EtherHaul™ System Description

August 2018

Release: 3.0

Table of Contents

Document Information

Revision	Date	Author	Revision notes
3.0	12 August 2018	SH	Updated with Features and Functions of System SW R7.6
2.0	6 March 2018	SH	Updated with Features and Functions of System SW R7.5
1.1	15 September 2016	SH	Initial Release, aligned with System SW R7.2.0

Intended Audience

- Solution architects and network planning staff
- Telecom backhaul engineers
- Wireless ISP, business connectivity and wireless networks pre-sale engineers

Terminology used in this document assumes audience familiarity with millimeter wave radio communication and networking technologies.

Comments and suggestions are welcome to: info@siklu.com.

1. Introduction

This document describes the generic features of the EtherHaul™ system software and hardware, which are common to all EtherHaul™ products. It complements the product specific information contained in the Production Description document relevant to a particular EtherHaul™ model. The feature description assumes that the EtherHaul™ units are running Siklu system software R7.6.

2. EtherHaul™ Family Generic Specifications

2.1 Integrated Ethernet switch

EtherHaul™ ODUs include an integrated 3 or 4 ports (model dependent) Gigabit Ethernet switch. Some ports are hard-wired 100/1000-BaseT, while others are an SFP MSA compliant cage (model dependent), for communications over multi-mode (MMF) or single-mode optical fiber (SMF) and longer distances.

Each port can be configured to support:

- Auto negotiation enabled/disabled
- Speeds: 100/1000 Mbps.
- Full-duplex / half-duplex
- Delivery of both payload traffic and/or management traffic
- OAM signaling
- SyncE

2.1.1 Benefits

- 2, 3 or 4 Ethernet ports are an ideal number of interfaces at a hub or daisy-chain site, as well as at a drop site delivering multiple services to several devices such as hot-spot, small-cell or surveillance cameras. This enables:
    - Advanced network topologies: ring, mesh and daisy chain
    - Connectivity for more services at each location, avoiding the need for external devices for services grooming/cascading, and thus reducing both CAPEX and OPEX.

2.2 Adaptive modulation

EtherHaul™ implements hitless/errorless adaptive bandwidth, coding and modulation adjustment to optimize the over-the-air transmission and prevent weather-related fading traffic disruption. The EtherHaul™ products can gain up to 25dB (model dependent) in link budget by dynamically adapting the rate:

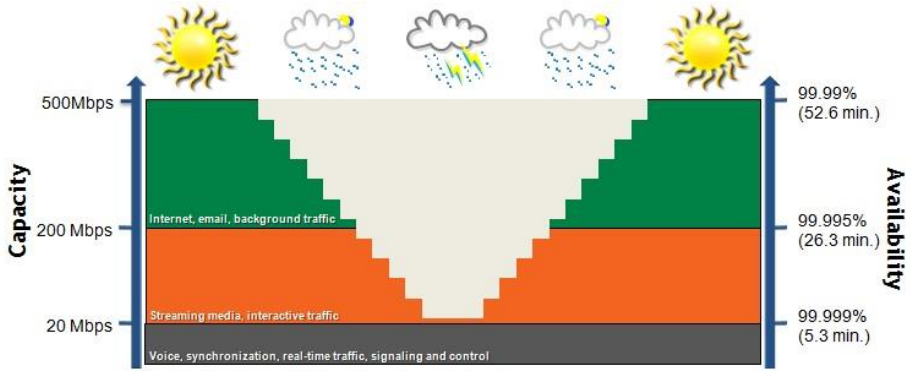


Figure 1 – Hitless Adaptive Bandwidth, Coding and Modulation

2.2.1 Benefits

- Adaptive bandwidth, coding, and modulation ensure maximum capacity most of the time with guaranteed high priority services all the time.
- EtherHaul™ hitless algorithm achieves zero down time to enable reliable voice and real-time services, allowing carriers to meet their service level agreements for enhanced user experience.

2.3 Alignment

As any other P2P millimeter wave system, the EtherHaul™ link must be precisely aligned during the installation process.

A standard voltmeter is used for RSSI reading via the (AUX) port, or one of the Ethernet ports and a special adapter (model dependent).

2.3.1 Benefits

- Simple and reliable antenna alignment process (no computer connection needed)
- Alignment is performed using standard single T-bar tool that matches all screws, worm clamps adjustments and locks.

3. EtherHaul™ Family Networking Features

4. Switching

4.1.1 QoS-Aware Transparent Bridge (IEEE 802.1d)

The out-of-the-box configuration of EtherHaul™ is the advanced transparent bridge mode (IEEE 802.1d), a zero-touch judicious match for simple networks. Quality-of-Service-awareness operation is automatic in this mode. Transparent forwarding of both tagged and untagged traffic is performed. It is possible to allocate a dedicated VLAN for in-band management.

4.1.2 Provider Bridge (IEEE 802.1ad)

Alternatively, the EtherHaul™ incorporates a full Provider Bridge mode of operation (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.

This enables servicing multiple customers on the same port (User Network Interface, UNI) and forwarding (or tunneling) through the radio link which acts as NNI – network network interface using Service VLAN (S-VLAN). The system is able to deliver multiple S-VLANs, and to manage several customers' VLANs (C-VLAN) in each S-VLAN. Sample VLAN encapsulations are illustrated in Figure 2.

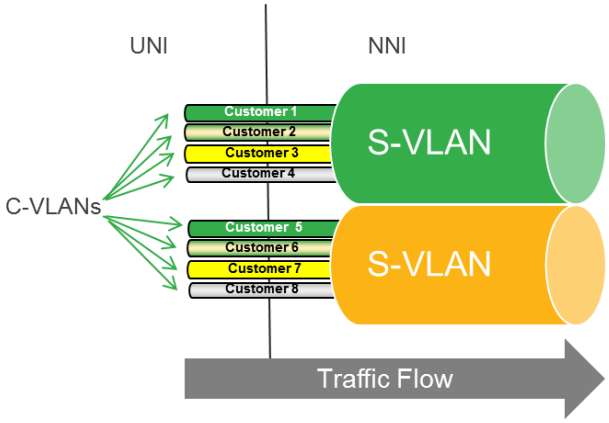


Figure 2: C-VLANs encapsulated in S-VLANs

The provider bridge, which may consist of multiple devices in the service provider domain, looks like a simple bridge port to the customer's traffic and maintains the Customer's VLANs (C-VLAN) with their ID number.

The implementation of Provider Bridge in EtherHaul™ is a network of up to five virtual bridges connected in a "cross-like" fashion as shown in Figure 3.

- 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.
- The operator can change the default bridge configuration to suit his network by removing or adding the desired bridge components.
- All components are created, managed, and removed using either CLI or WEB GUI.

