (identities, number of access attempts per requester, start and stop times, executed commands, etc.)

The EtherHaul is a Network Access Server (NAS) for requesters and functions as AAA client passing requester information (e.g. username, password, etc.). The AAA Server is responsible for receiving connection requests, authenticating or disqualifying the requester, and sending the permit or denies response to the EtherHaul client. Communication between the EtherHaul and the AAA Server are permitted by shared secrets which are never sent over the network. In addition, every administrator

password is encrypted before it is sent between the EtherHaul and the AAA Server in order to prevent deciphering.

The AAA Server can also provide accounting of requester commands and of changes in authorization level. This information is recorded in a special log file that enables a supervisor to view the activities of all the administrators. Accounting can include logging of commands or logging of transitions from one mode to another.

The EtherHaul supports authentication with up to five TACACS+ or Radius AAA servers.

14.1.2 Authentication Modes

Three Authentication modes supported:

- Local – Users configured in EtherHaul, including name, password and type.
- Tacacs – Users configured in the AAA Tacacs server. Only Admin user configured in EtherHaul.
- Radius – Users configured in the AAA Radius server. Only Admin user configured in EtherHaul.

Every change in the Auth-mode deletes all users (except for the admin user) and configured servers.

Communication between the EtherHaul and the AAA servers is done over shares secret.

14.1.3 TACACS Authentication Mode

Authentication Mode

Local
 Radius
 Tacacs
 Shared Secret:

Name	Type	Password
<input type="text" value="admin"/>	<input type="text" value="admin"/>	

Password Min Length :
 Password Min Difference :

#	IP Address	Protocol Port	Accounting Port	Dummy Auth Status
<input type="text" value="1"/>	<input type="text" value="192.168.0.222"/>	<input type="text" value="49"/>	<input type="text" value="ssh"/> <input type="button" value="v"/>	<input type="text" value=""/> <input type="button" value="trash"/>

Server Index :
 Username :
 Password :

Figure 14-1 Network Page: Users Administration – TACACS

Only **admin** user is defined in the system. All other users (including their name, password and type) are defined in the server.

Note that local admin access will always be available (regardless of the connectivity to the AAA server).

This section allows configuring the following parameters:

- Authentication Mode – Tacacs.
- Shared Secret – In Radius or Tacacs mode, Shared Secret should be entered (identical to the one in the server). Note that is using more than one AAA server, the servers should have the same Shared Secret.
- # - Server index. Up to 5 servers can be configured. The Authentication starts from the 1st server and goes down to the 5th.
- IP Address – of the AAA server.
- Protocol Port – the default port for Tacacs is 49.
- Accounting Port – none, SSH, HTTP, all.

Dummy Authentication is used for sanity check (connectivity test) to the AAA server.

If the AAA server has Dummy user define, select the Server Index and enter the username and password. After clicking **Send Dummy Auth**, you will be able to see the reply status in the **Dummy Auth Status** field.

Dummy Authentication is supported for Tacacs only.

14.1.4 Radius Authentication Mode

Authentication Mode

Local
 Radius
 Tacacs
 Shared Secret:

Name	Type	Password
<input type="text" value="admin"/>	<input type="text" value="admin"/>	
<input type="text" value="cvsadmin"/>	<input type="text" value="tech"/>	<input type="button" value="🗑"/>
<input type="text" value="db2admin"/>	<input type="text" value="super"/>	<input type="button" value="🗑"/>
<input type="text" value="bwadmin"/>	<input type="text" value="user"/>	<input type="button" value="🗑"/>

Password Min Length :
 Password Min Difference :

#	IP Address	Protocol Port	Accounting Port	Dummy Auth Status
<input type="text" value="1"/>	<input type="text" value="192.168.0.222"/>	<input type="text" value="1812"/>	<input type="text" value="none"/>	<input type="text" value=""/>

Server Index :
 Username :
 Password :

Figure 14-2 Network Page: Users Administration – Radius

Only **admin** user is defined in the system. All other users (including their name, password and type) are defined in the server.

Note that local admin access will always be available (regardless of the connectivity to the AAA server).

This section allows configuring the following parameters:

- Authentication Mode – Radius.
- Shared Secret – In Radius or Tacacs mode, Shared Secret should be entered (identical to the one in the server). Note that if using more than one AAA server, the servers should have the same Shared Secret.
- # - Server index. Up to 5 servers can be configured. The Authentication starts from the 1st server and goes down to the 5th.
- IP Address – of the AAA server.
- Protocol Port – the default port for Radius is 1812.
- Accounting Port – none, SSH, HTTP, all.

Dummy Authentication is not supported for Radius (Tacacs only).

Working with Radius

Add the following lines to your Radius dictionary:

```
#####      SIKLU Additions      #####  
ATTRIBUTE SKL_USERGROUP      170 string
```

When adding users to the SKL_USERGROUP and assigning them type, use '_' before the type:

```
User with 'admin' type:  
SKL_USERGROUP = "SKL_USERGROUP=_admin"  
  
User with 'super' type:  
SKL_USERGROUP = "SKL_USERGROUP=_super"
```

14.2 CLI Commands

- Users:

```
Viewing users list:  
show user
```

- Tacacs:

```
Viewing authentication:  
show aaa  
  
Configuring Tacacs authentication:  
set aaa mode tacacs shared-secret 123456  
  
Viewing servers:  
show aaa-server  
  
Configuring Tacacs server:  
set aaa-server 1 ip-addr 192.168.0.22 port 49 accounting-port ssh  
  
Sending Dummy Authentication request:  
set aaa-server 1 send-dummy-auth username dummy1 password pass1  
  
Viewing Dummy Authentication status:  
show aaa-server
```

- Radius:

```
Viewing authentication:  
show aaa  
  
Configuring Radius authentication:  
set aaa mode radius shared-secret 123456  
  
Viewing servers:  
show aaa-server
```

```
Configuring Tacacs server:
set aaa-server 1 ip-addr 192.168.0.22 port 1812 accounting-port ssh
```

14.3 SNMPv3 Users Configuration

Note:



SNMPv3 Users configuration supported in the CLI only.

