MultiHaul™

Wireless 60GHz Point to Multipoint Gigabit Ethernet

Installation, Operation and Maintenance Manual

MH-I&O-01, Issue 7

April 2019

Trademarks

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

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

Copyrights

Disclaimers

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.

About this Document

This document is the Installation, Operation and Maintenance manual for the MultiHaul™, Siklu's point-to-multipoint wireless radios.

It provides product overview and details the installation, setup and monitoring of the Base Unit (BU) and the different Terminal Units (TU).

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

- V-Band Point to multipoint – MultiHaul™ B100, T200, T201
  - MultiHaul™, minimum SW release MH-2.2.0

Audience

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

This document is intended for use by all persons who are involved in planning, installing, configuring, and using the MultiHaul™ 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 or describes an activity or situation that may or will interrupt normal operation of the MultiHaul™ system, one of its components, or the network.

Caution:

Describes an activity or situation that requires special attention or warning.

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.

Safety and Regulatory Notices

The following are mandatory notices for installation and operation of MultiHaul™ 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

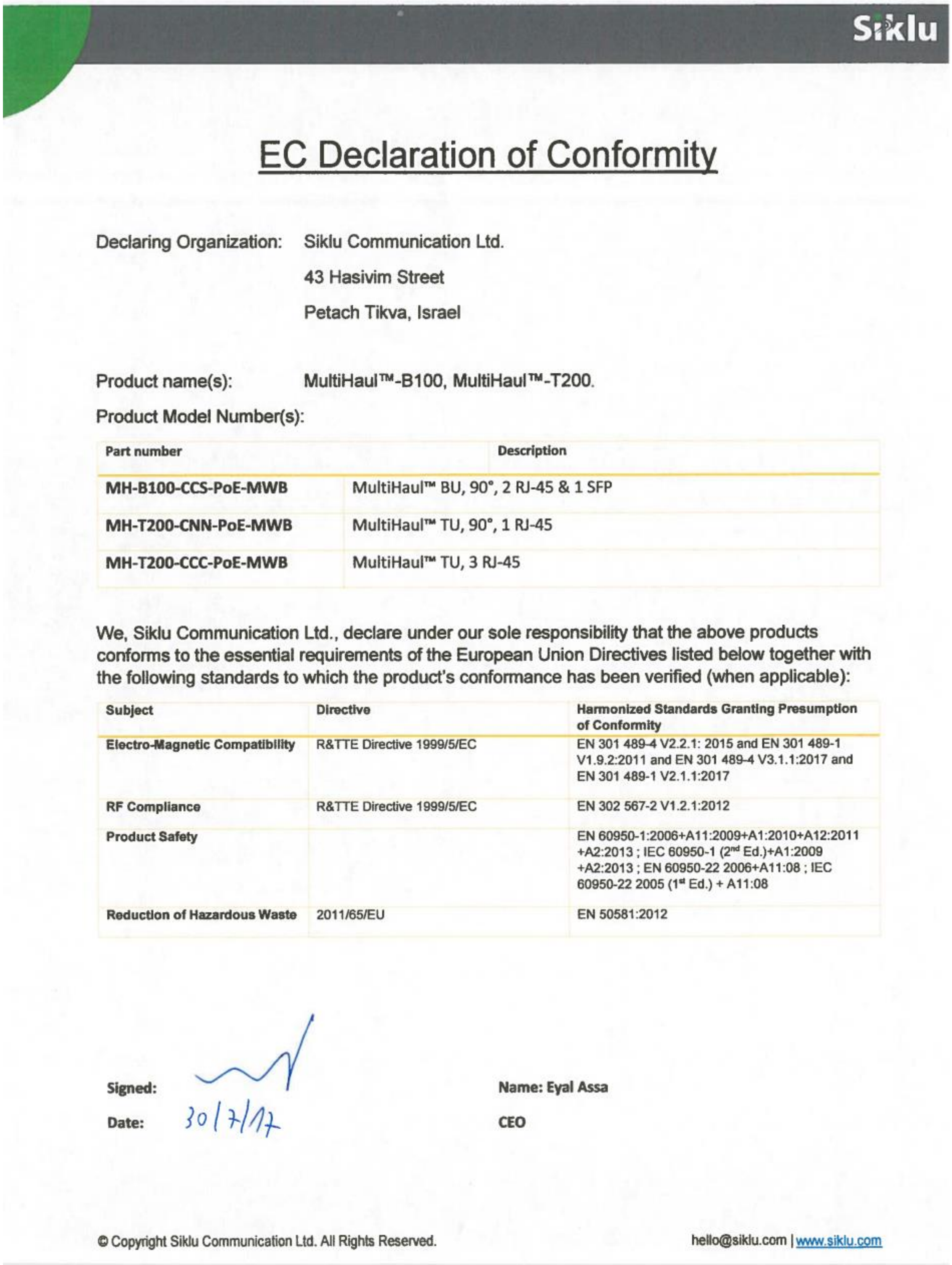
This product has been designed to comply with CE markings in accordance with the requirements of European Directive 1995/5/EC, 2011/65/EU and RED 2014/53/EU (see declaration of conformity enclosed).

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

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

This product is in full compliance with the following standards:

RF	EN 302 567-2 V1.2.1 V-Band FCC Part 15.255
EMC	EN 301 489-1, 301 489-4
Safety	IEC 60950
Operation	EN 300 019-1-4 Class 4.1
Storage	EN 300 019-1-1 Class 1.2
Transportation	EN 300 019-1-2 Class 2.2
Reduction of hazardous waste	EN 50581



Siklu

EC Declaration of Conformity

Declaring Organization: Siklu Communication Ltd.
43 Hasivim Street
Petach Tikva, Israel

Product name(s): MultiHaul™-B100, MultiHaul™-T200.

Product Model Number(s):

Part number	Description
MH-B100-CCS-PoE-MWB	MultiHaul™ BU, 90°, 2 RJ-45 & 1 SFP
MH-T200-CNN-PoE-MWB	MultiHaul™ TU, 90°, 1 RJ-45
MH-T200-CCC-PoE-MWB	MultiHaul™ TU, 3 RJ-45

We, Siklu Communication Ltd., declare under our sole responsibility that the above products conforms to the essential requirements of the European Union Directives listed below together with the following standards to which the product's conformance has been verified (when applicable):

Subject	Directive	Harmonized Standards Granting Presumption of Conformity
Electro-Magnetic Compatibility	R&TTE Directive 1999/5/EC	EN 301 489-4 V2.2.1: 2015 and EN 301 489-1 V1.9.2:2011 and EN 301 489-4 V3.1.1:2017 and EN 301 489-1 V2.1.1:2017
RF Compliance	R&TTE Directive 1999/5/EC	EN 302 567-2 V1.2.1:2012
Product Safety		EN 60950-1:2006+A11:2009+A1:2010+A12:2011 +A2:2013 ; IEC 60950-1 (2nd Ed.)+A1:2009 +A2:2013 ; EN 60950-22 2006+A11:08 ; IEC 60950-22 2005 (1st Ed.) + A11:08
Reduction of Hazardous Waste	2011/65/EU	EN 50581:2012

Signed:

Date: 30/7/17

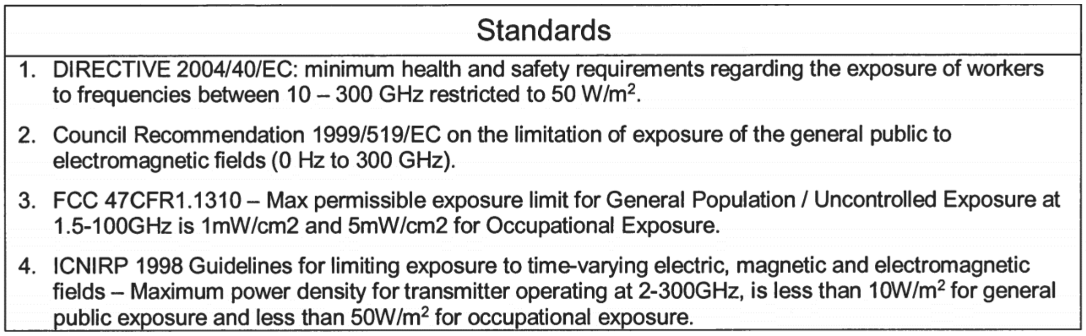
Name: Eyal Assa

CEO

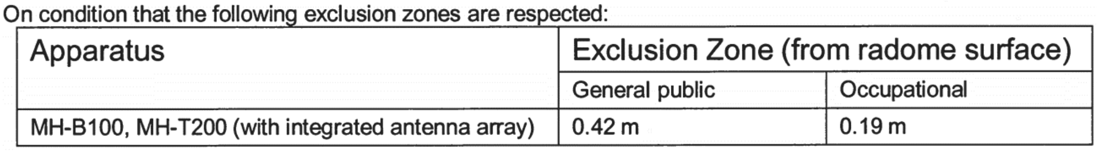
hello@siklu.com | www.siklu.com

Safe Distance and RF Exposure

This product conforms with the following:



Standards
1. DIRECTIVE 2004/40/EC: minimum health and safety requirements regarding the exposure of workers to frequencies between 10 – 300 GHz restricted to 50 W/m^2.
2. Council Recommendation 1999/519/EC on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).
3. FCC 47CFR1.1310 – Max permissible exposure limit for General Population / Uncontrolled Exposure at 1.5-100GHz is 1mW/cm2 and 5mW/cm2 for Occupational Exposure.
4. ICNIRP 1998 Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields – Maximum power density for transmitter operating at 2-300GHz, is less than 10W/m^2 for general public exposure and less than 50W/m^2 for occupational exposure.



On condition that the following exclusion zones are respected:

Apparatus	Exclusion Zone (from radome surface)	
	General public	Occupational
MH-B100, MH-T200 (with integrated antenna array)	0.42 m	0.19 m

FCC 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. 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 installées par des professionnels expérimentés d'installation qui sont familiers avec les normes locales et les codes de sécurité et, si applicable, sont agréées par les autorités gouvernementales. Ne pas le faire peut annuler la garantie du produit et peut exposer l'utilisateur final ou le fournisseur de services a des d'obligations juridiques et financieres. Les revendeurs ou distributeurs de ces équipements ne sont pas responsables des blessures, des dommages ou violations 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 au type d'antenne.

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction to the MultiHaul™ System

This chapter provides a brief overview of the MultiHaul™ product line.

The MultiHaul™ is the culmination of innovation for point to multipoint carrier-class systems operating in the uncongested unlicensed V-band, delivering very high adaptive bandwidth. It features unique self-aligning antennas for quick installation and long reach operations, in an outdoor yet eye-pleasing industrial design.