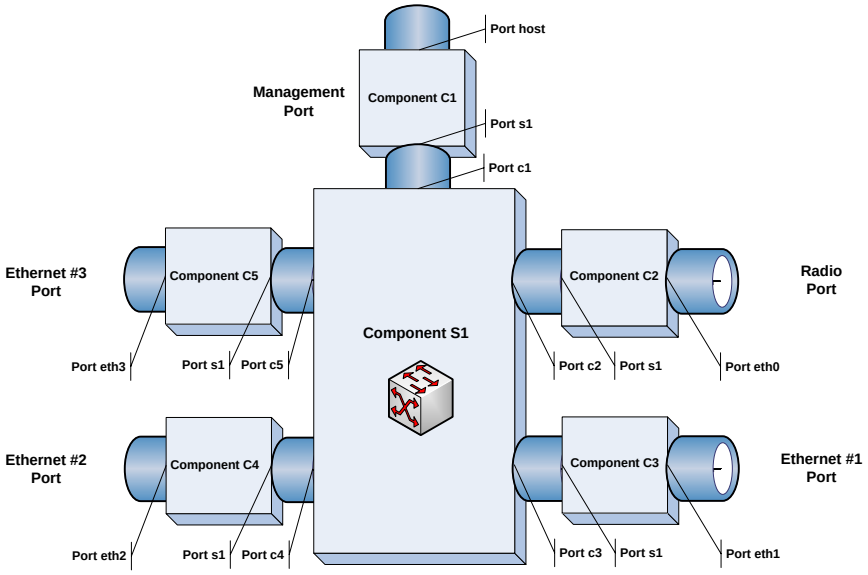


Figure 3: Provider Bridge Architecture*

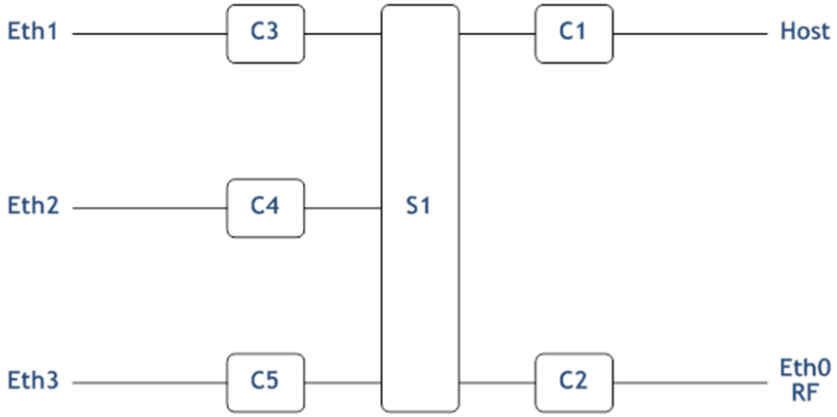


Figure 4– Generic Model of the EtherHaul™ Bridge

Each component acts as a virtual bridge. A component can have both external and internal ports. An external port name is identical to its interface name. An internal port name uses the name of its peer C-component 1 is connected to the S-component, the corresponding internal port in.

For example, the C-component is called S1 and the corresponding internal port in the S-component is called C1.

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

4.1.3 Standards compliance

- IEEE 802.1d - MAC Bridges
- IEEE 802.1Q - Virtual LANs (VLANs)
- IEEE 802.1ad – QinQ
- Metro Ethernet Forum (MEF) recommendations and defined services: MEF 9, Ethernet Services Functionality:
    - E-LINE, E-LAN and E-TREE services

- E-LINE with multiple user defined options:
  - Port based
  - Port with single VLAN
  - Port with double VLAN (QinQ)
- E-LAN with multiple user defined options:
  - MAC
  - VLAN
  - Double VLAN (QinQ)
- Multiple isolated E-LAN services – by multiple isolated MAC tables
- E-Tree with multiple user defined options:
  - Port based
  - Port with single VLAN
  - Port with double VLAN (QinQ)

- UNI attributes, Service frame delivery, VLAN tag support

4.1.4 Benefits

- Flexible networking topologies support
- Carrier class services, following leading standards with proven interoperability
- Integrated Gigabit Ethernet switch and advanced networking features allows all outdoor installation
- EtherHaul™ provider bridge is an easy and fast deployment enabler:
  - It takes any Ethernet based stream, wraps it with service provider tag
  - Enhanced QOS marking based routing of ingress traffic into multiple differentiated queues.
  - No limits on frame size (the EtherHaul™ systems supports 9K jumbo frames)

5. Quality of service (QOS)

There are 2 main motives to leverage QOS in a street-level wireless backhaul system:

1. QOS complements hitless adaptive bandwidth, coding, and modulation mechanisms with real time prioritization of several services. It allows ensuring performance and availability correlated with provider's SLA (service level agreement).
2. Enforcing QOS enables carriers to oversubscribe wireless links will supporting the SLA agreement of each individual service, and thus leads to enhanced ROI.

EtherHaul™ ODUs are equipped with a powerful network processor and Siklu's proven EtherHaul™ advanced software package, enabling any service provider to offer best in class differentiated services. With 8 queues, the EtherHaul™ have QoS granularity for the most demanding environment.

5.1 Classification and Policing

The EtherHaul™ QoS engine classifies the incoming packets onto streams using any combination of:

1. VLAN number (VID) – prioritizes frames based on their VLAN ID.
2. PCP - 3 priority bits that enables up to 8 differentiated QOS classed of service. PCP bits are part of the L2 VLAN header.
3. DSCP – 6 bits, part of the DS field in L3 IP header of incoming packets. The user configurable QOS scheme of EH-2500F enables allocating each of the potential 64 traffic classes, into the 8 queues of the system. EH-2500F support DSCP classification according to IPv4 and IPv6 L3 packets.
4. MPLS Traffic Class (TC, formerly EXP) - 3 priority bits that enables up to 8 differentiated classes of service. The 3 TC bits are part of the MPLS label.

EtherHaul™ supports 4 types of bandwidth profile with CIR (committed information rate), CBS (committed burst size), EIR (excess information rate), EBS (excess burst size), which can be assigned to each of the above listed (1-4) differentiated streams.

The implemented mechanism supports 3 colors and 2 rates:

- Frames that fit into CIR/CBS profile marked drop ineligible and colored “green”.
- Frames which are within excess profile but exceed committed profile are marked drop eligible (“yellow”), upon congestion at egress interface the yellow packets are dropped first.
- All remaining frames, which are out of profile, are colored “red” and discarded.
    - The “red” frames are dropped; “green” frames take precedence over “yellow” ones.

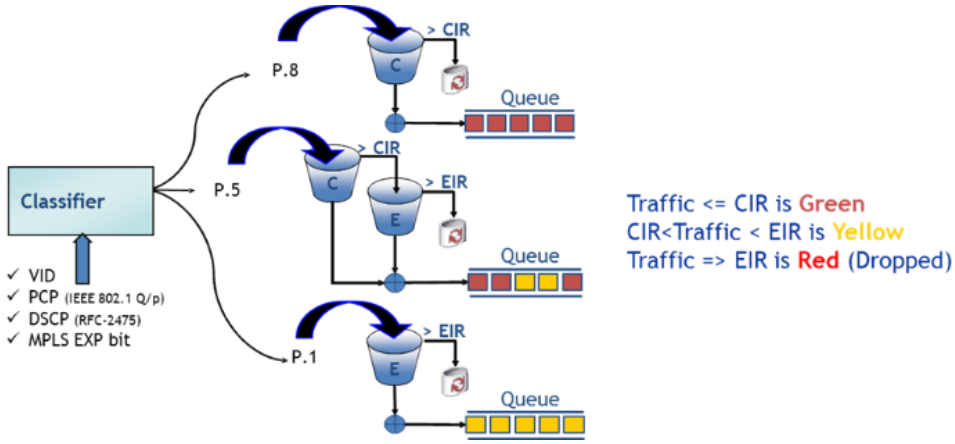


Figure 5 – EtherHaul™ Classifications and Policing

These packets are then mapped to 1 of the 8 priority queues (per interface). Each queue may be assigned buffering space (queue depth) manually or automatically by the SW that calculates the adaptive modulation BW changes. These queues are accessed by the scheduling mechanism.

5.2 Prioritization of Control Protocols

Control protocols such as OSPF, LACP, STP, LLDP, IEEE 1588 and CFM/OAM can be easily prioritized by the ODU, per the needs of the service provider.

5.3 Buffer size

Packets processed in the switch are held in buffers. If the destination queue is congested, the switch holds on to the packet as it waits for capacity to become available on the loaded queue. The ratio between delay and number of dropped frames is a result of the buffer size configuration.