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 other than the user name are supplied to the set command, an entry is created for the user identified by the name while privacy and authentication algorithms are set to NULL.

If a privacy algorithm (des or aes) is not supplied, the privacy algorithm is set to NULL.

If a privacy-passphrase is not supplied, the privacy-passphrase is the same as the authentication passphrase.

SNMP Managers

Each SNMPv3 agent has an engine ID that uniquely identifies the agent in the device and also the unique identification of the MIB objects within a domain.

In SNMPv3 communication, Engine ID is used as an identifier for an agent among other agents.

When you define **get** and **set** commands for SNMPv3 user, set Engine ID to Local. When you define trap for SNMPv3 user, set Engine ID to the value of the Engine ID of the remote manager.

Note that get, set, and trap commands should be defined for the same user. The same user should be defined twice: once with Engine ID=Local and the second time with the Engine ID of the remote manager.

14.4 Zero-Touch Configuration

Zero Touch enables the user to quickly and easily commission the link and complete the startup configuration process.

The process begins with the remote and automatic configuration files, which enable the transfer and loading of the software file. The process results in full radio configuration, completed without any need for intervention from the installer part.

Note:



Zero Touch configuration supported in the CLI only.

14.4.1 Requirements

Ensure that the following requirements are in fulfilled in order to enable Zero Touch:

- The system must have an enabled DHCP server and a TFTP server, as well as access to your servers.
- Connectivity to the servers must be verified. The Vlan for Inband management must be set to the correct operator Vlan.
- The operator must set the unit's frequency to the requested or default frequency.

System configuration:

- Enable the Net-config file (`set net-config config-file enable`).
- Enable the DHCP server (`set ip 2 ip-addr dhcp`).

14.4.2 Zero Touch System Process

1. The system starts and attempts to run the startup-config file.
2. If the startup-config file does not exist, the system runs the default config file and then the customer_default_config file if it exists on the system.
3. If the DHCP-config file is enabled, the script runs on the DHCP server allocating an IP address to the system.
4. The DHCP server points to the TFTP server that contains the user's "zero_touch.txt" configuration file.

In the following example, system name is changed to EtherHaul_SiteA, it then copies a new software version and upgrades the software version if the current version number is not the same as the most recently available version.

```

### Configuration file ###
# Set the system name
set system name EtherHaul_SiteA
# Copy the following sw and upgrade it if differs from
siklu-uimage-5.0.0-9900
copy sw tftp://192.168.0.222/siklu-uimage-5.0.0-9931
if-version-differs-from siklu-uimage-5.0.0-9900
run sw immediate no-timeout if-version-differs-from
siklu-uimage-5.0.0-9931

```

The configuration file and the SW version should be stored in the TFTP server directory. If any errors occur during the execution of the DHCP script, the error file uploads to the server, restarts the system and sends an SNMP trap.

14.4.3 CLI Configuration for Zero Touch using the CLI

Begin the configuration with the following command to enable the net-config file. This allows the unit to be configured through the network:

```

default>set net-config config-file enable
Set done: net-config

```

Confirm that the config file was successfully enabled:

```

default>show net-config
net-config config-file          : enable
net-config config-error-restart-delay: 60

```

Then ensure that the DHCP server is enabled:

```

default>set ip 1 ip-addr dhcp
Set done: ip 1

```

Confirm that that the DHCP server was successfully enabled:

```

EH1200F_Left_213>show ip
ip 1 ip-addr          : dhcp 0.0.0.0
ip 1 prefix-len      : 0
ip 1 vlan            : 0
ip 1 default-gateway : 212.143.164.214

ip 2 ip-addr          : static 212.143.164.213
ip 2 prefix-len      : 30
ip 2 vlan            : 0
ip 2 default-gateway : 212.143.164.214

```

Move the configured file to the unit through the TFTP Server:

```

Run configuration file /var/sw/etc//customer_default_config.txt

```

If an error occurs in the script, causing the configuration to fail, an error message to the TFTP Server and the unit sends an SNMP trap. The following command allows you to set the delay time before the system restarts the configuration:

```
set net-config [config-file <value>] [config-error-restart-delay <value>]
```

The Show status command shows the status of the net config or the startup-config:

```
default>show status
startup-config | net-config
```

The following response to the prompt to show the net-config status indicates that the Zero Touch configuration is complete:

```
default>show status net-config
NetConfig was successful
```

14.5 Monitoring CLI Sessions

Note:



Monitoring CLI login sessions supported in the CLI only.

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

ddd: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.

The maximum number of CLI sessions is 10.

14.6 DHCP Relay (Option 82)

Since DHCP packets cannot travel across a router, a relay agent is necessary in order to have a single DHCP server handle all leases.

Relay agents receive broadcast DHCP packets and forward them as unicast packets to a DHCP server.

Note:



Configuring DHCP Relay supported in the CLI only.