The plug and play system is designed for an easy single person installation. The patent-pending scanning antenna automatically aligns with the Base Units. For buildings with difficult roof-top access, a single base unit needs to be installed on a roof to serve multiple locations. The Base Unit (BU) supports advanced auto-provisioning: Terminal Units (TU) configuration files are stored in the BU to enable early and advanced provisioning. The TU can be located on building sides with no need for internal re-wiring of buildings to achieve net gigabit throughput.

- The MultiHaul™ Base Unit B100 (MH-B100) radio delivers carrier-grade wireless point-to-multipoint Gigabit Ethernet services.

The Base Unit supports up to 8 terminal units in a 90 degrees sector.

MH-B100-CCS-PoE-MWB	MultiHaul™ BU, 90°, 500Mbps upgradable to 1800Mbps, 2 RJ-45 & 1 SFP (1 port PSE enabled), MK & PoE injector included, IP-65, White

- The MultiHaul™ Terminal Unit T200 (MH-T200) radio delivers carrier-grade wireless point-to-multipoint Gigabit Ethernet services.

2 types of T200 Terminal Unit available:

MH-T200-CCC-PoE-MWB	MultiHaul™ TU, 90°, base rate 100Mbps upgradable to 1000Mbps, 3 RJ-45 with PSE (2 ports PSE enabled), MK & PoE injector included, IP-65, White
MH-T200-CNN-PoE-MWB	MultiHaul™ TU, 90°, base rate 100Mbps upgradable to 1000Mbps, 1 RJ-45, MK & PoE injector included, IP-65, White

- MultiHaul™ T201, also known as cTU (Compact TU), is the most compact self-aligning millimeter-wave Terminal Unit, for discrete installations on homes or poles.

The Compact T201 condenses MultiHaul™ rich feature set, proven in Service Providers and Smart Cities networks, into the smallest mmW radio in the industry, 6.5x 3.1x 1 in. (16.5x 8x 2.5 cm).

MH-T201-CNN-PoE-MWB	MultiHaul™ Compact TU, 90°, base rate 100Mbps upgradable to 1000Mbps, 1 RJ-45, built-in MK, PoE injector included, IP-65, White.

1.1 Functional Description

The key features of the system are:

- PtMP wireless connectivity in the un-licensed 60GHz band, for up to 8 stations
- Up to 8 Terminal Units
- Scanning antenna, to simplify the alignment process of the units

There are two options for this system, functionally wise. A system can serve as an access point (“Base Unit” – BU) or as an end-point station (“Terminal Unit” – TU).

The RF Section comprises an array of 32 dipole antennas, electronically controlled for smart beam-steering, allowing point to multipoint operations and auto-alignment of the narrow beams.

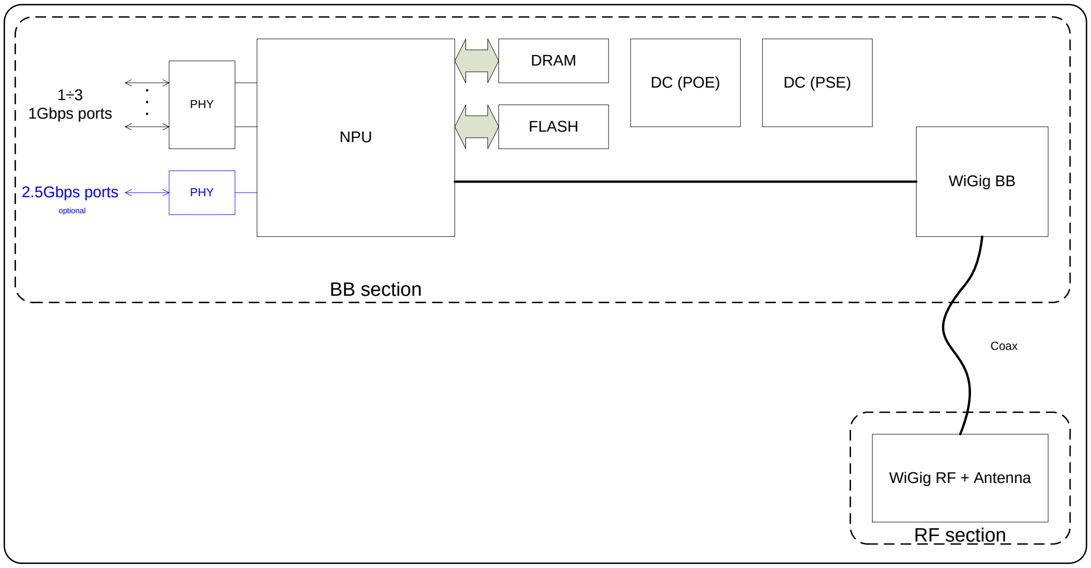


Figure 1-1 MultiHaul™ B100 and T200 Functional Block Diagram

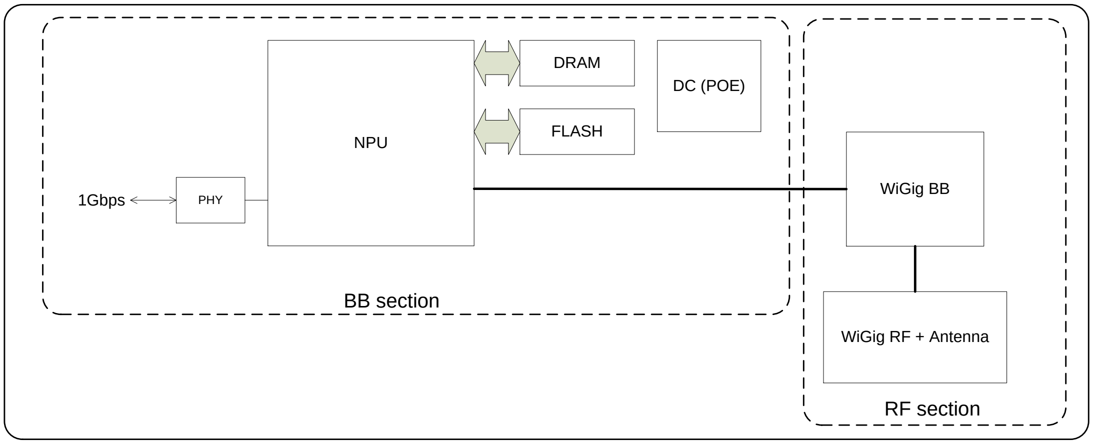


Figure 1-2 MultiHaul™ Compact TU (MH-T201) Functional Block Diagram

1.2 Technical Specifications

For detailed technical specifications, please refer to the datasheet.
For detailed supported features list please refer to the product's release notes.

		MH-BU	MH-TU
Topologies	Point to Multi-point Point to Point	✓	✓
Built-in Antenna	Horizontal scanning: 90° Vertical beam-width: 20°	✓	✓
Frequency & Duplexing	57-64GHz	✓	✓
Channels	2160MHz wide, 2 non-overlapping channels	✓	✓
Modulation & Adaptive rate	10 level of hitless adaptive coding and modulation	✓	✓
Air-interface Rate (Mbps) (1)	Air interface line rate up to	2300	2300
Aggregate L1 Rate (Mbps) (1)	Usable Ethernet line rate up to	1800	1000
System Gain (link budget)	125dB (including antenna)	✓	✓
Interfaces	3x GbE SFP supports 1GbE & 2.5GbE	2x RJ-45 1x SFP	1 or 3 x RJ-45
Terminal Units (TU)	Up to 8 Terminal Units	✓	-
Ethernet Features	IEEE 802.1d transparent bridging VLAN & VLAN stacking Jumbo frames	✓	✓
Encryption	AES 128-bits	✓	✓
Management & Provisioning	Zero-touch turn up; In-band, out-of-band management Web GUI (one-click configuration of local and remote units) & Embedded CLI SNMPv2/3, TACACS+, RADIUS	✓	✓
Conformance	Radio: FCC Part 15.255 EMC: FCC 47CFR.part 15 Safety: UL 60950	✓	✓
Power Supply	PoE (IEEE 802.3af/at)+, 10W without PoE-Out, 50W with PoE-Out.	✓	✓
PoE-Out	ETH2: 26W, 802.3at	✓	✓

---

[1] Actual throughput varies with traffic patterns to/from the Terminal Units

	ETH3: 13W, 802.3af	(SFP)	✓
Environmental	Operating Temperature: -30÷+55°C (optional -49° to +131°F) Ingress Protection Rating: IP65 (optional IP67)	✓	✓
Dimensions (HxWxD)	11.4 x 5.2 x 3.5 in. (Compact MH-T201 6.5x 3.1x 1 in.)	✓	✓
Weight	3 lbs. (including mounting kit)	✓	✓

1.3 Management

You can manage MultiHaul™ system using a Web-Based Element Management System (Web EMS) or a Command Line Interface (CLI).

Advanced network features must be managed using the CLI.

The MultiHaul™ system features a wide range of built-in indicators and diagnostic tools for advanced OAM functionality. The system is designed to enable quick evaluation, identification, and resolution of operating faults.

2 Installing the MultiHaul™ System

This chapter describes how to perform the installation of a MultiHaul™ radio (Base Unit or Terminal Unit), including:

- Preparing the Site
- MultiHaul™ Package Content
- Unpacking the MultiHaul™
- Required Tools
- Mounting the MultiHaul™
- Connecting the Cables
- System LEDs
- Installing the MultiHaul™
- Link Up Verification and Initial Commissioning

The installation of the MultiHaul™ radio is followed by initial system setup that will be described in the next chapter.

Caution:

Avertissement:

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

L'installation et l'entretien de la liaison MultiHaul™ ne doivent être effectués par du personnel de service qui sont formés et accrédités pour mener à bien ces activités.

Minimum safe distance from antenna while radiating is 42cm (general public) or 19cm (occupational) (according to calculation done based on "Environmental evaluation and exposure limit according to FCC CFR 47part 1, 1.1307, 1.1310; RSS-102, Safety Code6).

Distance de sécurité minimum de l'antenne tout en rayonnant est 42cm (selon le calcul fait sur la base de "l'évaluation environnementale et la limite d'exposition selon FCC CFR 47part 1, 1,1307, 1,1310, RSS-102, CODE6 sécurité).

2.1 Preparing the Site

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

2.1.1 Physical and Environmental Requirements

Each site should adhere to the following requirements:

- There must be a clear, unobstructed line-of-sight between the radios.
- The MultiHaul™ radio should be mounted on a fixed, stable, permanent structure. A reinforced steel mounting pole is required, with a diameter measuring from 2-4 inches (recommended). Note that the radio can be mounted on poles from 1.5-12 inches using the provided self-locking bands.