5.4 Scheduling Mechanisms

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

- Strict Priority (SP): Advanced mechanism for assuring both prioritization and minimal delay for mission critical traffic. Higher priority traffic is fully served through its differentiated queues, only if all high priority traffic, identified as SP, is fully served the lower priority traffic is delivered to its queues.
- Weighted Fair Queuing (WFQ): A 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. This queueing mechanism is suitable for high capacity statistical applications and it ensures pre-defined serving of multiple services even when the link is fully loaded.
- 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. Shaper capabilities of internet serving access devices, is crucial for assuring effective and stable delivery of TCP oriented traffic with minimizing re-transmissions and maximizing utilization of the available capacity.
- Best Effort: used for the lowest priority traffic types and simply enable further utilization of statistical multiplexing. Capacity is not guaranteed for this queue, and it enables dynamic utilization of all non-used (by higher queues) available capacity.

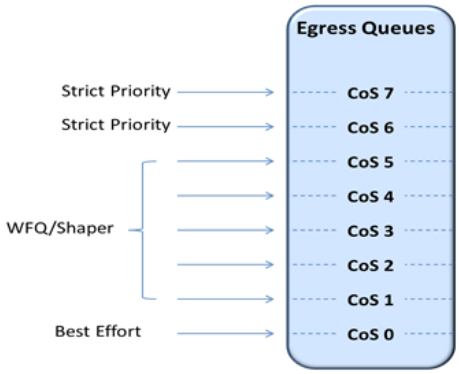


Figure 6 –Scheduling Mechanism

5.4.1 Standard compliance

- IEEE 802.1Q / IEE802.1P - 3 bits identified as priority code point (PCP).
- RFC-2475 - Architecture for differentiated services.
- RFC-5865 - A differentiated services code point (DSCP) for capacity-admitted traffic
- Related Metro Ethernet Forum (MEF) recommendations:
    - MEF 14, Ethernet Service Performance
        - Service performance, bandwidth profiles, BW profile rate enforcement.

5.4.2 Benefits

- Quality of Service (QoS) mechanism enables service providers to offer different classes of service for different types of traffic or customers.
- QoS mechanism 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 user defined, wide range of buffer size values, enable fine adjustments for various implementation scenarios, and thus contribute to operators' network capability to optimize traffic flows at heavy load conditions.
- The statistical behavior of today data services enables service providers to oversubscribe their networks while differentiating services based on QoS driven SLA, and thus leads to faster ROI and improved utilization of the network.

6. Queue management - WRED

WRED function (Weighted random early detection) adds queue management mechanism to EtherHaul™. Weighted Random Early Detection (WRED) is a queue management algorithm with congestion avoidance capabilities. 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.

WRED enables the EtherHaul™ ODUs to detect the onset of congestion and takes corrective action. EtherHaul™ have several different queue thresholds. Each queue threshold is associated to a particular traffic class.

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.

6.1.1 WRED Benefits

- WRED assures that the queue does not fill up, so that there will be most of the time room for high-priority packets within the same queue.
- Random drops cause TCP sessions to reduce window sizes and thus extends efficiency.
- Average capacity usage is much closer to actual capacity of the link.

7. Configurable Ethertype

IEEE 802.1ad Provider Bridging (a.k.a Q-in-Q) defines the Ethertype as 0x88A8 and lists additional Ethertype field values for S-VLAN: 0x8100, 0x9100 and 0x9200 to support backwards compatibility.

7.1.1 Benefits

The configurable Ethertype feature eliminates Ethertype compatibility issues when connecting EtherHaul™ ports/services to 3rd party switches and routers or other network devices such as access points, small-cells etc. It is another tool for easy integration of EtherHaul™ into any network.

8. LLDP

The Link Layer Discovery Protocol (LLDP) is a unidirectional neighbor discovery protocol.

LLDP performs periodic transmissions of an ODU's capabilities to the adjacent 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 or network element using CLI and/or system's web based GUI, 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. The user can use this information, especially the 'retrieved management IP addresses' option, in order to access these discovered nodes.

LLDP enables EtherHaul™ to discover other network elements that are connected to it as well as being discovered. This feature enables, amongst other things, to discovery third-party network elements connected to the EtherHaul™ so that they can be managed. In addition, it enables easier integration of EtherHaul™ links in a LLDP supported network.

8.1.1 Standard compliance

- IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)

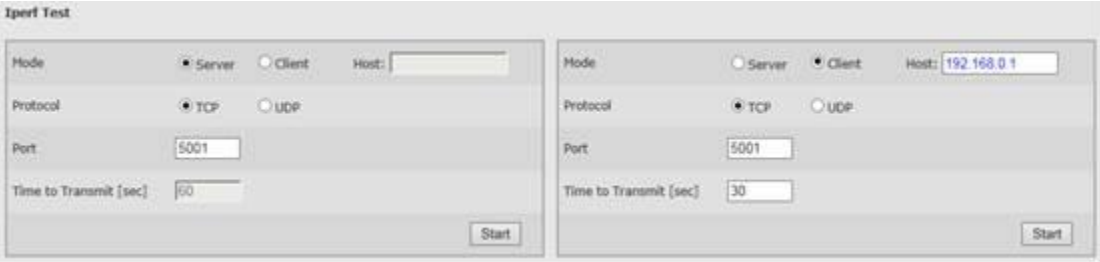
8.1.2 Benefits

- Enhances troubleshooting process
- Standard based topology discovery by 3rd party network monitoring and management systems

9. Iperf

The built-in Iperf tester implementation includes client/server nodes for over the air TCP/UDP test. Configure one side as Server and run it (click Start) and remote end as Client (and enter the server IP address).

Iperf test run in parallel to traffic over the link.



9.1.1 Benefits

Running Iperf helps the installer to make sure the link is installed properly without the need for external tools. More importantly, Iperf onboard support troubleshooting network and packet losses issues to identify connectivity problems much faster, without the need for on-site visits.

10. Port Mirroring

The Port Mirroring function allows duplicating of all the traffic on a source Ethernet port to a target Ethernet port on the same ODU. Any Ethernet port can be source or destination. Mirroring can be configured to ingress, egress or both directions.

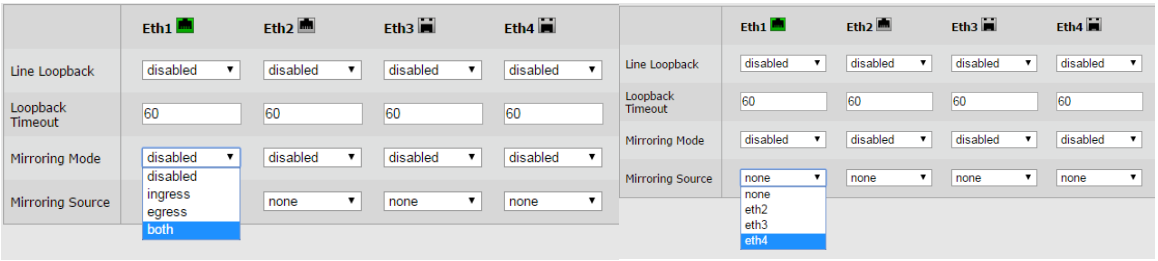


Figure 7: Port Mirroring Configuration

Note: the target port may not be able to mirror all traffic when the source port handles high-throughput in both directions, which combined may exceed the line rate on the target port.

10.1.1 Benefits

Port mirroring is a convenient tool for monitoring traffic across the network.

11. DHCP

The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network. DHCP is built on a client-server model, where designated DHCP server allocates network addresses and delivers configuration parameters to dynamically configured hosts. "Client" refers to a host requesting initialization parameters from a DHCP server.

The EtherHaul™ management Interface can be configured as a DHCP client.

11.1.1 Standard compliance

- RFC 2131 - Dynamic Host Configuration Protocol

11.1.2 Benefits

- This protocol reduces system administration workload, allowing networks to add devices with little or no manual intervention.
- Easy and fast discovery of new EtherHaul™ elements added to any DHCP enabled network

12. Link OAM

Link OAM, as defined in IEEE802.3ah, is an Ethernet layer operation, administration, and management (OAM) protocol designed to ease monitoring and troubleshooting of networks. Link OAM enables to detect, verify, and isolate connectivity failures in point-to-point connections. Link OAM is intended for single point-to-point links, usually used at network edges, between network-termination (NT) device

located at customer premises and the directly connected to it, service provider's located access/aggregation network element.