With the DHCP option-82 feature enabled, port-to-port DHCP broadcast isolation is achieved when the client ports are within a single VLAN. During client-to-server exchanges, broadcast requests from clients connected to VLAN access ports are intercepted by the relay agent and are not flooded to other clients on the same VLAN. The relay agent forwards the request to the DHCP server. During server-to-client exchanges, the DHCP server sends a broadcast reply that contains the option-82 field. The relay agent uses this information to identify which port connects to the requesting client and avoids forwarding the reply to the entire VLAN.

When enabling DHCP relay agent option 82:

- The host (DHCP client) generates a DHCP request and broadcasts it on the network.
- The system (DHCP relay agent) intercepts the broadcast DHCP request packet and inserts the relay agent information option (option 82) in the packet. The relay information option contains the system's MAC address (the remote ID sub-option) and the port SNMP ifindex from which the packet is received (circuit ID sub-option).
- The system forwards the DHCP request that includes the option-82 field to the DHCP server.
- The DHCP server receives the packet. If the server is option-82 capable, it might use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.
- If the server does not support option 82, it ignores the option and does not echo it in the reply.
- The DHCP server unicasts the reply to the relay agent. The relay agent makes sure that the packet is destined for it by checking the IP destination address in the packet. The relay agent removes the option-82 field and forwards the packet to the system port that connects to the DHCP client, which sent the DHCP request.

Enabling DHCP Relay

```
set net-config dhcp-relay enable
```

Viewing DHCP Relay status

```
show net-config dhcp-relay
```

```
net-config dhcp-relay          : enable
```

15 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 for 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:

- Troubleshooting Process
- System LEDs
- Alarms
- Performance Statistics
- Loopbacks

15.1 Troubleshooting Process

Follow this step-by-step process whenever you encounter a problem with the link.

Step 1: 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).

Step 2: 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.

Step 3: 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.

Step 4: 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 you repeat commissioning tests in order to verify that the problem link is now operating correctly.

Step 5: Need Support?

Contact Siklu for technical support in case assistance is needed.

Include detailed description of the issue and what steps were taken trying to solve it.

Send the output of the **System_info** script from both sides (copy its output to a text file) for efficient service.

The script collects all the relevant system status, logs, configurations and statistics.

15.2 System LEDs

LED	Color	Description
PWR (Power)	Green – Power OK	Blink Green – Device boot
	Red – Power Failure	
	Off – No Power	
RF	Green – Link Up	Blink Green – Device boot
	Orange – Alignment Mode	
	Off – Link Down	
ETH1/2/3/4:	Green – Link 1G	Blink Green – 1G activity
	Orange – Link 10/100	Blink Orange – 10/100 activity
	Off – No Link (Carrier)	

15.3 Alarms

System alarms can be found on the **Main** Page, including:

- Current Alarms – list of currently active alarms and date+time raised.
- History Log – System alarms and events history log

Event Name	Description	Probable Cause	Corrective Actions
Cold start: the first time wake up	System power up after power connection	1) Restoring the power 2) Reset caused by power disruption	Power restored, no corrective actions needed
Cold start: software initiated reset	System power up after user-initiated software reset	1) User action: reset system 2) User action: rollback timeout expired 3) User action: SW upgrade	Power restored after user action, no corrective actions needed
Cold start: reset button has been pushed for less than 5 sec	System power up after user pressed the reset button (for less than 5 seconds)	1) User action: reset button pressed for less than 5 seconds causing a reset	Power restored after user action, no corrective actions needed
Cold start: reset button has been pushed for more	System power up after user pressed the reset button	1) User action: reset button pressed for more than 5 seconds causing	Power restored after user action, no corrective actions needed

than 5 sec	(for more than 5 seconds), restoring factory defaults	factory defaults restore	
Cold start: power failure reset	System power up after system reset due to power or internal failure	1) Restoring the power 2) Reset caused by power disruption or internal power failure	Power restored, no corrective actions needed. If repeated and no indication for power disconnection, might indicate system failure and ODU should be replaced.
Cold start: hardware watchdog reset	System power up internal HW watchdog reset, indication system fault	System failure	Replace ODU
Cold start: the hardware watchdog has not been activated in time	Internal HW watchdog failure, indicating system fault	System failure	Replace ODU
Cold start: software watchdog reset	System power up internal SW watchdog reset, indication system fault	System failure	Replace ODU
Link down	Link down (operational down) on one of the Ethernet interfaces	Line interfaces (eth1,eth2,eth3,eth4): 1) Ethernet cable disconnected or not connected properly. 2) Ethernet interface disabled (admin down). 3) Port settings mismatch 4) Interface HW fault. Radio interface (eth0): 1) Low receive signal (due to antenna mis-alignment or rain fading). 2) Mismatch in rf configuration between sides or wrong configuration. 3) Interference. 4) HW fault.	Line interfaces (eth1,eth2,eth3,eth4): 1) Verify cable terminated and connected properly. 2) Verify port configuration, including auto-neg and speed/duplex. 3) Replace ODU. Radio interface (eth0): 1) Improve antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.
Link Up	Link up (operational up on one of the Ethernet	Link down state cleared and interface is up (operational).	Link restored, no corrective actions needed.