Caution:

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

- The MultiHaul™ may be installed directly on a wall using its mounting kit.
- You must mount the MultiHaul™ radio in a site that is easily accessible to authorized personnel, and only authorized personnel.
- Operating temperature: between -30° and +55°C.
- Relative humidity: 0 to 100%.
- Maximum altitude: 4,500m.

2.1.2 Cabling Requirements

- Install the MultiHaul™ radio where network connections and optional power cabling are ready for operation and easily accessible.
- All cabling connected to the radio should be outdoor-grade, with UV protection.
- PoE input – Connect Ethernet cable to Eth1
- PSE Output (PoE Out) – for models with more than a single Ethernet port.

  The voltage output at the PSE port is following the voltage at the PoE input port. The total cables length, from the PoE device to the powered device (PD) should not exceed 100 meter (PoE to first radio + first to second radio).

Note:

PSE Output available only is directly powered by PoE Injector/Midspan!

PSE Output is over 2 pairs. It means you can use the PSE Output to power up other devices or other MultiHaul™ units, however, the MultiHaul™ that was powered by PSE will not be able to power up other devices (no PSE Output).

- You should use shielded outdoor Cat5e cables terminated with metallic RJ45 connectors.
- In order to protect indoor equipment, you must install surge protection circuits on all copper cables on their entrance to the building.

- Install the MultiHaul™ radio in a location where proper electrical outdoor grounding is readily available. Typically, the grounding connection is attached directly to the mounting pole. If not already present, then suitable structure-to-earth grounding connections must be created before installation. Ground the radio using a minimum quantity of 16AWG grounding cable or according to local electrical code.

Note:

The MultiHaul™ T201 (cTU) does not require grounding.

Caution:

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

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

2.2 MultiHaul™ Package Content

The MultiHaul™ B100 or T200 packages include the following components:

Package	Description	Quantity
MultiHaul™ Radio		
	MultiHaul™ radio (integrated antenna)	1
	All-Weather shells, protecting cable entry	1 or 3 (model dependent)
	Unit grounding cable (90 cm)	1
	MultiHaul™ mounting assembly (attached to the radio)	1
	Self-locking bands	2
	PoE injector with AC cable	1

The MultiHaul™ T201 packages include the following components:

Package	Description	Quantity
MultiHaul™ Radio		
	MultiHaul™ radio (integrated antenna)	1
	All-Weather shell, protecting cable entry	1
	Cable ties	2
	PoE injector with AC cable	1

2.3 Unpacking the MultiHaul™

The MultiHaul™ package content should be examined carefully before installation.

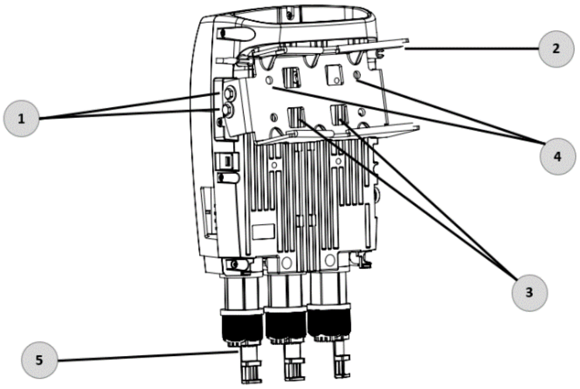
When you unpack the components of the MultiHaul™, it is important to use care to avoid damaging or scratching the antenna radome.

2.4 Required Tools

Ensure that you have the following tools with you when performing a MultiHaul™ installation:

- Philips screwdriver, medium size head
- Flat-head screwdriver, medium size (5mm) head
- 7mm Hex socket driver
- Standard open-end wrench, 13mm for the ports’ caps
- Cable ties (for securing network and optional power cables)
- Cutter
- Cable labeling

2.5 Mounting the MultiHaul™



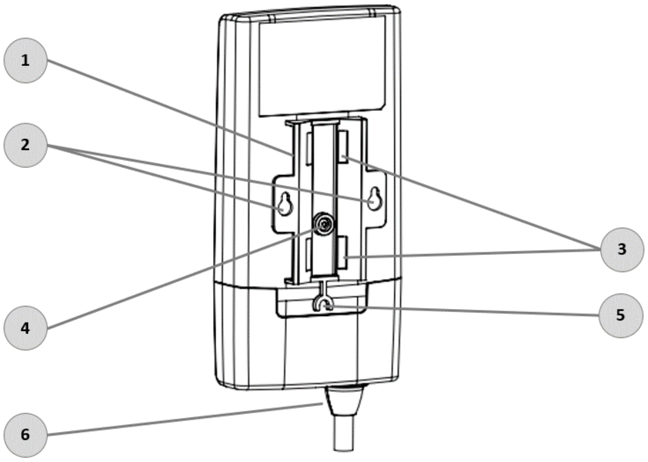
1. Elevation Lock Bolts (2x 7mm on each side)
2. Mounting bracket
3. Self-locking bands fixing points (for 2x 130mm bands provided)
4. Wall-mount fixing holes (x4)
5. All-weather shells (1 or 3, depending on model)

Figure 2-1 MultiHaul™ B100/T200 and Mounting Bracket

The mounting kit may be installed on a wall. Use 4 wall mount screws (not provided).

The MultiHaul™ radio is compatible with the EH-MK-SM mounting kit that may be used in case of extreme height difference between the sides.

2.5.1 Mounting the Compact MultiHaul™ T201

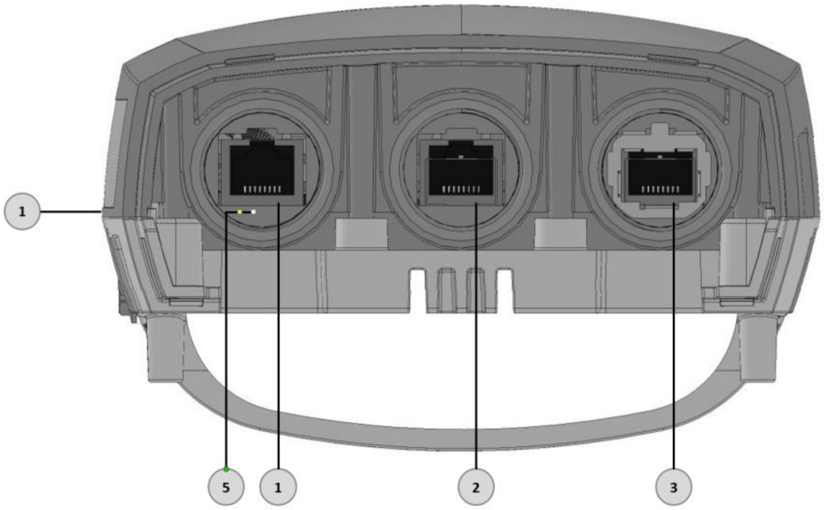


1. Integral mounting bracket (pole or wall mount)
2. Wall-mount fixing holes (x2)
3. Self-locking bands fixing points (for 2x cable ties provided)
4. Radio board fixing screw (DO NOT REMOVE)
5. Wall-mount screw location
6. All-weather rubber ring

Figure 2-2 MultiHaul™ T201 and Mounting Bracket

The compact MultiHaul™ T201 has a mounting bracket as part of its body. Use two cable ties to fix it to the pole.

2.6 Connecting the Cables – MultiHaul™ B100/T200



1. Electrical Ground Point (GND)
2. Ethernet RJ45 Eth#1 (PoE in)
3. Ethernet RJ45 Eth#2 (PoE Out) – model dependent
4. Ethernet Eth#3 or RJ45 (PoE Out) – model dependent
5. Reboot push-button. Restore Factory Default (push for more than 10 seconds)

Figure 2-3 MultiHaul™ B100/T200 Connection Panel Details

Caution:

Use only Class 1 Laser SFP with rated voltage of 3.3Vdc which is safety approved to UL/EN/IEC 60950-1 and which is CDRH registered.

2.6.1 Power Options

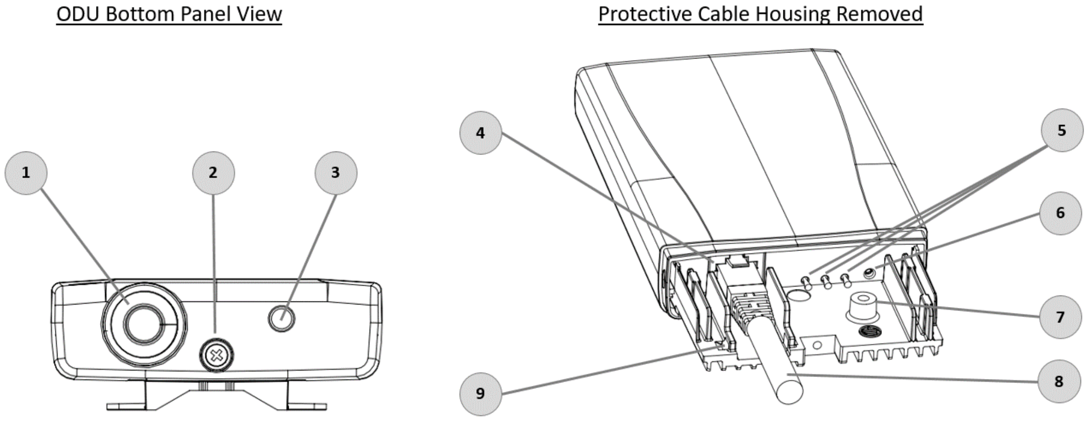
To power up the MultiHaul™ using PoE, connect the cable to Eth#1.

You may use direct DC (input range: 36÷57Vdc) by using an RJ45-DC Adapter (can be obtained from Siklu). In this case, port ETH#1 will be used for power only.

Caution:

Use a PoE power supply which is safety approved to UL/EN/IEC 60950-1 as a limited power source (LPS) with rated voltage of 42-57Vdc and rated current of 1.4A max, and approved for the altitude where it is deployed

2.7 Connecting the Cables – MultiHaul™ T201



1. Ethernet RJ45 cable entry
2. Protective cable housing lock screw
3. Optional ground cable inlet (drilling required)
4. Eth1 RJ45 PoE In
5. ODU LEDs – Eth1, RF and Power
6. Reboot push-button. Restore Factory Default (push for more than 10 seconds)
7. Optional ground (GND) point
8. Ethernet RJ45 cable
9. Ethernet RJ45 cable tie fixing points

Figure 2-4 MultiHaul™ T201 Connection Panel Details

To connect the cable to the radio, unlock the Phillips screw at the bottom of the unit and remove the protective cable housing.