The following IEEE802.3ah functionality is supported by EtherHaul™:

- Discovery:
    1. Detect remote element
    2. Exchange link state and configuration information:
    3. Enable OAM on link
- Remote Loopback
    - Initiated by a loopback control OAMPDU
    - The loopback command is acknowledged by responding with an Information OAMPDU with the loopback state indicated in the state field.
    - The periodic exchange of OAMPDUs must continue while in the loopback state to maintain the OAM session.

12.1.1 Standard compliance

- IEEE802.3ah: EFM - Ethernet in the first mile

12.1.2 Benefits

- Standardized mechanism to monitor the health of a link and perform diagnostics
- Remote loopback enables standard based test equipment, to be connected at a central location in the network and perform service performance tests all the way to the network edge were the EtherHaul™ unit is usually located.
- Reduces the probability for truck-rolls

13. Connectivity Fault Management (CFM)

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 enable easier commissioning and troubleshooting at 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.

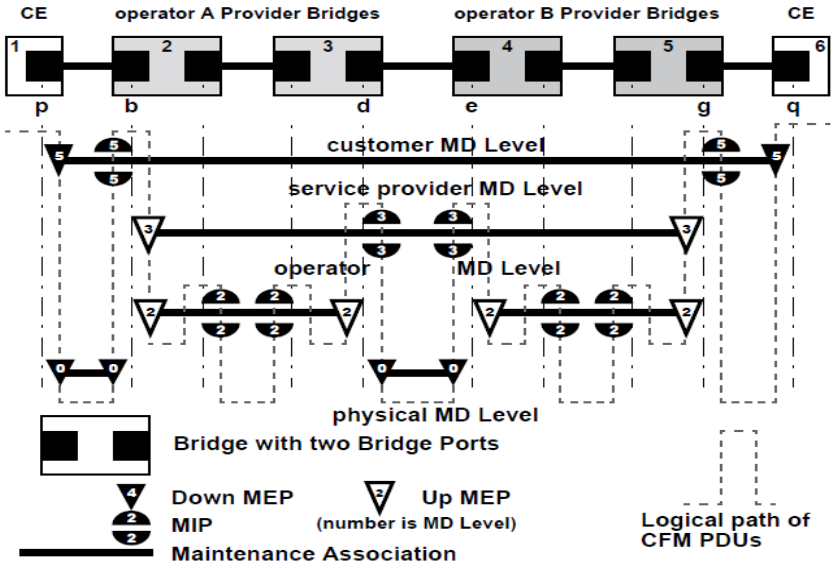
The major features of CFM are fault detection, path discovery, fault verification, fault isolation, and fault recovery.

The system allows to:

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

The system supports the following monitoring tools:

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



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

Figure 8 – Typical CFM network

CFM allows the operator or service provider perform the following actions:

- Fault detection
- Path discovery
- Fault verification
- Fault isolation
- Fault recovery

13.1.1 Standard compliance

- IEEE 802.1ag: CFM - Connectivity Fault Management

13.1.2 Benefits

- End-end Monitoring of services
- Detection of faults before they are noticed or reported by the user
- Faster faults location isolation
- Enhances SLA assurance
- When used to monitor services across multi-networks, enables hiding internal topologies and network elements.
- Running in parallel to service traffic, in same paths, with no interfering the user traffic.

13.2 Performance monitoring OAM

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

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

13.2.1 Standard compliance

- ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
- EtherHaul™ OAM functionality also complies with MEF 21, UNI Type 2 – Link OAM:
- OAM Discovery process.
- OAM PDU tests.
- OAM TLV tests

13.2.2 Benefits

- Allows operators or service providers to monitor network performance and commit to SLA to the customer.
- Useful both for in-service monitoring and during faults troubleshooting.

14. Smart Pipes Mode

The Smart Pipe mode allows bypassing MAC learning function of the Ethernet switch in the ODU, and tunneling of all traffic on 1 Ethernet port to a designated port on the other ODU in the link. More than 1 port can be set in Smart Pipe mode in each ODU.

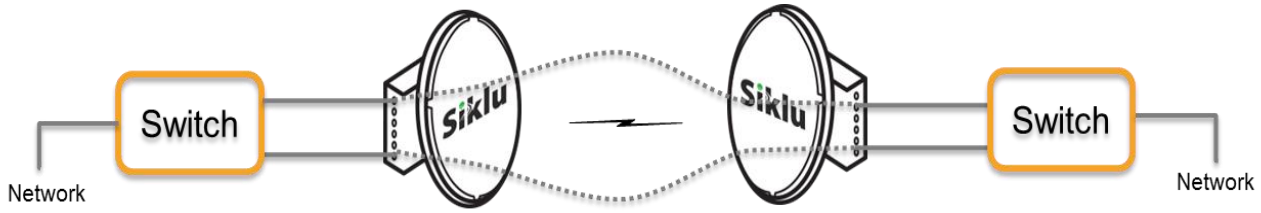


Figure 9: Smart Pipe mode

14.1.1 Benefits

- High-throughput between 2 Ethernet end-point by combination of multiple lower speed links.
- Allowance for non-standard implementations of link aggregation, when the 2 Ethernet switches connected to the ODU support the same proprietary implementation.

15. LAG

Link Aggregation is an IEEE standard which serves multiple purposes: protection of the traffic between 2 end-points by mean of multiple links, and delivery of high-throughput between 2 devices by aggregation of multiple low speed links.

The protection is provided at the facility layer, the physical transport between the 2 end-points, and at the port layer. Multiple links load-share the traffic between the 2 end-points. When a facility or a port is not available, the whole link is taken out of service and the traffic carried on this link is redistributed across the other links between the 2 end-points.

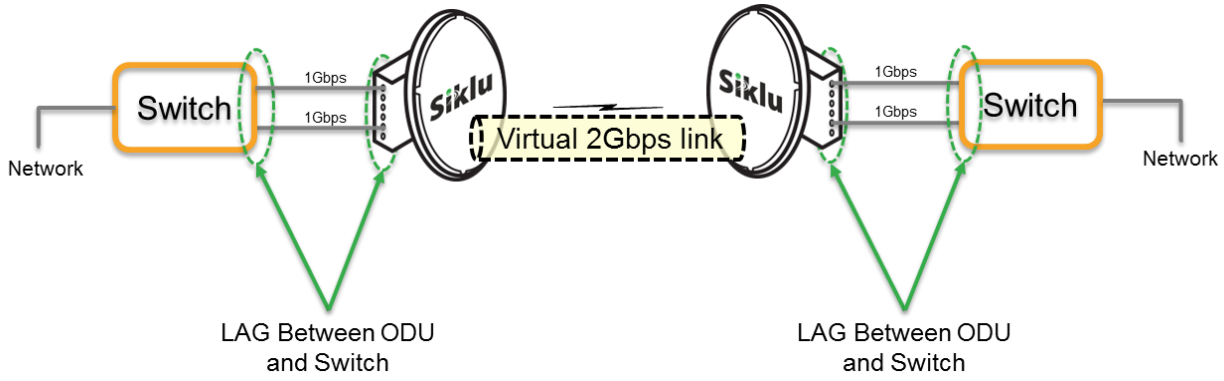


Figure 10: LAG between EtherHaul™ and Ethernet switch

The higher-throughput is achieved also by aggregation: several low speed links are combined to a higher throughput, example 4x links of 1Gbps each can deliver a total of 4Gbps between the 2 endpoint. It should be noted that due to the rules in LAG, a single service may not exceed the throughput of a single link; following the same example above, a file transfer session between the 2 end-points would still run at 1Gbps.