	interfaces		
Modulation Change	RF link modulation changed to the specified modulation profile	In adaptive mode: Modulation changed (up or down) due to change in link RF link conditions. In static mode: Modulation changed manually or when link changed state to up or down.	Verify if modulation change is due to rain fading, mis-alignment or interference. 1) Improve antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.
Temperature High	Extreme temperature condition (unit temperature is too high or too low, exceeding the configurable thresholds)	Extreme temperature condition.	1) Verify air-flow not obstructed. 2) Verify ODU is installed in temperature range according to specs.
Temperature Normal	Unit temperature returned to normal	The unit temperature condition returned to normal.	Temperature returned to normal, no corrective actions needed.
SFP In	SFP inserted to one of the Line Ethernet ports	User action: SFP was inserted.	User action: No corrective actions needed.
SFP Out	SFP extracted from one of the Line Ethernet ports	User action: SFP was extracted.	User action: No corrective actions needed.
Ref Clock Changed	Interface reference clock changed its Quality Level	Reference clock have changed due to: (eth1,eth2,eth3,eth4): 1) The previously-active clock source in SyncE configuration is down. 2) The active clock source received SSM with different quality level. 3) User action: change of clock settings in SyncE configuration. Note that "ref-clock change host ql-eec1" event is part of the normal startup of the system.	Verify reason for ref-clock change (line disconnected, RF link down...) and implement the relevant corrective actions.
EEC1 or worse	The SyncE interface receives SSMs with QL	1) Clock source of Host is used. 2) Active clock source used	Verify reason for ref-clock change (line disconnected, RF link down...) and implement the

	level equal to EEC1 or worse.	has Quality Level of EEC1 or worse.	relevant corrective actions.
Better than EEC1	The SyncE interface receives SSMs with QL level equal to EEC1 or worse.	1) Active clock source has Quality Level better than EEC1	Normal state, no corrective actions needed.
Loop Enabled	Loopback was enabled on one of the Ethernet interfaces	User action: Loopback enabled.	User action: No corrective actions needed.
Loop Disabled	Loopback was disabled on one of the Ethernet interfaces	1) Loopback cleared as loopback timeout expired. 2) User action: Loopback disabled.	User action: No corrective actions needed.
Tx Mute Enabled	Tx mute enabled (ODU will not transmit on its radio interface)	User action: ODU muted.	User action: No corrective actions needed.
Tx Mute Disabled	Tx mute disabled (ODU will resume transmitting on its radio interface)	1) Tx mute cleared as Tx mute timeout expired. 2) User action: Tx mute disabled.	User action: No corrective actions needed.
CFM Fault Alarm	CFM Defect has been detected (loss of CCMs)	CFM connectivity defect: 1) Loss of connectivity due to cable or radio disconnection. 2) Configuration mistake. None: CFM connectivity (remote ccm) restored.	Verify reason for ccm disconnection (line disconnected, RF link down...) and implement the relevant corrective actions.
Net Config Error	Error in Net-Config script	1) Missing config file 2) Config file cannot be loaded	1) Verify net-config configuration, including DHCP and FTP setup and connectivity. 2) Verify config file exists.
ERP Ready	ERP state is optimal (no alarms and working on primary path) with indication if CW or ACW ports are blocked (not sending traffic) or unblocked (sending traffic)	ERP state is OK and protection is available.	No corrective actions needed.

ERP Forced Switch	ERP Forced Switch notification on local or remote (any remote unit in the ring) with indication if CW or ACW ports are blocked (not sending traffic) or unblocked (sending traffic)	User action: Forced Switch	
ERP Manual Switch	ERP Manual Switch notification on local or remote (any remote unit in the ring) with indication if CW or ACW ports are blocked (not sending traffic) or unblocked (sending traffic)	User action: Manual Switch	
ERP Signal Fail	ERP Signal Fail notification on local or remote (any remote unit in the ring) with indication if CW or ACW ports are blocked (not sending traffic) or unblocked (sending traffic)	<ol style="list-style-type: none"> 1) ERP config mismatch or wrong configuration 2) Disconnection in the ring, sending alarm 	<ol style="list-style-type: none"> 1) Verify ERP configuration and RAPS continuity. 2) Verify reason for signal fail state (line disconnected, RF link down...) and implement the relevant corrective actions.
ERP Invalid version	ERP different versions (ERP V1 or V2) notification.	One of the elements in the ring has different ERP version.	Verify same version is used
CINR Out Of Range	CINR dropped below configured CINR threshold.	CINR drop (below configured threshold) due to change in RF link conditions.	<p>Verify if CINR drop is due to rain fading, mis-alignment or interference and if threshold was not set too close to the nominal operation values.</p> <ol style="list-style-type: none"> 1) Improve antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.

RSSI Out Of Range	RSSI dropped below configured RSSI threshold.	RSSI drop (below configured threshold) due to change in RF link conditions.	Verify if RSSI drop is due to rain fading, mis-alignment or interference and if threshold was not set too close to the nominal operation values. 1) Improve antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.
Lowest Modulation	System dropped to lowest modulation profile configured (in Adaptive Mode).	Modulation changed (down to lowest configured threshold) due to change in RF link conditions.	Verify if modulation change is due to rain fading, mis-alignment or interference. 1) Improve antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.

15.4 Performance 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.

Refer to the *Statistics* chapter of this manual for detailed description of the performance monitoring statistics.

15.5 Loopbacks

The EtherHaul radio uses Ethernet and RF loopbacks designed to enable fault isolation and Ethernet service performance testing.

- Ethernet Line Loopback – Internal and external loopbacks are performed on the interface, testing the local system, the radio link, and the remote system.
- RF (Radio) Loopback – Internal loopback is performed on the system’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.

Loopbacks can be applied with a timeout (up to 24 hours). When timeout expires, the loopback will be removed.