Power up the MultiHaul™ T201 by connecting the PoE device to the Eth1 port.

2.7.1 Grounding the MultiHaul™

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

To make a protective earth connection, use the grounding point located on the System ODU using a minimum amount of 16AWG grounding cable or according to local electrical code.

Note: The compact MultiHaul™ T201 is designed to work without ground. However, do verify that the PoE is grounded and shielded cables+connectors used.

It is recommended to use Lightning Surge Protector on every Ethernet cable to protect the indoor networking equipment. The Lightning Surge Arrestor should be installed indoor next to the cable’s point-of-entry and should be properly grounded.

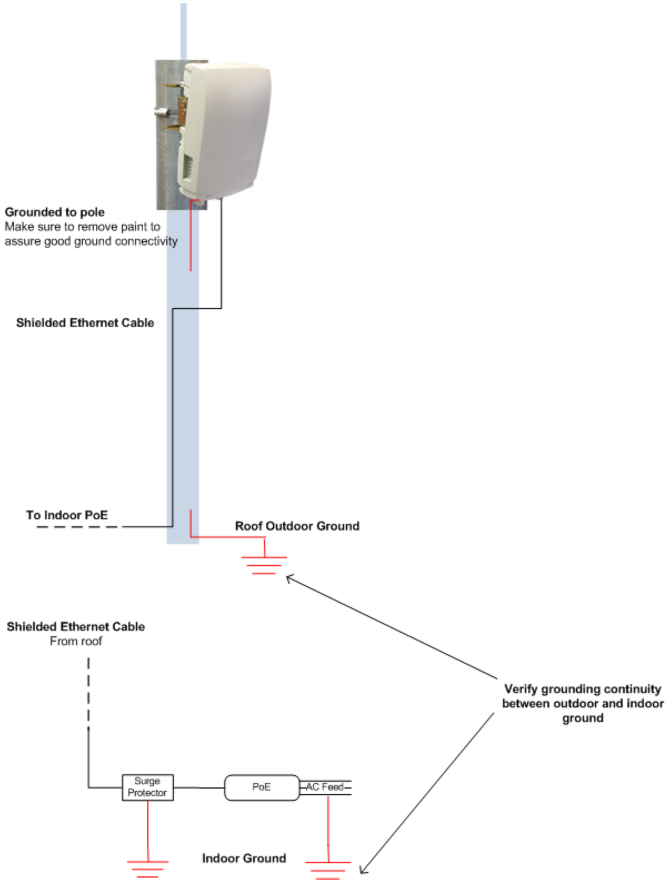


Figure 2-5 Grounding Scheme

2.7.2 Weatherproofing the Cables

Before inserting a cable connector into the ODU, you must first enclose the cable connector in a protective All-Weather shell. Three sets of All-Weather shells are provided with the ODU for the ODU interfaces.

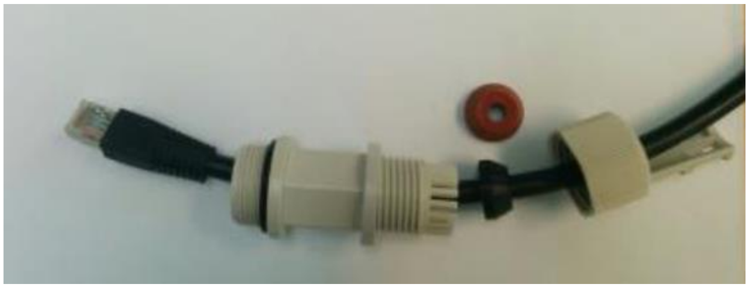


Figure 2-6 All-Weather Connecting Cable Shell Assembly

The provided protective All-Weather Shells fit cables from 3.5mm to 9.0mm diameter.

1. Thread the cable and tight the shell to the ODU firmly by hand (do not use tools).

2. Insert the rubber gasket snugly and tight the connector lock.

Caution:

To avoid accidental damage to the connector, when removing the All-Weather Shell, unlock the gland first.

2.7.3 Preparing and Weatherproofing the Cable – MultiHaul™ T201

The ODU is provided with rubber gasket (for cables from 3.5mm to 9.0mm diameter) designed to weatherproof the cable entry to the compact TU housing.

1. To connect the cable to the radio, unlock the Phillips screw at the bottom of the unit and remove the protective cable housing.
2. Connect the the Ethernet RJ45 cable to the radio. Use a miniature cable tie (not provided) to secore the cable.
3. Positing the rubber gasket and assemble the protective housing.
4. Lock the Phillips screw.

Figure 2-7 All-Weather Connecting Cable Shell Assembly

2.8 System LEDs

LED	Color	Description
PWR (Power)	Green – Power ON	Blink Green – booting up
	Orange – Booting up (2 seconds)	Boot failure (if continues)
	Off – No Power	
RF	Green – Link up	TU: connected to the BU BU: at least one TU connected
	Off – No link	
ETH1/2/3:	Green – Link 1G	
	Orange – Link 10/100	
	Off – No Link (Carrier)	

2.9 Installing the MultiHaul™

1. Mount the radio and its mounting bracket on a fixed reinforced steel mounting pole, 1.5-12 diameter (recommended 2-4 inches).
2. Use included self-locking bands to secure the bracket to the mounting pole.
3. In order to allow free movement when pointing the radio, unlock the Elevation Lock Bolts.
4. Verify visually that the radio is pointing to the remote site. Optimize the Azimuth alignment by turning the mounting bracket (make sure the self-locking bands are not tightened) and change the Elevation alignment by moving the radio up and down.
5. Once optimum achieved, fasten the self-locking bands to secure the bracket to the mounting pole and tighten the Elevation Lock Bolts.

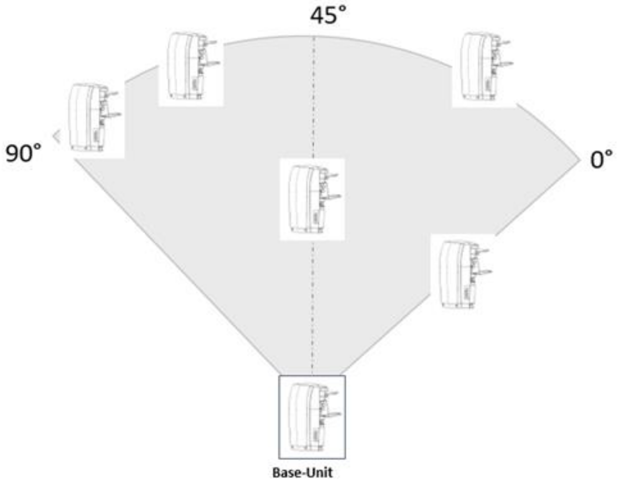


Figure 2-8 Scanning Antenna

<u>Notes regarding alignment:</u>

The Multihaul™ antenna sector coverage is 90° horizontally and 20° vertically.

For optimal coverage, point the Base Unit towards the sector center (45°) horizontally and to the farthest terminal unit vertically.

Terminal Units should be pointed towards the Base Unit.

Alignment is now completed. The system's scanning antenna will automatically align the beams for optimal performance.

2.10 Link Up Verification and Initial Commissioning

1. Verify that RF LED is green on the TUs, indicating association (Link UP).

The MultiHaul™ link can now pass traffic and management between the ports and over the radio link.

Base-Unit (BU):

1. Verify the BU is pointing towards the sector center (45°) horizontally and to the farthest terminal unit vertically.
2. Verify the self-locking bands are tightened.
3. Power up the BU and verify Power LED is green.

Terminal Unit (TU):

Up to 8 TUs may be connected to one BU.

1. Point the TU towards the BU. When wall mount is used, verify the BU is located within the 90° sector's coverage.
2. Verify the self-locking bands and the Elevation Lock Bolts are locked.
3. Power up the TU and verify Power LED is green. The RF LED should be green, indicating correct association (Link Up).

Repeat these steps for the next TUs.

Use the Web-based Management or Command Line Interface for radio link configuration and monitoring.

3 Setup and Monitoring Using the Web-based Management

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

There are 2 options to connect and manage the MultiHaul™:

1) HTML Web-Based Management with Graphical User Interface (GUI)
2) Command Line Interface

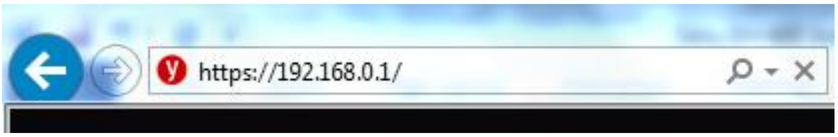
It is recommended to use the web-based management option that is described in details in this document as it provides self-explanatory graphical user interface for managing both ends of the link and the PTMP cluster.

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

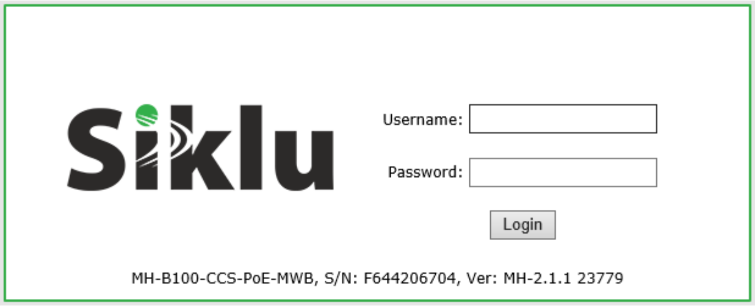
1. Launch an Internet Browser and enter **`https://`** followed by the system's IP address. The system's default IP address is **`192.168.0.1`**.