EtherHaul™ supports the following options with LAG:

- LACP:
  - Disable: no LACP
  - Passive: ports send LACP packets only after receiving LACP packets from the partner port
  - Active: the ports send LACP packets (LACPDUs) at regular intervals to the partner ports
- Hashing algorithm for dividing the packets between the ports:
  - L2: based on source and destination MAC addresses (SA and DA)
  - L2-L3: based on SA and DA + source and destination IP address
  - L2-L3-L4: based on SA and DA + IP address + Port

15.1.1 Standard compliance

- IEEE 802.1ax 2008 Link Aggregation

15.1.2 Benefits

- Port and Facility protection between 2 Ethernet end-points.
- High-throughput between 2 Ethernet end-point by combination of multiple lower speed links.

16. Ethernet Ring Protection (Resiliency)

Ethernet Ring Protection (ERP) is a network resiliency protocol defined by the ITU-T G.8032 recommendation. ERP functionality enables ultra-fast protection for any point of failure in a ring-topology network. This means that network connectivity is maintained in the event that the Ethernet link, the radio link, or even an entire EtherHaul™ link fails in the ring. This provides resiliency for both Ethernet-physical 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.

EtherHaul™ supports ITU-T G.8032v2, with backwards compatibility to previous versions. Using ERP, EtherHaul™ provides protection and recovery switching within 50 ms for typical rings. The ERP mechanism occupies extremely low portion from the available bandwidth.

Figure 11 illustrates the basic ERP protection mechanism. In normal ring operation, the RPL is blocked, between nodes C and D. In a failure condition, the failed link, between A & F, is blocked and R-APS messages are sent from the nodes adjacent to the failed links in order to unblock the RPL. An FDB flush is performed on all ring nodes as necessary.

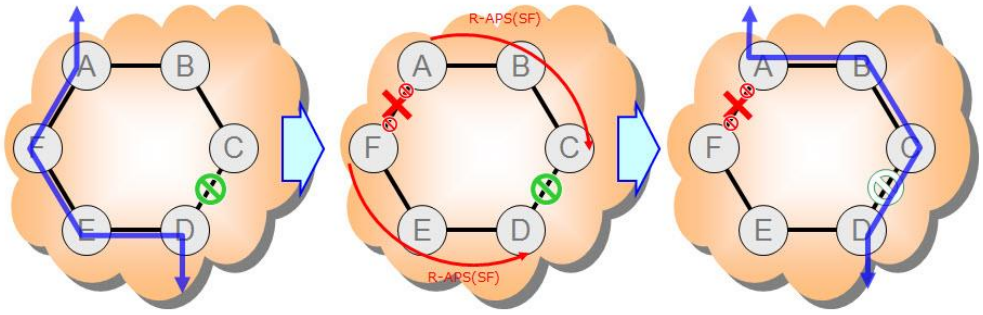


Figure 11 - Basic ERP Protection Mechanism

Among the ERP features supported by 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

16.1.1 Standard compliance

- ITU-T G.8032v2 Ethernet Ring Protection Switching

16.1.2 Benefits

- Non-proprietary protection resiliency standard that allows mixed-vendor deployments
- Carrier-class reliability, with sub-50ms performance
- Can be deployed in both all wireless backhaul environment as well as in mixed wireless / optical
- Overcomes old spanning-tree protocols issues while adding the faster restoration performance

17. Ethernet Synchronization

17.1.1 Synchronous Ethernet (ITU-T G.8261)

EtherHaul™ supports Synchronous Ethernet (SyncE). EtherHaul™ supports Synchronized Ethernet link input from the network side through one of the physical ports or from the radio side and providing a synchronized Ethernet link over the air to the other end of the wireless link within the required masks.

SyncE is a link-by-link timing distribution scheme that uses the Ethernet physical layer to accurately distribute clock frequency. The ITU-T G.8261 recommendation 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.

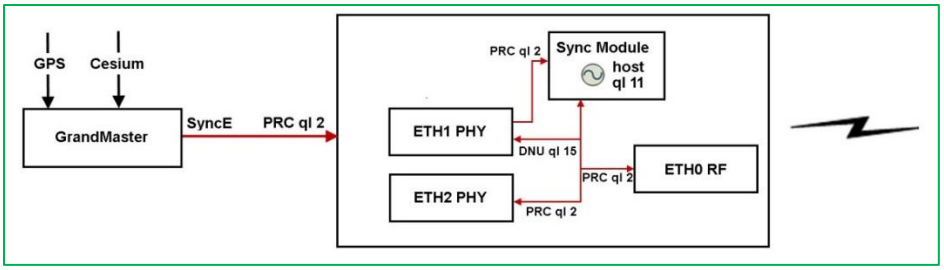


Figure 12 - EtherHaul™ ODU SyncE Functional Diagram

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 EtherHaul™ products to determine which clock source to use, based on performance and the need to avoid loops. Quality Level is based on the clock's holdover performance.

17.1.1.1 Standard compliance

ITU-T G.8261 defines various aspects of Synchronous Ethernet such as the acceptable limits of jitter and wander for packet networks as well as the minimum requirements for the synchronization function of network elements.

ITU-T G.8262, Timing characteristics of Synchronous Equipment Slave Clock (EEC), defining the SyncE clock specs

ITU-T G.8264, Distribution of timing status information through packet networks, defining the Ethernet Synchronization Messaging Channel (ESMC) protocol.

17.1.1.2 Benefits

SyncE allows operators and service providers a faster and reliable migration from legacy SDH/PDH/SONET networks to packet switched networks and thus significantly reduce OPEX.

Together with support of IEEE 1588, EtherHaul™ provide carrier class timing to remote sites and cell-sites, avoiding the need to deploy cumbersome GPS-based timing.

17.1.2 IEEE 1588 Transparent Clock

Siklu's EtherHaul™ supports IEEE 1588v2 Transparent Clock (TC). The EtherHaul™ products comply with the mobile backhaul specifications for packet synchronization distribution.

1588v2 Transparent Clocks (TCs) used to overcome the 1588 synchronization performance issue due to packet delay variation over the network. In a wireless links, the compensation of the PDV needs to be done for the entire link including the air interface, and not only per node. Time stamping and the correction field update are HW based in EtherHaul™ ODUs.

17.1.2.1 Standard compliance

- IEEE 1588v2 - Precision Time Protocol (PTP)

17.1.2.2 Benefits

- Allows accurate "Wall time" synchronization in the packet switched network.
- Enables stamping updates

17.1.3 1588 optimization

The EtherHaul™ products provide optimized transport of the IEEE 1588v2 packets allowing the slave to regenerate the clock within the required masks.

The IEEE standard 1588-2008, also known as 1588v2, defines a packet-based, timestamp distribution between a master clock and a slave, whereby the timing information originates from a Grandmaster clock function that is usually traceable to a Primary Reference Clock (PRC) or Coordinated Universal Time (UTC).

17.1.3.1 Standard compliance

- IEEE 1588v2

17.1.3.2 Benefits

Allow accurate "Wall time" synchronization in the packet switched network.

18. EtherHaul™ Family Management Concepts

EtherHaul™ is capable of delivering services out of the box, without any user configuration input. In this mode, the system acts as a fully transparent bridge, which matches many network configuration and it is intended for fast and easy service activation process.

For managed operations, EtherHaul™ includes all fundamentals that enable easy configuration, monitoring, and troubleshooting, by variety of all leading Telco-grade systems, as well as direct local and remote management directly from operator's desktop.
The supported management options are:

CLI	Professional Command Line Interface for full configuration and maintenance activities, with multiple privileges levels as required by service providers.
WEB GUI	Easy to interact user-interface via standard web-browser to manage both ends of the link, from one graphical screen.
RADIUS and TACACS+	RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) are advanced authentication and report standards for large scale networks.
SNMP	Both versions 2 and 3 of the Simple Network Management Protocol are supported for north-bound connectivity to central configuration and monitoring systems.
FTP SFTP TFTP	FTP, TFTP and SFTP protocols designed to provide file transfer and other manipulations. EtherHaul™ uses SFTP/FTP/TFTP for software upgrades, configuration uploads and downloads
SikluView	EMS – Elements Management System. Siklu solution for high level centralized administration and monitoring of EtherHaul™ elements and links

19. CLI

All EH-2500F's functionality is accessible via secured command line interface (SSH).
The user type defines the user's access privileges.