15.5.1 Loopbacks Diagram

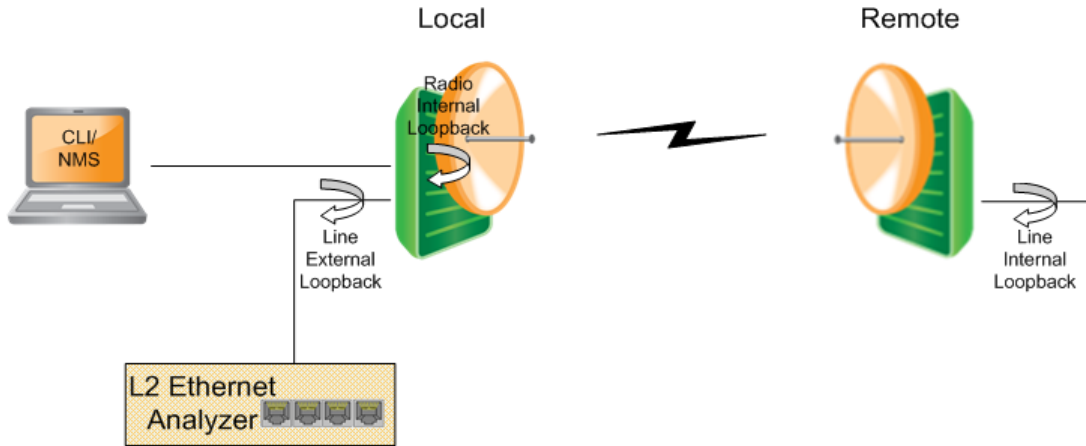


Figure 15-1 System Loopback Points

15.5.2 Ethernet Line Loopbacks

The loopback can be applied separately for each one of the interfaces (Eth1 to Eth4) and can be set with or without MAC Address swapping.

Set the loopback mode for the desired Ethernet port and set the loopback-timeout in seconds (up to 24 hours, 0= no timeout).

Ethernet loopbacks can be set in the **Maintenance** section of the **Eth Ports** page.

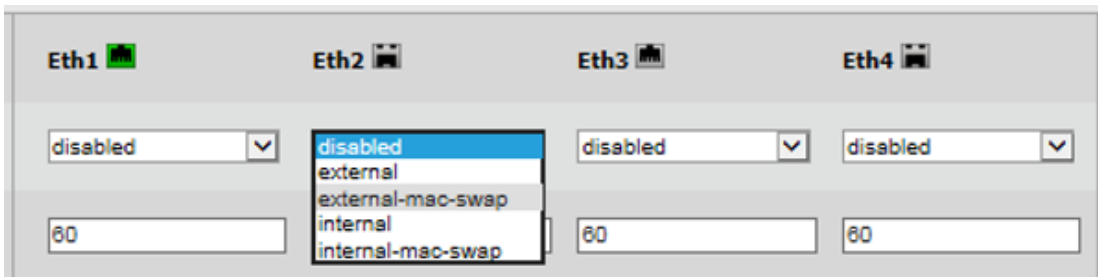


Figure 15-2 Ethernet Line Loopback

External Line Loopback

The Ethernet traffic from the customer’s end-equipment or Ethernet analyzer is looped on the Ethernet interface. It enables testing the connection (cable/fiber) and the interface between end-equipment and the local system.

When testing a link from one side (local), apply an external line loopback should be applied on the local unit.

Internal Line Loopback

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 system, enabling testing of the connection (cable/fiber), the interface between end-equipment and the local system, both local and remote systems and the radio transmission.

15.5.3 Radio (RF) Loopback

The Ethernet traffic from a customer’s end-equipment or Ethernet analyzer is looped on the system’s radio output, enabling testing of the connection (cable/fiber), the interface between the system and end-equipment and the local system.

The loopback is set with MAC Address swapping and on specific modulation profile set by the user.

For error-free operation at high modulation profiles, no interference should be present. Switch off or mute remote system before applying the RF loopback.

Note:



Alternatively, change remote frequency to eliminate risk of interference.

It will take the system to stabilize after loopback about 3 minutes before checking ODU performance using the alarms and statistics.

Enable the loopback and set the loopback-timeout in seconds (up to 24 hours, 0= no timeout, recommended minimum of 600 seconds).

RF loopback can be set in the **Maintenance** section of the **Radio** page.

RF Loopback	<input checked="" type="checkbox"/>	Timeout [sec]: <input type="text" value="600"/>	Modulation: <input type="text" value="QAM64 4 1 0.5"/>
Mute	<input type="checkbox"/>	Timeout [sec]: <input type="text" value="60"/>	

Figure 15-3 RF Loopback

15.5.4 Loopbacks CLI Commands

- Loopback timeout:

```
Line loopback timeout
set eth eth1 loopback-timeout 600

RF loopback timeout
set rf loopback-timeout 600
```

- Activating loopback:

```
Line internal loopback
```

```
set eth eth1 loopback-mode internal-mac-swap
```

Line external loopback

```
set eth eth1 loopback-mode external-mac-swap
```

RF loopback timeout

```
set rf loopback internal-mac-swap qam64 4 1 0.5
```

```
set eth eth1 loopback-mode external-mac-swap
```

Use the following command to clear the loopback:

```
set eth eth1 loopback-mode disable
```

- Clearing loopback:

Line loopback

```
set eth eth1 loopback-mode disabled
```

RF loopback timeout

```
set rf loopback disabled
```

16 Statistics

The EtherHaul uses advanced RF and Ethernet counters to provide real-time performance statistics for radio transmission activities, Ethernet ports, VLAN traffic and QoS queues.

The following statistics enable quick analysis of system and component performance in support of troubleshooting and diagnostics.