https://192.168.0.1/

Figure 3-1 Launching the Web-Based Management

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

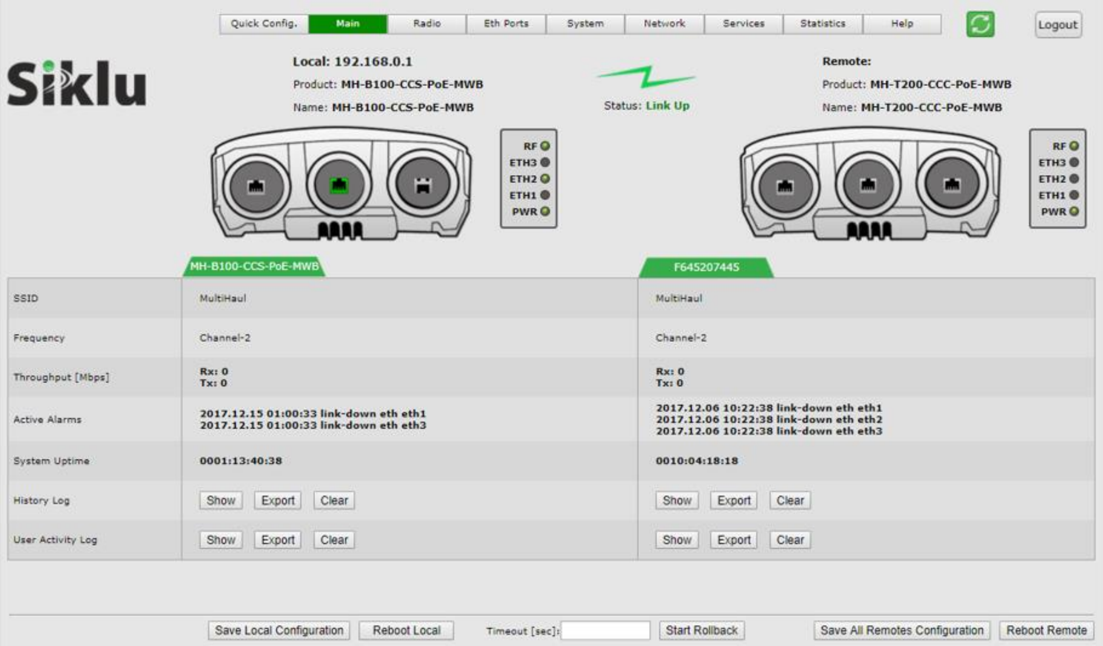


MH-B100-CCS-PoE-MWB, S/N: F644206704, Ver: MH-2.1.1 23779

Figure 3-2 Entering Username and Password

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

When connecting to a Base Unit, all Terminal Units will be displayed on the remote tab, on the right.



Local: 192.168.0.1
Product: MH-B100-CCS-PoE-MWB
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

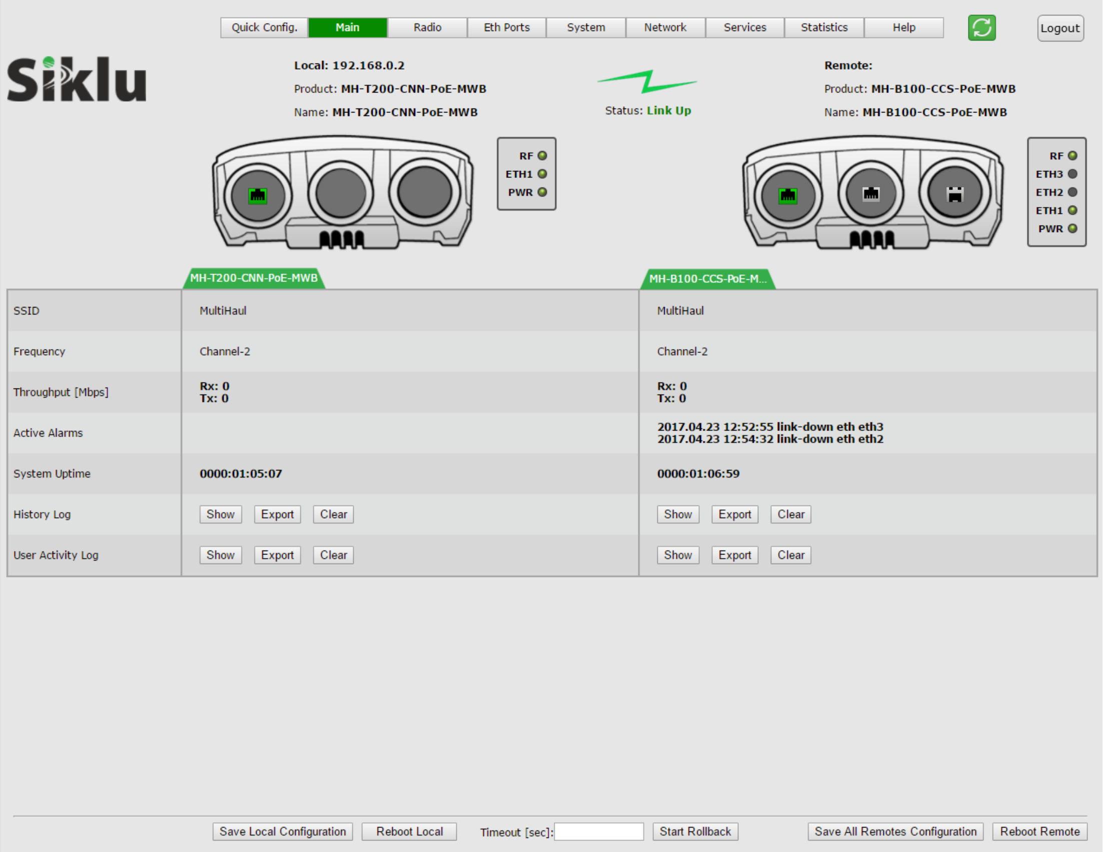
Remote:
Product: MH-T200-CCC-PoE-MWB
Name: MH-T200-CCC-PoE-MWB

	MH-B100-CCS-PoE-MWB	F645207445
SSID	MultiHaul	MultiHaul
Frequency	Channel-2	Channel-2
Throughput [Mbps]	Rx: 0 Tx: 0	Rx: 0 Tx: 0
Active Alarms	2017.12.15 01:00:33 link-down eth eth1 2017.12.15 01:00:33 link-down eth eth3	2017.12.06 10:22:38 link-down eth eth1 2017.12.06 10:22:38 link-down eth eth2 2017.12.06 10:22:38 link-down eth eth3
System Uptime	0001:13:40:38	0010:04:18:18
History Log	Show Export Clear	Show Export Clear
User Activity Log	Show Export Clear	Show Export Clear

Timeout [sec]:

Figure 3-3 Web-Based Management Main Page (Base Unit)

When connecting to a Terminal Unit, the Base Unit will be displayed in the remote tab, on the right.



Local: 192.168.0.2
Product: **MH-T200-CNN-PoE-MWB**
Name: **MH-T200-CNN-PoE-MWB**

Status: **Link Up**

Remote:
Product: **MH-B100-CCS-PoE-MWB**
Name: **MH-B100-CCS-PoE-MWB**

	MH-T200-CNN-PoE-MWB	MH-B100-CCS-PoE-M...
SSID	MultiHaul	MultiHaul
Frequency	Channel-2	Channel-2
Throughput [Mbps]	**Rx: 0** **Tx: 0**	**Rx: 0** **Tx: 0**
Active Alarms		**2017.04.23 12:52:55 link-down eth eth3** **2017.04.23 12:54:32 link-down eth eth2**
System Uptime	**0000:01:05:07**	**0000:01:06:59**
History Log	Show Export Clear	Show Export Clear
User Activity Log	Show Export Clear	Show Export Clear

Timeout [sec]:

Figure 3-4 Web-Based Management Main Page (Terminal Unit)

3.2 Web-Based Management Main Page

The Web-Based Management provides link view, presenting both local and remote (or remotes, in case of multiple Terminal Units) configuration and monitoring.

Note:

Depending on your work 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).

Although the local and remote systems IP address are identical (default IP address 192.168.0.1), the remote can be displayed as the MultiHaul™ 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:

When first connecting to a link or cluster with units in their default IP address, you may connect to a different unit, not necessarily the one you are connected to. Assign additional dedicated IP addresses and use it instead of the default one.

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

- Product – product model (factory).
- Name – the configured name of the unit (by default, same as Product).
- Physical view – of local and remote units, with interfaces and led status.
- Link Status – Link up or down (with visual indication).
- Frequency – channel number (2 or 3).
- Throughput – for Tx and Rx over the RF interface (in Mbps). Displayed for the last 1-second interval.
- 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.

3.3 General Configuration Commands

3.3.1 Apply

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

The Local-Remote (and multiple remotes in case of multiple Terminal Units) 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(s) 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.

3.3.2 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` and **`Save All Remotes Configuration`** buttons are available for local and remote systems.

3.3.3 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(s) systems.

3.3.4 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.

3.3.5 Copy to Remote

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

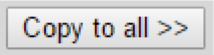


Figure 3-5 Copy to all >> button

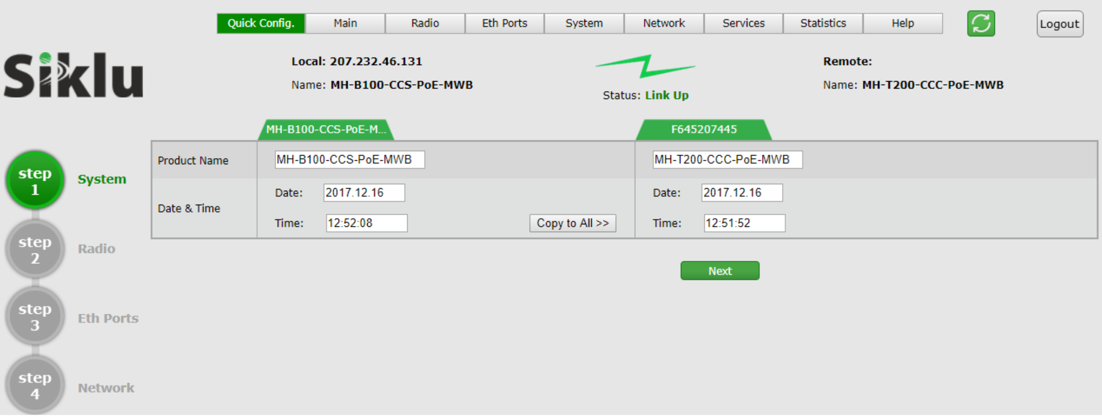
3.4 Quick Configuration Wizard

Use the Quick Configuration wizard to configure the basic system parameters. It covers 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.

To access the Quick Configuration wizard, go to the **Quick Config** page.