User	Read-only access, but cannot view user names, passwords, and other security settings.
Tech	Basic technical operations: can clear statistics, alarms, and log lists, and run diagnostics, but read-only access to configuration settings.
Super	Advanced operations and complete access to configuration options, but no access to user names, passwords, and other security settings.
Admin	Full access to all management and operations parameters.

19.1.1 Benefits

- Well know professional configuration and troubleshooting tool.
- Enables efficient, large scale projects rollouts with an easy loading of configurations scripts.
- Systems logs are easily reviewed and uploaded.
- Intuitive events' investigations and troubleshooting.

20. Web GUI

EtherHaul™ units' and link functionality are accessible via secured HTML based Web interface (HTTPS), for monitoring, configuring, SW upgrades and diagnostic.

The GUI enables an easy, realistic view and operation:

- One screen manages both ends of the link
- 'Quick Configuration' wizard to help fast, easy and reliable installation by non-experts staff
- Link status is presented
- Ports highlighted according to actual status
- Real reflection of systems LED indicators
- When mouse pointer touches each topic in the menu, it automatically show list of available functions with no need to enter the other screen
- Link configuration and settings

20.1.1 GUI main screen

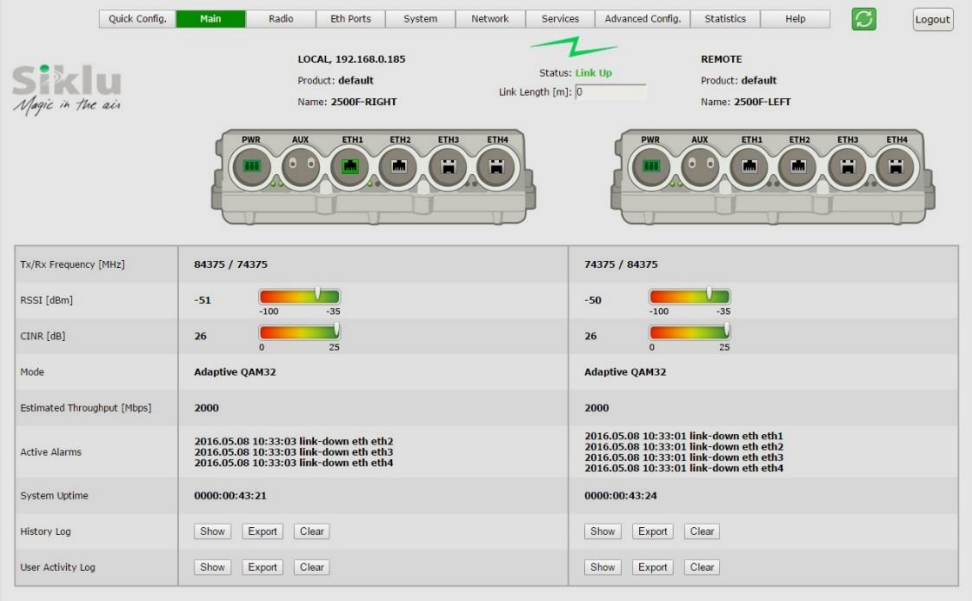


Figure 13: EtherHaul™ GUI main screen display

The main screen (Figure 13) displays all essential link status information to enable easy and fast overview:

- Link status (up/down)
- Actual link length, automatically calculated by EtherHaul™ from the measured wireless delay between both ends of the link
- Used Ethernet ports
- RSSI and CNIR
- Current modulation level
- Available capacity
- Active events or alarms summary
- Shortcuts to both system log and user activity log

Note: the GUI will reflect the exact configuration and physical layout of the ODU (example: PWR port may be present or not; there may be 2, 3 or 4 Ethernet ports).

20.1.2 Quick configuration wizard

Easy, fast, and minimal configuration process enables one quick flow, for the user to set up a link with all mandatory parameters that leads to a fully managed mode of operation.

The quick configuration wizard includes 4 steps:

1. Configuration of system parameters:
    - Specific system identification for the related location/service.
    - Date and time (there is also an option for redundant central NTP connection).

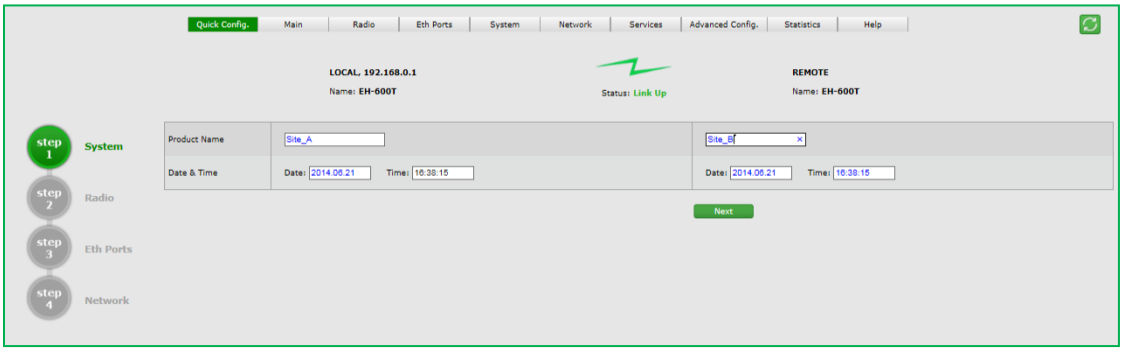


Figure 14: GUI managed mode wizard step 1

2. Configuration of the Radio:
    - Frequency channel selection
    - Tx power
    - Maximum allowed modulation
    - Symmetric / asymmetric mode selection

3. Management IP address
    - Up to 4 concurrent addresses are supported
    - Both IPv4 and IPv6 addresses are supported.
4. SNMP connectivity parameters

20.1.3 Standard compliance

- RFC2616 - Hypertext Transfer Protocol (HTTP)

- RFC2246 - Transport Layer Security (TLS) protocol
- RFC2818 - HTTP Over TLS

20.1.4 Benefits

- Configuration an EtherHaul™ link is made in a simple, fast, and in a secured manner.
- No need for dedicated client or plugins in user's terminal.
- Multiple supported management addresses enable multiple network domains connections, eliminating the need for dedicated router/VPN for multi domains connectivity.

21. SNMP

The system supports SNMP v2 and SNMP v3 – for configuration, monitoring and northbound. EtherHaul™ supports SNMP over both IPv4 and IPv6 L3 addresses schemes.

21.1.1 Standard compliance

- SNMP v2
- SNMP v3

SNMP is defined by the Internet Engineering Task Force (IETF).

21.1.2 Benefits

- Allows simple and standard integration into network management system.
- Enables monitoring, configuring and alarms flows to/from single or multiple north-bound systems.
- Most of the SNMP objects (sub element for control / monitor) are well defined by the IETF standard, thus time to market with most of systems' parameters can be within hours.

22. FTP/SFTP/TFTP

FTP, TFTP and SFTP are network protocols designed to provide file transfer and file manipulation facilities, with optional security services. EtherHaul™ uses SFTP/FTP/TFTP for software upgrades, configuration uploads and downloads.

22.1.1 Standard compliance

RFC4251- The IETF extension, of the Secure Shell protocol (SSH) version 2.0.

22.1.2 Benefits

EtherHaul™ maintenance activities are performed in a secured and standard based method, with standard IT tools.