- RF statistics – displays 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
- VLAN statistics - displays statistic counters of each EtherHaul link component per VLAN
- Ethernet statistics - displays Ethernet statistics counters per Ethernet port
- Queues statistics – displays statistics per egress queue

This chapter describes the system's statistics.

The statistics are presented in the dedicated **Statistics** page.

Statistics can be exported to Excel by clicking the **Export to Excel** button next to the relevant table.

16.1 Radio (RF) Statistics Monitoring

16.1.1 RF Statistics Summary

Summary of radio statistics – 96 intervals of 15 minutes (last 24 hours), recording the minimum and maximum values per interval of RSSI, CINR and Modulation profile.

Start Time	Min RSSI	Max RSSI	Min CINR	Max CINR	Min Modulation	Max Modulation
2014.07.02 07:00:00	-43	-37	22	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 06:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 06:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 06:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 06:00:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 05:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 05:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 05:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 05:00:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 04:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 04:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 04:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 04:00:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 03:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 03:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 03:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 03:00:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 02:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 02:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 02:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 02:00:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 01:45:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 01:30:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.02 01:15:00	-40	-40	23	25	QAM64 4 1 0.5	QAM64 4 1 0.5

Figure 16-1 Statistics Page: RF Statistics Summary

RF Statistics Summary is cleared upon system reset.

16.1.2 RF Statistics Summary – 30 days

Summary of radio statistics – 30 intervals of 24 hours, recording the minimum and maximum values per interval of RSSI, CINR and Modulation profile.

Start Time	Min RSSI	Max RSSI	Min CINR	Max CINR	Min Modulation	Max Modulation
2014.07.20 00:00:01	-42	-38	22	24	QAM64 4 1 0.5	QAM64 4 1 0.5
2014.07.19 23:39:07	-128	-29	2	29	QPSK 1 4 0.5	QAM64 4 1 0.5

Export to Excel

Figure 16-2 Statistics Page: RF Statistics Summary – 30 days

RF Statistics Summary is cleared upon system reboot.

16.1.3 RF Statistics

Start Time	In Octets	Out Octets	In Idle Octets	Out Idle Octets	In Good Octets
2014.07.02 07:00:00	13914744921792	13914744932856	13880392263432	13880430190739	2964848465
2014.07.02 06:45:00	109151825116	109151820624	108882355139	108882633246	232569812
2014.07.02 06:30:00	109169986320	109169996920	108900470950	108900775055	232608591
2014.07.02 06:15:00	109134519924	109134509988	108865091526	108865375361	232533068
2014.07.02 06:00:00	109039643916	109039645640	108770450479	10877047162	232331115
2014.07.02 05:45:00	109263111264	109263113392	108993265811	108993662573	232806868
2014.07.02 05:30:00	109040401728	109040394960	108771206461	108771494736	232332421
2014.07.02 05:15:00	109206014112	109206014400	108936409672	108936704069	232684897
2014.07.02 05:00:00	109174962960	109174968580	108905436613	108905735309	232618248
2014.07.02 04:45:00	109078239600	109078236176	108808951181	108809241339	232412724
2014.07.02 04:30:00	109194121296	109194124072	108924546001	108924843843	232660130
2014.07.02 04:15:00	109118369808	109118369608	108848981444	108849276269	232498399
2014.07.02 04:00:00	109152664704	109152669724	108883192632	108883492923	232571197
2014.07.02 03:45:00	109152179280	109152174444	108882709906	108882997671	232568621
2014.07.02 03:30:00	109152187488	109152185276	108882719037	108883009787	232568514
2014.07.02 03:15:00	109158974352	109158974200	108889487847	108889782795	232583695
2014.07.02 03:00:00	109169609764	109169611168	108900094330	108900392289	232608253
2014.07.02 02:45:00	109041973532	109041983312	108772774019	108773080074	232335865
2014.07.02 02:30:00	109159584720	109159575840	108890094990	108890381969	232586629
2014.07.02 02:15:00	109190988308	109190988444	108921420670	108921715907	232635367
2014.07.02 02:00:00	109180198348	109180195036	108910656416	108910948556	232631006
2014.07.02 01:45:00	109166853024	109166852168	108897344570	108897639296	232602804
2014.07.02 01:30:00	109030185648	109030184564	108761013465	108761307828	232311808

Clear Statistics Export to Excel

Figure 16-3 Statistics Page: 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**. If incremented, these parameters indicate radio errors. No errors in these indicators indicate 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** indicate frame-loss over the radio that is noticed by the Ethernet service. The indication for link's quality and operation without frame-loss is indicated by no loss on these indicators.

Radio statistics counters – recording 96 intervals of 15 minutes (last 24 hours) of the following parameters:

Attribute	Description
Incoming Octets (in-octets)	The total number of octets received from the RF link.
Incoming Idle Octets (in-idle-octets)	The total number of octets received from the RF link while idle.
Incoming Good Octets (in-good-octets)	The number of good octets received from the RF link.
Incoming Erroneous Octets (in-errored-octets)	The number of received erred octets from the RF link.
Outgoing Octets (out-octets)	The total number of octets transmitted to the RF link.
Outgoing Idle Octets (out-idle-octets)	The total number of octets transmitted to the RF link while idle.
Incoming Packets (in-pkts)	The total number of packets received from the RF link.
Incoming Good Packets (in-good-pkts)	The total number of good packets received from the RF link.
Incoming Erroneous Packets (in-errored-pkts)	The total number of erred packets received from the RF link.
Incoming Lost Packets (in-lost-pkts)	The total number of packets that are considered lost by the receiver (from the RF link side).
Outgoing Packets (out-pkts)	The total number of packets transmitted to the RF link.
Minimum CINR value (min-cinr)	The minimal CINR value recorded in the interval.
Maximum CINR value (max-cinr)	The maximal CINR value recorded in the interval.
Minimum RSSI value (min-rssi)	The minimal RSSI value recorded in the interval.
Maximum RSSI value (max-rssi)	The maximal RSSI value recorded in the interval.
Minimum modulation value (min-modulation)	The lowest modulation profile recorded in the interval.
Maximum modulation value (max-modulation)	The highest modulation profile recorded in the interval.
Outgoing dropped packets (arq-out-loss)	The total number of packets dropped by the transmitter.