3.4.1 Quick Configuration: Step 1 – System



Local: 207.232.46.131

Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:

Name: **MH-T200-CCC-PoE-MWB**

	MH-B100-CCS-PoE-M...	F645207445
Product Name	MH-B100-CCS-PoE-MWB	MH-T200-CCC-PoE-MWB
Date & Time	Date: 2017.12.16 Time: 12:52:08	Date: 2017.12.16 Time: 12:51:52

Figure 3-6 Quick Config Page: Step 1 - System

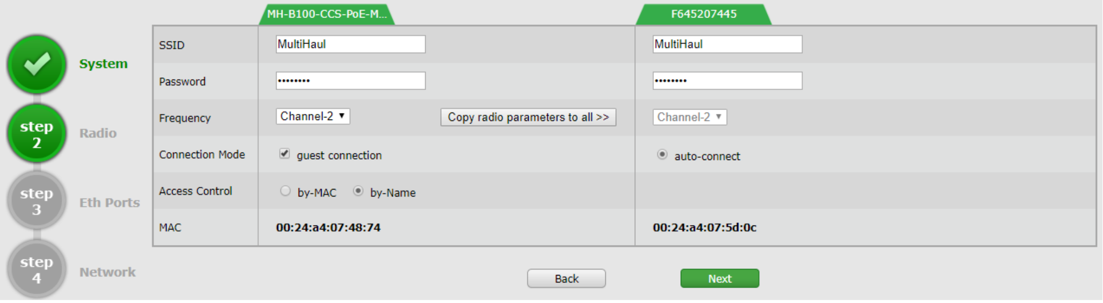
The first section allows configuring the following parameters:

- Name – you can give a name to each system
- Date – [YYYY.MM.DD]
- Time – [HH:MM:SS]

Click **Copy to all** to set identical Date & Time on remote terminals.

Click **Next** to continue.

3.4.2 Quick Configuration: Step 2 – Radio



	MH-B100-CCS-PoE-M...	F645207445
SSID	MultiHaul	MultiHaul
Password	••••••••	••••••••
Frequency	Channel-2 ▾	Channel-2 ▾
Connection Mode	☑ guest connection	● auto-connect
Access Control	○ by-MAC ● by-Name	
MAC	**00:24:a4:07:48:74**	**00:24:a4:07:5d:0c**

Figure 3-7 Quick Config Page: Step 2 - Radio

This section allows configuring the following parameters:

- SSID – Service Set Identifier (SSID) of the BU. Default: MultiHaul.

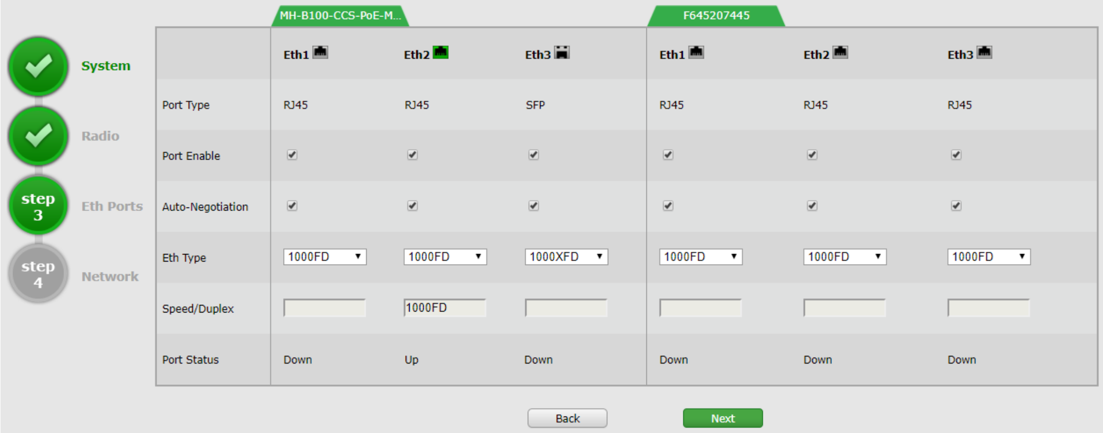
  The BU broadcasts openly its SSID.

- Password – password used for authentication. Default: MultiHaul.
- Frequency – the channel number (channel2 or 3). Default: channel-2.

  Frequency setting is available for BU only. The TU will scan and be able to connect to a BU on all channels.

- Connection Mode
  - Guest-connection (Base Unit only) – determines if guest (unmanaged) TUs can be associated with the BU. If guest-connection is enabled, any TU with the correct SSID and password can connect to the BU, up to the maximum number of supported TUs.
  - Auto-Connect (Terminal Unit only) – TU will connect automatically to BU in case SSID/password match.
- Access Control (Base Unit only)
  - By-MAC or By-Name. determines if TUs are identified by MAC address or by configured name (relevant for TU management by BU feature).
- MAC (R/O) – radio's MAC address.

3.4.3 Quick Configuration: Step 3 – Eth Ports



	MH-B100-CCS-PoE-M...			F645207445		
	Eth1	Eth2	Eth3	Eth1	Eth2	Eth3
Port Type	RJ45	RJ45	SFP	RJ45	RJ45	RJ45
Port Enable	☑	☑	☑	☑	☑	☑
Auto-Negotiation	☑	☑	☑	☑	☑	☑
Eth Type	1000FD	1000FD	1000XFD	1000FD	1000FD	1000FD
Speed/Duplex		1000FD				
Port Status	Down	Up	Down	Down	Down	Down

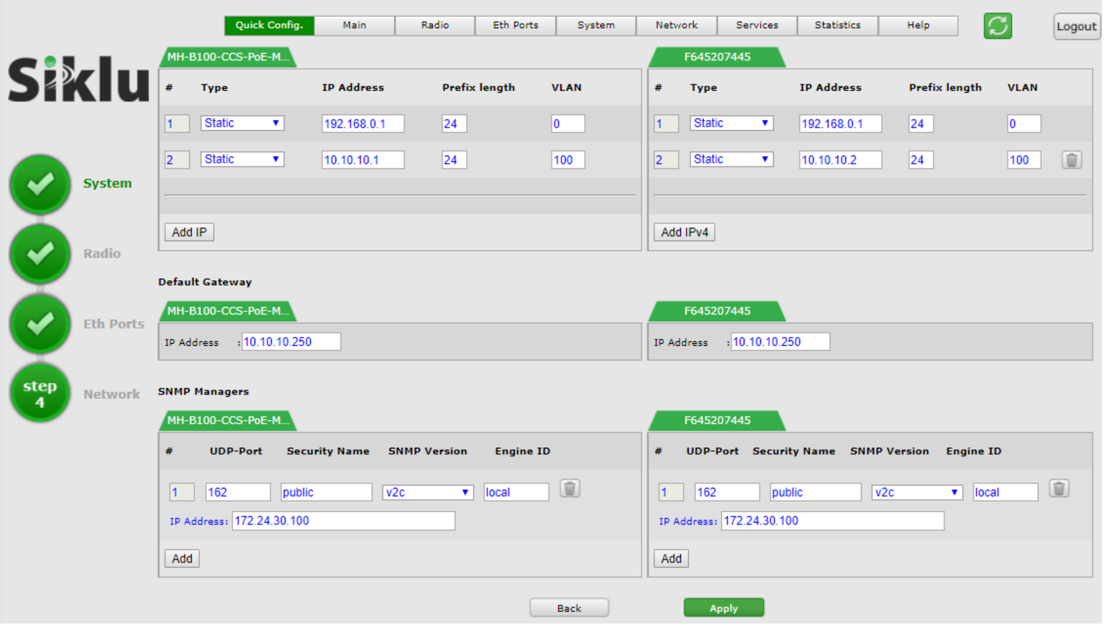
Figure 3-8 Quick Config Page: Step 3 – Eth Ports

This section allows configuring the following parameters:

- Port status visual display (Green – port is up).
- Port Type – RJ45 or SFP
- Port Enable – checkbox to enable the port.
- Auto Negotiation – checkbox to enable auto-neg.
- Speed/Duplex – speed (10/100 or 1000) and duplex (half/full) setting:
    - When Auto Negotiation Enabled – R/O field indicating the current speed/duplex
    - When Auto Negotiation Disabled – allows configuring the speed/duplex.
    - R/O field indicating the current speed/duplex (note that for SFP ports, only 1000 speed is available).
- Speed/Duplex (SFP) – 1000XFD (for 1Gbps) or 2500XFD (for 2.5Gbps) SFPs.

Click **`Next`** to continue or **`Back`** to return to previous section.

3.4.4 Quick Configuration: Step 4 – Network



MH-B100-CCS-PoE-M...

#	Type	IP Address	Prefix length	VLAN
1	Static	192.168.0.1	24	0
2	Static	10.10.10.1	24	100

F645207445

#	Type	IP Address	Prefix length	VLAN
1	Static	192.168.0.1	24	0
2	Static	10.10.10.2	24	100

Default Gateway

MH-B100-CCS-PoE-M...

IP Address : 10.10.10.250

F645207445

IP Address : 10.10.10.250

SNMP Managers

MH-B100-CCS-PoE-M...

#	UDP-Port	Security Name	SNMP Version	Engine ID
1	162	public	v2c	local

IP Address: 172.24.30.100

F645207445

#	UDP-Port	Security Name	SNMP Version	Engine ID
1	162	public	v2c	local

IP Address: 172.24.30.100

Figure 3-9 Quick Config Page: Step 4 – Network

This section allows configuring the following parameters:

- IP Address

The MultiHaul™ units support up to four management IP addresses that can be associated with different VLANs. IP address may be Static or acquired by DHCP.

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

- Default Gateway
- SNMP Managers

Up to five managers that will receive SNMP traps can be configured (SNMPv2c or SNMPv3).

  - # - Index (1-5)
  - IP Address – Destination IP Address
  - UDP Port – port number for sending traps
  - Security Name (community)

  - SNMP Ver – SNMP version (SNMPv2c or SNMPv3)
  - Engine ID – Used for SNMPv3

Click **`Apply`** to execute the configuration changes or **`Back`** to return to previous section.

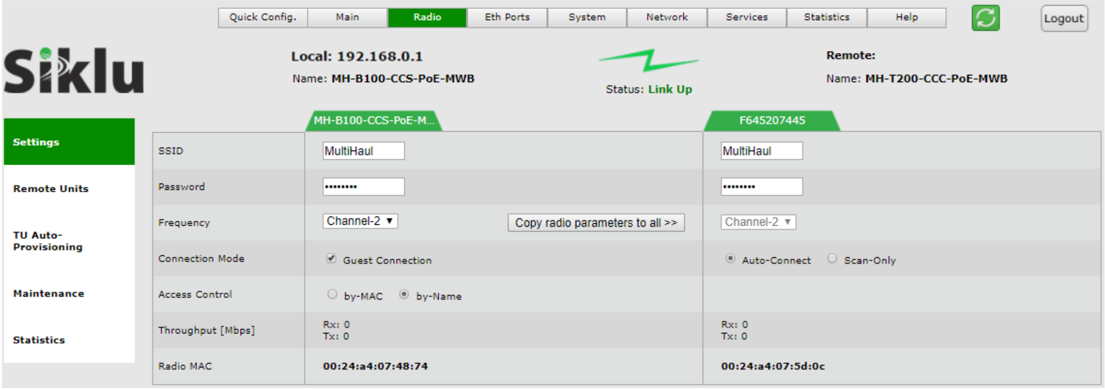
3.5 Radio Configuration and Monitoring

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

This chapter includes the following topics:

- Settings
- Remote Terminals
- Maintenance
- Scan Results

3.5.1 Settings



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

	MH-B100-CCS-PoE-M...	F645207445
SSID	MultiHaul	MultiHaul
Password	••••••••	••••••••
Frequency	Channel-2	Channel-2
Connection Mode	☑ Guest Connection	● Auto-Connect ○ Scan-Only
Access Control	○ by-MAC ● by-Name	
Throughput [Mbps]	Rx: 0 Tx: 0	Rx: 0 Tx: 0
Radio MAC	00:24:a4:07:48:74	00:24:a4:07:5d:0c

Figure 3-10 Radio Page: Settings

This section allows monitoring and configuring the following parameters:

- SSID – Service Set Identifier (SSID) of the BU. Default: MultiHaul.