23. Software images

The software images of EtherHaul™ radios are encrypted and signed with a security certificate. The EtherHaul™ radios validate a new software image prior to applying the new software, by checking the validity of the signature.

23.1.1 Benefits

EtherHaul™ radios are protected from mistakes or harmful software updates, an increased protection in the operations of wireless networks built with EtherHaul™ radios.

24. SW Updates

The software images of EtherHaul™ radios can be updated from the Web GUI, or SNMP or CLI. After the images are updated in the radios, the user can apply the update immediately, or schedule the update for a planned maintenance window in the future.

24.1.1 Benefits

Remote and scheduled upgrades bring a maximum of flexibility to the implementation of the SW updates, while minimizing the operation expenses.

25. User management

EtherHaul™ supports both local user management as well as centralized management with industry standard Radius or TACACS server.

25.1.1 Local/Remote user management

The user type defines the user's access privileges.

User	Read-only access, but cannot view user names, passwords, and other security settings.
Tech	Basic technical operations: can clear statistics, alarms, and log lists, and run diagnostics, but read-only access to configuration settings.
Super	Advanced operations and complete access to configuration options, but no access to user names, passwords, and other security settings.
Admin	Full access to all management and operations parameters.

25.1.2 Radius and TACACS+ user management

RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) are 2 industry standard for Authentication, Authorization and Accounting (AAA):

- 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.)

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™ as a client. Communication between EtherHaul™ and the AAA Server is performed by shared secrets which are never sent over the network. In addition, every administrator password is encrypted before it is sent between 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.

EtherHaul™ supports user authentication with TACACS+ or Radius AAA servers, up to five servers.

25.1.3 Benefits

- The hierarchical 4 levels user's access privileges suits all network sizes: large network operators, carrier-of-carrier providers as well as smaller local operators and WISPs. It enables clear separation between multiple classes of users.
- The RADIUS and TACACS supports, adds centralized user and rights management for large network operators, carrier-of-carrier providers by enabling connectivity control and accounting to minimize IT interactions with end-users without compromising security aspects.

26. EtherHaul™ Family Security

26.1.1 Security features description

- Physical
    - Penciled RF beam: requires a physical location within the antenna transmission path.
    - Minimal reflections: the extremely low transmit power and ultra-high frequencies both contribute to minimal reflections and thus enhances system's resiliency and noticeable footprint.
    - Proprietary DSP (Digital Signal Processor) for RF signals requires Siklu ODU to intercept.
    - Synchronized transmission: only 'man-in-the-middle' interception for eavesdropping.
- Link / data encryption
    - Link ID – link layer password
    - AES with 128/256 bit security (licensed based)
- Management aspects
    - SNMPv3 - Supporting both HMAC (Hash-based message authentication code) and MD5 (message-digest algorithm)
    - Access list for Host (management access) - ACL based on IP and Mask for security and Denial of Service
    - Management Vlan for isolated control of the device
    - Secured communication protocols for management: SSH (Command Line Interface, with SHA-256), HTTPS (Web-GUI, with SHA-256), SFTP (SW download and File Transfer)
- Software images
    - Software images are encrypted and signed
- User access
    - Different user types and privileges categories

26.1.2 Interface to external access rights management systems

EtherHaul™ includes full Radius/TACACS+ AAA support:

- 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.)

27. EtherHaul™ Family Logging and auditing features

Advanced logging and performance monitoring logs/stats are available and kept in the device. The information can also be exported and collected using File Transfer (both FTP, SFTP are supported).

Logs:

1. Current alarms
2. Alarm & event log file (history)
3. User activity log (stores all actions and configuration commands)

Performance statistics:

1. RF link statistics: RSSI, CINR, Modulation changes, RF statistics (errors and frame loss counters)
2. Ethernet ports statistics
3. VLAN statistics
4. Queues statistics

28. System statistics

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

EtherHaul™ collects a full day of 15 minutes statistics (96 bins) and 30 days of 24 hours history summary, the counters are available for RF, per ETH port and per VLAN (service).

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

RF	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 **Detailed collected statistics:** in-octets, in-idle-octets, in-good-octets, in-errored-octets, out-octets, out-idle-octets, in-pkts, in-good-pkts, in-errored-pkts, in-lost-pkts, out-pkts, min-cinr, max-cinr, min-rssi, max-rssi, min-modulation, max-modulation

VLAN	Displays statistic counters of each EtherHaul™ link component per VLAN **Detailed collected statistics:** in-octets, in-ucast-pkts, in-discards, in-errors, out-octets, out-ucast-pkts, out-errors, in-mcast-pkts, in-bcast-pkts, out-mcast-pkts, out-bcast-pkts, out-discards, in-no-rule-discards
Ethernet Ports	Displays Ethernet statistics counters per Ethernet port **Detailed collected statistics:** in-pkts, out-pkts, drop-pkts

28.1.1 Benefits

Real time and historical data, including RF, Ethernet ports, and VLANs values enable simple and reliable way to identify operating faults and monitor link's performance by both operators and automatic statistics collection systems.

28.1.2 Standard compliance

RFC2819 – RMON Remote Network MONitoring

29. System loopbacks

EtherHaul™ provides Ethernet and RF loopbacks designed to enable fault isolation and Ethernet service performance testing. Loopbacks functions are user configurable and support timeout in seconds.

- **Ethernet Loopback** – Internal and external loopbacks are performed on the interface, testing the local ODU, the radio link, and the remote ODU.
- **RF (Radio) Loopback** – Internal loopback is performed on the ODU's RF output.

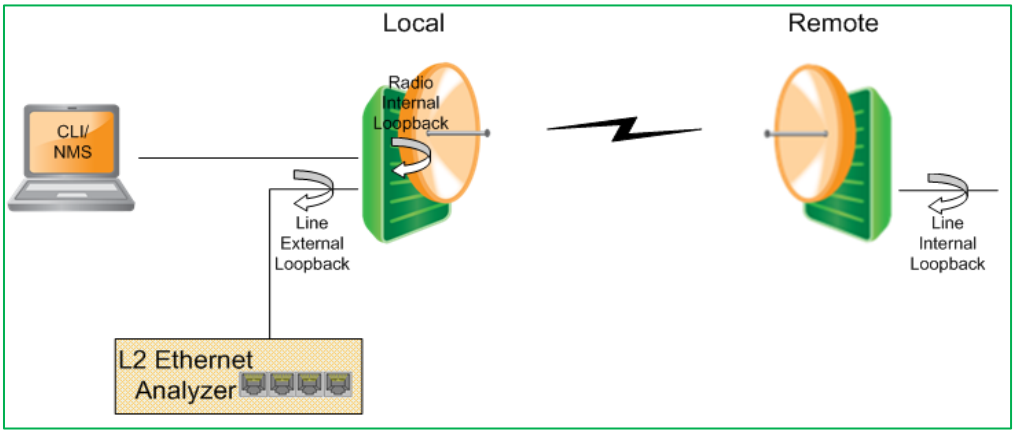


Figure 15 –System loopback points

System alarms as well as statistic displays should be used to determine if Loopback testing has passed or failed.

29.1.1 Benefits

- Enables end-to-end link tests or single unit self-test for fault detection and isolation.
- Significantly reduces operation costs by saving truck-rolls as well as number of test equipment needed for network maintenance.

30. EtherHaul™ Family Power Supply

EtherHaul™ has 2 power input options working in redundancy.

- Carrier-grade 48VDC (DC input range: 36 ÷ 57 VDC, flexible grounding)
- PoE++ (IEEE 802.3at+) over port ETH1

The power draw of a specific ODU is listed in the product specific Product Description document. Some models are equipped with both DC and PoE, while others are equipped with PoE only.