Attribute	Description
Incoming dropped packets (arq-in-loss)	The total number of packets dropped by the receiver.

16.2 Bandwidth Utilization Statistics

Presented per port: Eth0 (RF), Eth1 to Eth4 – 96 intervals of 15 minutes (last 24 hours).

The total **in-octets**, **out-octets**, **in-rate**, **out-rate** and **utilization** (aggregated, meaning Tx and Rx) are displayed.

For Eth0 (RF), bandwidth utilization is displayed as percentage of the aggregated (total Tx and Rx) max radio rate per the current modulation.

The rates displayed are averaged over the 15 minutes intervals.

Eth0

Start Time	In Octets	Out Octets	In Rate	Out Rate	Utilization
2014.07.02 07:00:00	31244378556	32775841614	2176937	2283676	0
2014.07.02 06:45:00	244830964	256844702	2176231	2283018	0
2014.07.02 06:30:00	244819137	256822797	2175628	2282301	0
2014.07.02 06:15:00	244856964	256862675	2176738	2283467	0
2014.07.02 06:00:00	244841059	256843714	2178492	2285287	0
2014.07.02 05:45:00	244960694	256970551	2175101	2281741	0
2014.07.02 05:30:00	244715421	256712404	2177357	2284101	0
2014.07.02 05:15:00	244857467	256862803	2175401	2282061	0
2014.07.02 05:00:00	244868100	256874243	2175952	2282641	0
2014.07.02 04:45:00	244749224	256748929	2176922	2283653	0
2014.07.02 04:30:00	245149780	257168577	2178136	2284922	0
2014.07.02 04:15:00	244564405	256554727	2174461	2281069	0

Eth1

Start Time	In Octets	Out Octets	In Rate	Out Rate	Utilization
2014.07.02 07:00:00	153292215	264027322	9193	32866	0
2014.07.02 06:45:00	834241	2409516	7415	21417	0
2014.07.02 06:30:00	821291	2104123	7298	18698	0
2014.07.02 06:15:00	705905	1678639	6275	14922	0
2014.07.02 06:00:00	701843	1945952	6244	17314	0
2014.07.02 05:45:00	745450	1969290	6619	17486	0

Figure 16-4 Statistics Page: Bandwidth Utilization Statistics

16.3 Ethernet Statistics

Figure 16-5 Statistics Page: Ethernet Statistics

Presented per port: Eth0 (RF interface of the bridge), Eth1 to Eth4 – 96 intervals of 15 minutes (last 24 hours).

Radio statistics counters – recording 96 intervals of 15 minutes (last 24 hours) recording the following parameters:

Attribute	Description
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.
Incoming Unicast Packets (in-ucast-pkts)	The number of unicast packets received on the interface.
Discarded Incoming Packets (in-discards)	The number of packets which were chosen to be discarded due to RX FIFO full.
Erroneous Incoming Packets (in-errors)	The number of received erred packets.
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.
Outgoing Unicast Packets (out-ucast-pkts)	The number of unicast packets transmitted out of the interface.
Discarded Outgoing Packets (out-discards)	The number of outbound packets which were chosen to be discarded due to excessive collision or excessive deferral.
Erroneous Outgoing Packets (out-errors)	The number of outbound packets that could not be transmitted because of errors.
Incoming Multicast Packets (in-mcast-pkts)	The number of multicast packets received on the interface.

Attribute	Description
Incoming Broadcast Packets (in-bcast-pkts)	The number of broadcast packets received on the interface.
Outgoing Multicast Packets (out-mcast-pkts)	The number of multicast packets transmitted out of the interface.
Outgoing Broadcast Packets (out-bcast-pkts)	The number of broadcast packets transmitted out of the interface.

16.4 VLAN Statistics

VLAN statistics counters (since last cleared) are presented per bridge component, per port and per VLAN ID, recording the **in-pkts**, **out-pkts** and **drop-pkts**.

Note that packets may be dropped due to traffic exceeding the radio link's maximum bandwidth.

The screenshot shows the 'Vlan Statistics' page with two data tables and control buttons. The left table shows statistics for components s1, c6, and undef across various ports and VLANs. The right table shows similar statistics for components s1 and c6. Both tables include columns for Time, Component, VLAN, Port, In-pkts, Out-pkts, and Drop-pkts. Below each table are buttons for 'Clear Statistics' and 'Export to Excel'.