  The BU broadcasts openly its SSID.

- Password – password used for authentication. Default: MultiHaul.
- Frequency – the channel number (channel2 or 3). Default: channel-2.

  Frequency setting is available for BU only. The TU will scan and be able to connect to a BU on all channels. The TU will present the frequency channel it is on.

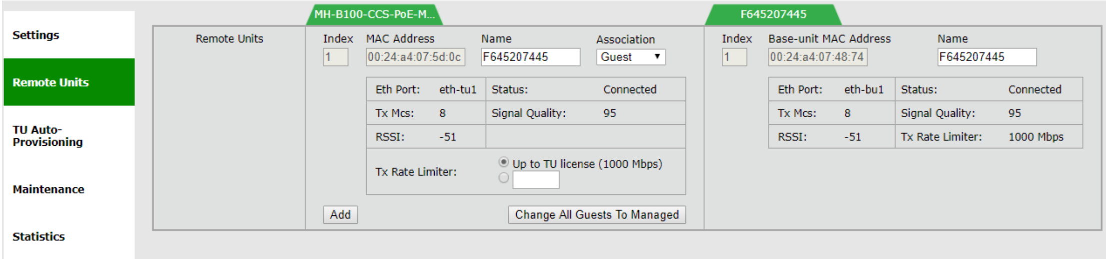
- Connection Mode
  - Guest-connection (Base Unit only) – determines if guest (unmanaged) TUs can be associated with the BU. If guest-connection is enabled, any TU with the correct SSID and password can connect to the BU, up to the maximum number of supported TUs.
  - Auto-Connect (Terminal Unit only) – TU will connect automatically to BU in case SSID/password match.

  - Scan only (Terminal Unit only) – TU will scan and present all visible BUs (without connecting to any of them, even if SSID/password match). User will then be able to select which BU to connect to.

    Note that when link to BU is down, the TU will be in 'scanning' mode and will present its scan results.

- Access Control (Base Unit only)
  - By-MAC or By-Name. determines if TUs are identified by MAC address or by configured name (relevant for TU management by BU feature).
- Throughput – the transmitted and received throughput over the RF interface (in Mbps).
- MAC (R/O) – radio's MAC address.

3.5.2 Remote Terminals (Base Unit Only)



MH-B100-CCS-PoE-M...

Index	MAC Address	Name	Association
1	00:24:a4:07:5d:0c	F645207445	Guest

Eth Port:	eth-tu1	Status:	Connected
Tx Mcs:	8	Signal Quality:	95
RSSI:	-51		
Tx Rate Limiter:		● Up to TU license (1000 Mbps) ○	

F645207445

Index	Base-unit MAC Address	Name
1	00:24:a4:07:48:74	F645207445

Eth Port:	eth-bu1	Status:	Connected
Tx Mcs:	8	Signal Quality:	95
RSSI:	-51	Tx Rate Limiter:	1000 Mbps

Figure 3-11 Radio Page: Remote Terminals

From the Base Unit you can provision the remote Terminal Units.

This section allows monitoring and configuring the following parameters:

- MAC Address – radio MAC address of the remote TU/BU.
- Name – text string representing the name of the remote TU. Default: Serial Number of the remote TU.

Note:

Either MAC Address or Name will be available for configuration, depending on the Access-control setting on the Radio-Settings page (By-MAC or By-Name).

- Association – guest or managed.
  - Guest – TUs that are connected as 'guest' do not require setting on the BU side. An RF port will be created in case TU is connected.

    No services configuration is supported for 'guest' TUs (transparent bridge only).

  - Managed – TUs that are set to 'managed' reserve their RF port settings and will allow settings of services.

Note:

TUs connected as 'guests' will be displayed only in case they are connected. TU that went offline and then up again, might be displayed with different RF port.

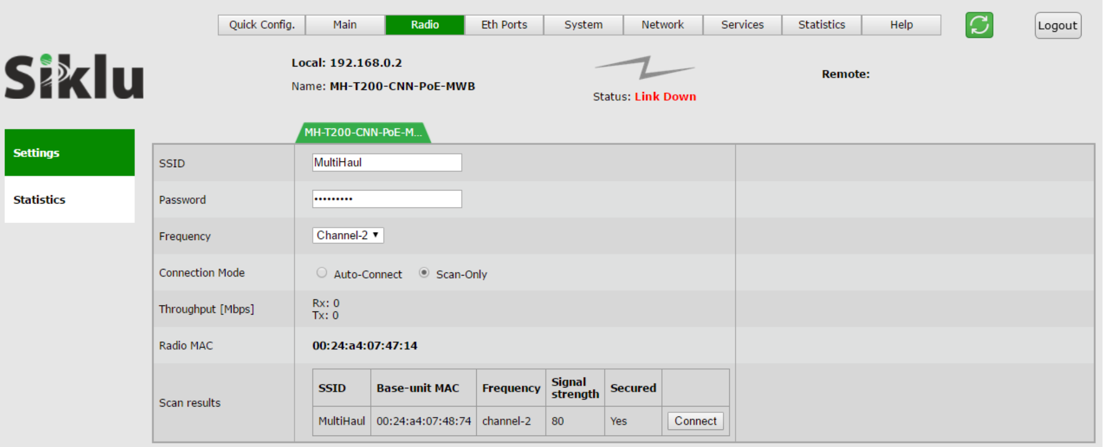
TUs connected as 'managed' will be displayed even if they are down and will not change their RF port.

- Eth Port – name of the RF port that is used for connection. BU: eth-tu1, eth-tu2…eth-tu8. TU: eth-bu1.
- Tx MSC – the Adaptive Modulation & Coding Scheme (A-MCS) which is used to transmit the packets. MCS values: 1 to 8 (MCS 10 for very short links). MCS 0 is used to carry control messages only (no data traffic).
- Signal Quality – the signal's quality indication. Values: 0 to 100.
- RSSI – Receive Signal Strength Indication (in dBm). Available as long as the TU is connected.
- Tx Rate Limiter – User may set rate limiter to limit the data rate on the radio from BU towards the TU. Value in Mbps. Default is 'up-to-TU-license', meaning the rate limiter will be set to the value of the TU data rate license and cannot be set to a higher value even if the BU data rate license is higher.

Note:

The TU's Tx rate Limiter, meaning the max data rate the TU transmits towards the BU is determined by theTU configured configured capacity license (Data Rate set on System->Maintenance->Licensing page).

3.5.3 Scan Results (Terminal Unit Only)



Local: 192.168.0.2
Name: MH-T200-CNN-PoE-MWB
Status: Link Down
Remote:

SSID: MultiHaul
Password: ••••••••••
Frequency: Channel-2 ▾
Connection Mode: ○ Auto-Connect ● Scan-Only
Throughput [Mbps]: Rx: 0 Tx: 0
Radio MAC: 00:24:a4:07:47:14

Scan results

SSID	Base-unit MAC	Frequency	Signal strength	Secured	
MultiHaul	00:24:a4:07:48:74	channel-2	80	Yes	Connect

Figure 3-12 Radio Page: Terminal Scan Results

On “Connection Mode = Scan-only” or when terminal unit is not associated to a base unit (link down), the automatic frequency scan results will be displayed.

It provides the details of the received networks, including SSID, MAC, Frequency and Signal Strength.

By clicking **`Connect`** you will be asked to provide the password and then the link will go up.

3.5.4 TU Auto-Provisioning

The configuration of a TU can be managed and stored in the BU, even when the TU is not connected (example: TU pre-provisioning or replacement). The configuration information is sent to the TU upon (re)connection if the TU is configured to allow remote configuration (“Remote Config” is enabled on System->Settings page).

The auto-provisioning of the TU can be based on TU MAC address or name. The TU name is identical to its serial number by default, and is changeable in the GUI if needed.

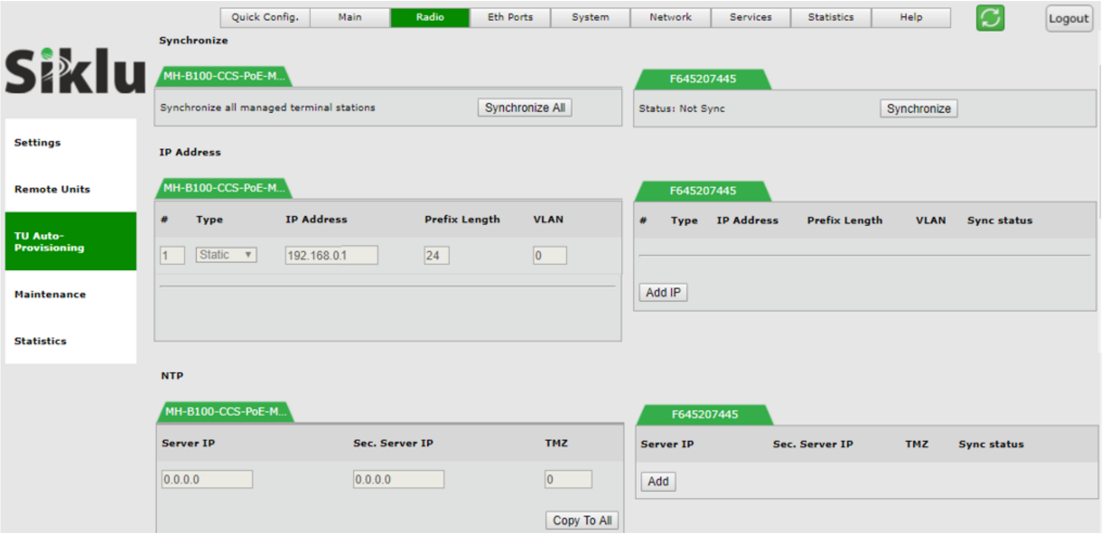
Note: TU Auto-Provisioning is available for managed TUs only.