30.1.1 Benefits

Thanks to the efficient system design and high integration, EtherHaul™:

- Reduces the power consumption and accordingly the associated energy costs.
- Simplifies the installation scenario, by enabling use of a single cable for both power and data.
- Overcomes single point of failure with power redundancy for high availability and carrier grade services

31. PoE-Out

Most EtherHaul™ ODUs support PoE-Out options. The number of ports and their ratings are detailed in the specific Product Description Document.

32. EtherHaul™ Family Deployment Topologies

EtherHaul™ is easy to integrate in various topologies such as:

- Point-to-Point - Two units are used to implement a point-to-point single hop
- Point-to-Multipoint – A number of links are deployed in star configuration. The ODUs at the start of the links in the hub site may be chained to each other, or aggregated using a managed or un-managed Ethernet switch.
- Daisy-chain – A number of links are used to implement an open series of point-to-point hops, where traffic could be dropped and added at each node in the chain, while extending the reach much beyond that of a single hop. Typically the nodes can be connected without an Ethernet switch.
- Ring – A number of links are used to implement a closed series of point-to-point hops, where traffic could be dropped and added at each node in the ring. This topology also enables a diversity of packet routing options and redundancy. Typically the nodes can be connected without an Ethernet switch.
- Mesh - A number of links are used to implement a series of point-to-point hops which enable interconnection between the nodes, where traffic could be dropped and added at each node in the mesh. This topology enables redundant interconnections between the nodes. Typically the nodes can be connected without an Ethernet switch.

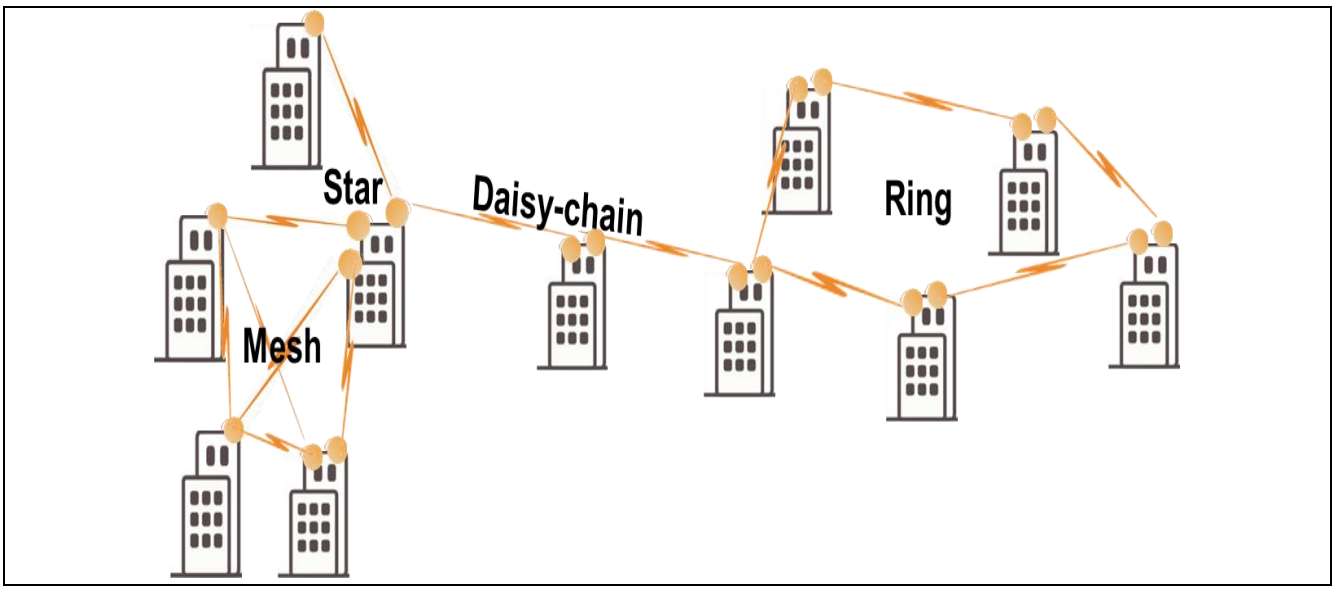


Figure 16 – Deployment topologies: Ring, Daisy-chain, Star and Mesh

In all these topologies, EtherHaul™ performs packet forwarding based on L2, and QoS based on either L2 or L3 information. Thus each incoming packet at any port in the entire network can be classified at any other node in the network, typically according to its VLAN tag and CoS bits. Based on this classification, a node can assign the packet to the proper priority queue, and thus allocate resources or force it to share the BW in a controlled manner with packets coming from other sources. The bandwidth allocation policy (QoS) at each node is fully controlled based on operator's QoS scheme configured into the system.

32.1.1 Solution benefits

- Integrated, MEF compliant switch with 2, 3 or 4 GE interfaces, especially designed for daisy chain and still preserve the ability to connect "drop" more customers/services (Technology/ costumers co-location)
- Max installation flexibility - Any combination between the chained links

33. EtherHaul™ Family Standards Compliance

The list of standards and recommendations supported generically by EtherHaul™ software and hardware is:

Management (reference also to Security)

- IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)
- IEEE 802.1ag – Connectivity Fault Management (CFM)
- IEEE 802.3ah - Ethernet in the first mile (EFM), OAM
- ITU-T Y.1731- OAM functions and mechanisms for Ethernet based networks
- RFC 1157 SNMPv2/3
- RFC 2131 - Dynamic Host Configuration Protocol
- RFC2819 – RMON Remote Network MONitoring

Security

- IETF TACACS+
- RADIUS
- RFC 2246 - Transport Layer Security (TLS) protocol
- RFC 2818 – HTTPS, HTTP over TLS
- RFC 4251 - the IETF extension of the Secure Shell protocol (SSH) version 2.0
- RFC 913 SFTP, SFTP, TFTP
- U.S. FIPS PUB 197 (FIPS 197), AES with 128/256 bits
- RFC2616 - Hypertext Transfer Protocol (HTTP)

Networking

- IEEE 1588v2, Transparent Clock mode (TC), Synchronization Messaging Channel - ESMC
- IEEE 802.1ad Provider Bridge – QinQ VLAN/VLAN stacking
- IEEE 802.1ax, LAG / LACP
- IEEE 802.1d Transparent Bridge
- IEEE 802.3ab / Ethernet 1000BASE-T
- ITU-T G.8032 Ethernet Ring Protection Switching
- ITU-T G.8261/8262/8264: Synchronous Ethernet
- MEF 21, UNI Type 2, Link OAM
- MEF 9,14
- RFC-2475 - Architecture for differentiated services.
- RFC-5865 - A differentiated services code point (DSCP) for capacity-admitted traffic
- Traffic management: 802.1p (L2), DSCP (L3) & MPLS EXP (L2.5)

Environmental, Power

- CE: CE Marked
- EMC: EN 301 489-4 ;FCC 47 CFR part 15
- IEEE 802.3af or 802.3at PoE power source (model dependent)
- IEEE 802.3at++ PoE power(ed) device (model dependent)
- Ingress Protection Rating: IP67
- MSA SFP INF-8074 Small Form Factor Pluggable
- Operation: EN 300 019-1-4 Class 4.1E
- Safety: UL 60950
- Storage: EN 300 019-1-1 Class 1.2
- Transportation: EN 300 019-1-2 Class 2.2

Additional standards and recommendations supported specifically by an EtherHaul™ ODU are listed in the product specific Product Description.

About Siklu

Siklu delivers Gigabit capacity millimeter wave wireless backhaul solutions operating in the 60, 70 and 80 GHz bands. Ideal for dense, capacity-hungry urban security networks, the ultra-high capacity wireless links can be easily and discreetly installed on the very same street fixtures as the security cameras. The most deployed mmW radios in the world, thousands of units are delivering carrier grade performance in varying weather conditions around the world.

Siklu Communication Ltd.
43, HaSivim St.
Petach Tikva 49517, Israel
Tel: +972 3 921 4015
Fax: +972 3 921 4162
hello@siklu.com