Time	Component	VLAN	Port	In-pkts	Out-pkts	Drop-pkts
2014.06.30 02:59:45	s1	1	host	746024	705665	0
2014.06.30 02:59:45	s1	1	eth0	77160	75731	0
2014.06.30 02:59:45	s1	1	eth1	639096	684611	0
2014.06.30 02:59:45	s1	1	eth2	0	0	0
2014.06.30 02:59:45	s1	1	eth3	0	0	0
2014.06.30 02:59:45	s1	undef	host	0	0	0
2014.06.30 02:59:45	s1	undef	eth0	0	0	0
2014.06.30 02:59:45	s1	undef	eth1	0	0	0
2014.06.30 02:59:45	s1	undef	eth2	0	0	0
2014.06.30 02:59:45	s1	undef	eth3	0	0	0
2014.06.30 03:00:05	c6	1	eth4	0	0	0
2014.06.30 03:00:05	c6	undef	eth4	0	0	0

Time	Component	VLAN	Port	In-pkts	Out-pkts	Drop-pkts
2014.06.30 02:59:45	s1	1	host	746024	705665	0
2014.06.30 02:59:45	s1	1	eth0	77160	75731	0
2014.06.30 02:59:45	s1	1	eth1	639096	684611	0
2014.06.30 02:59:45	s1	1	eth2	0	0	0
2014.06.30 02:59:45	s1	1	eth3	0	0	0
2014.06.30 02:59:45	s1	undef	host	0	0	0
2014.06.30 02:59:45	s1	undef	eth0	0	0	0
2014.06.30 02:59:45	s1	undef	eth1	0	0	0
2014.06.30 02:59:45	s1	undef	eth2	0	0	0
2014.06.30 02:59:45	s1	undef	eth3	0	0	0
2014.06.30 03:00:05	c6	1	eth4	0	0	0
2014.06.30 03:00:05	c6	undef	eth4	0	0	0

Figure 16-6 Statistics Page: VLAN Statistics

16.5 Queues Statistics

Queue statistics for outgoing queues and incoming queues per port. Packets counters displayed since last cleared.

16.5.1 Out-Queue Statistics

The out-queue counters are available per port and per queue (one of the 8 queues per port available). The **Tx** counter indicates the number of transmitted packets and the **Drop** counter indicates the number of packets dropped.

Out-Queue Statistics

Time	Interface	Queue	Tx	Drop
2014.06.30 02:59:45	rf	0	71896	0
2014.06.30 02:59:45	rf	1	0	0
2014.06.30 02:59:45	rf	2	0	0
2014.06.30 02:59:45	rf	3	3862	0
2014.06.30 02:59:45	eth0	0	71896	0
2014.06.30 02:59:45	eth0	1	0	0
2014.06.30 02:59:45	eth0	2	0	0
2014.06.30 02:59:45	eth0	3	0	0
2014.06.30 02:59:45	eth0	4	0	0
2014.06.30 02:59:45	eth0	5	0	0
2014.06.30 02:59:45	eth0	6	0	0
2014.06.30 02:59:45	eth0	7	3862	0
2014.06.30 02:59:45	eth1	0	681645	4
2014.06.30 02:59:45	eth1	1	0	0
2014.06.30 02:59:45	eth1	2	0	0
2014.06.30 02:59:45	eth1	3	0	0
2014.06.30 02:59:45	eth1	4	0	0
2014.06.30 02:59:45	eth1	5	0	0
2014.06.30 02:59:45	eth1	6	0	0
2014.06.30 02:59:45	eth1	7	3421	0
2014.06.30 02:59:45	eth2	0	0	0
2014.06.30 02:59:45	eth2	1	0	0
2014.06.30 02:59:45	eth2	2	0	0
2014.06.30 02:59:45	eth2	3	0	0

Clear Statistics Export to Excel

Figure 16-7 Statistics Page: Out-Queue Statistics

The 4 rf queues are not relevant (internal mapping of queues).

16.5.2 In-Queue Statistics

The 4 rf in-queues are for the internal mapping of queues.

The **Good** counter indicates the number of good packets received, the **Error** counter indicates the number of errored packets received and the **Lost** counter indicates the number of packets lost.

In-Queue Statistics

Time	Interface	Queue	Good	Error	Lost
2014.06.30 02:59:45	rf	0	73366	0	0
2014.06.30 02:59:45	rf	1	0	0	0
2014.06.30 02:59:45	rf	2	0	0	0
2014.06.30 02:59:45	rf	3	3852	0	0

Clear Statistics Export to Excel

Figure 16-8 Statistics Page: In-Queue Statistics

16.6 CLI Commands

- RF Statistics Summary (last 24 hours):

```
Viewing summary (since last system reboot):
show rf statistics-summary
```

- RF Statistics Summary (last 30 days):

```
Viewing summary (since last system reboot):
show rf statistics-summary-days
```

- RF Statistics:

```
Viewing summary (since last cleared):  
show rf statistics  
  
Viewing last 24 hours (96 intervals of 15 minutes):  
show rf statistics 0 95  
  
Viewing last 30 days (30 intervals of 24 hours):  
show rf statistics-days 0 30  
  
Clearing statistics:  
clear rf statistics
```

- Bandwidth Utilization Statistics:

```
Viewing radio summary (since last system reboot):  
show eth eth0 statistics-summary  
  
Viewing port summary (since last system reboot):  
show eth eth1 statistics-summary
```

- Ethernet Port Statistics:

```
Viewing statistics (since last cleared):  
show eth eth1 statistics  
  
Clearing statistics:  
clear eth all statistics
```

- VLAN Statistics:

```
Viewing statistics (since last cleared):  
show vlan all all statistics  
  
Clearing statistics:  
clear vlan all all statistics
```

- Queues Statistics:

```
Viewing out-queue statistics (since last cleared):  
show out-queue all all statistics  
  
Viewing in-queue statistics (since last cleared):  
show in-queue all all statistics  
  
Clearing statistics:  
clear out-queue all all statistics  
clear in-queue all all statistics
```