Configuration received and implemented from the BU will be recorded in the user-activity log under user: admin.

Auto-provisioning of remote TU is available for the following paramets:

- IP Address(es)
- NTP
- Authentication Mode (AAA)
- Ethernet ports

- 802.1x
- PSE
- Bridge
- SNMP Agent
- SNMP Managers



Status: Not Sync

MH-B100-CCS-PoE-M...

#	Type	IP Address	Prefix Length	VLAN
1	Static	192.168.0.1	24	0

F645207445

#	Type	IP Address	Prefix Length	VLAN	Sync status

MH-B100-CCS-PoE-M...

Server IP	Sec. Server IP	TMZ
0.0.0.0	0.0.0.0	0

F645207445

Server IP	Sec. Server IP	TMZ	Sync status

Figure 3-13 Radio Page: TU Auto-Provisioning

To configure Auto-Provisioning:

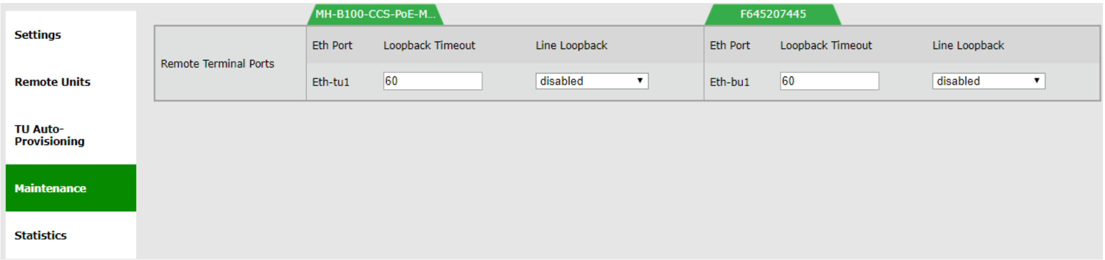
1. Set the TUs to beprovisioned to 'managed' mode.
2. Set the name that the TUs will be identified as (default: TU serial number).
3. Set the attributes and parameters of the remote TUs. Note the settings on the BU side are there to allow you copying them to the TU.
4. Verify TUs configured to accept remote config.
5. Syncronize the configuration.

   By clicking "Synchronize" (one by one for each TU or "Synchronize All"), the settings will be transmitted to the remote TU and executed locally.

The TU will report its auto-provisioning status:

- Sync – running settings received from the BU.
- Not Sync – not running.
- Remote Config Disabled – remote TU is not set to accept config from BU
- Disconnected – TU is disconnected.

3.5.5 Maintenance



	Eth Port	Loopback Timeout	Line Loopback	Eth Port	Loopback Timeout	Line Loopback
Remote Terminal Ports	Eth-tu1	60	disabled	Eth-bu1	60	disabled

Figure 3-14 Radio Page: Maintenance

This section allows monitoring and configuring the following parameters:

- Loopback –enable loopback on the bridge’s RF port. Internal (towards the line side) loopback is available with MAC addresses swap.
- Loopback Timeout – in seconds. Loopback will clear when timeout expires.

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

3.6 Eth Ports Configuration and Monitoring

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

The MultiHaul™ system has up to four fixed Ethernet interfaces:

- **Host** – Internal management interface (relevant for VLAN settings)
- **Eth1** – ODU interface, port 1
- **Eth2** – ODU interface, port 2 (model dependent)
- **Eth3** – ODU interface, port 3 (model dependent)

In addition, RF interfaces are allocated based on the number of units connected.

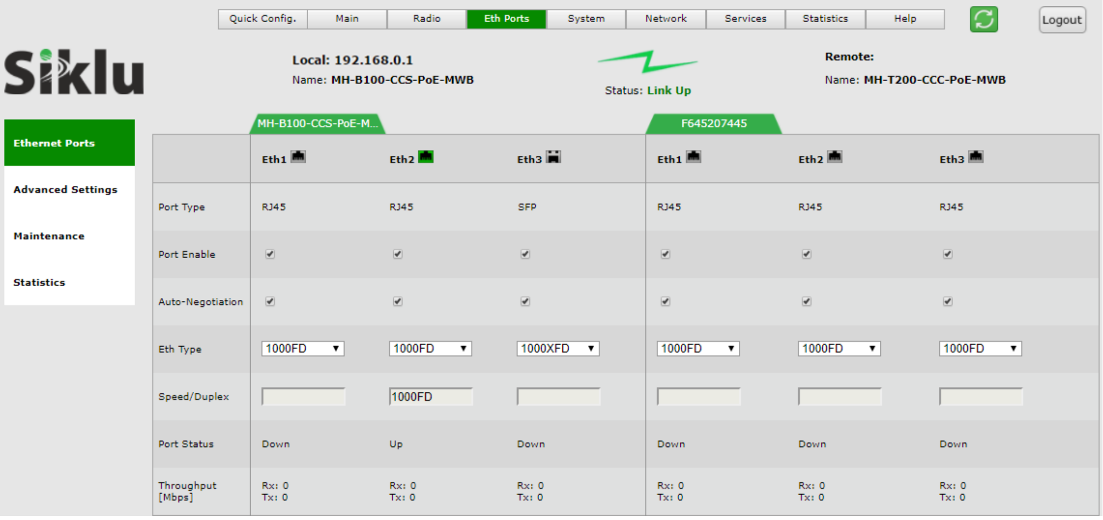
On Base Units, RF interfaces are created when remote TUs are connected or set.

The default Ethernet RF interfaces are named eth-tu1, eth-tu2…eth-tu8. On a Terminal Unit, one RF interface is available. The Ethernet RF interface is named eth-bu1.

This chapter includes the following topics:

- Settings
- Advanced Settings

3.6.1 Settings



Local: 192.168.0.1
Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:
Name: **MH-T200-CCC-PoE-MWB**

	MH-B100-CCS-PoE-M...			F645207445		
	Eth1	**Eth2**	**Eth3**	**Eth1**	**Eth2**	**Eth3**
Port Type	RJ45	RJ45	SFP	RJ45	RJ45	RJ45
Port Enable	☑	☑	☑	☑	☑	☑
Auto-Negotiation	☑	☑	☑	☑	☑	☑
Eth Type	1000FD	1000FD	1000XFD	1000FD	1000FD	1000FD
Speed/Duplex		1000FD				
Port Status	Down	Up	Down	Down	Down	Down
Throughput [Mbps]	Rx: 0 Tx: 0	Rx: 0 Tx: 0	Rx: 0 Tx: 0	Rx: 0 Tx: 0	Rx: 0 Tx: 0	Rx: 0 Tx: 0

Figure 3-15 Eth Ports Page: Settings

This section allows monitoring and configuring the following parameters:

- Port status visual display (Green – port is up).
- Port Type – RJ45 or SFP
- Port Enable – checkbox to enable the port.
- Auto Negotiation – checkbox to enable auto-neg.
- Speed/Duplex – speed (10/100 or 1000) and duplex (half/full) setting:
    - When Auto Negotiation Enabled – R/O field indicating the current speed/duplex
    - When Auto Negotiation Disabled – allows configuring the speed/duplex.
    - R/O field indicating the current speed/duplex (note that for SFP ports, only 1000 speed is available).
- Speed/Duplex (SFP) – 1000XFD (for 1Gbps) or 2500XFD (for 2.5Gbps) SFPs.

3.6.2 Advanced Settings

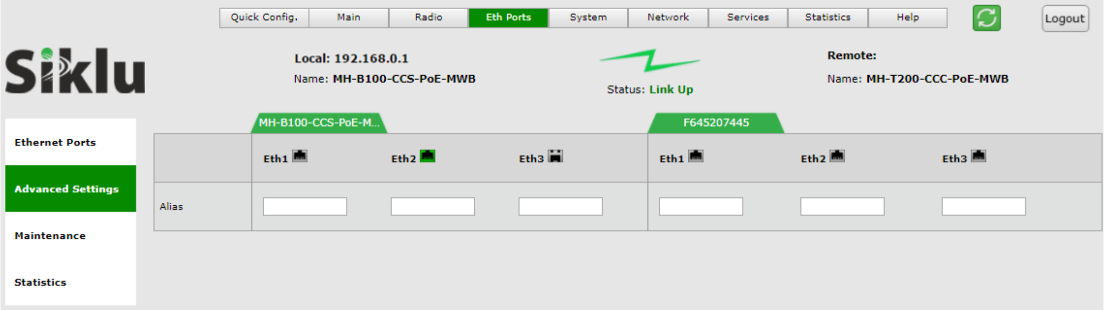
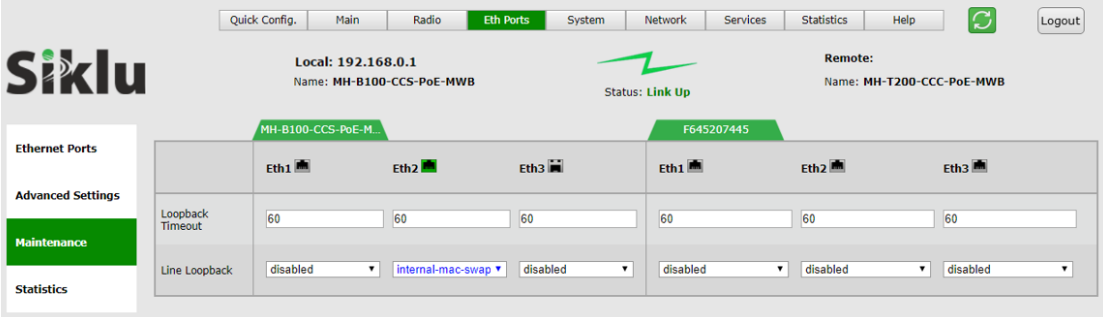


Figure 3-16 Eth Ports Page: Advanced Settings

This section allows monitoring and configuring the following parameters:

- Alias – text field for port.

3.6.3 Maintenance



	Eth1	Eth2	Eth3	Eth1	Eth2	Eth3
Loopback Timeout	60	60	60	60	60	60
Line Loopback	disabled	internal-mac-swap	disabled	disabled	disabled	disabled

Figure 3-17 Eth Ports Page: Maintenance

This section allows monitoring and configuring the following parameters:

- Line Loopback –enable loopback on the port. Internal (towards the radio side) loopback is available with MAC addresses swap.
- Loopback Timeout – in seconds. Loopback will clear when timeout expires.

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

3.7 System Configuration and Monitoring

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

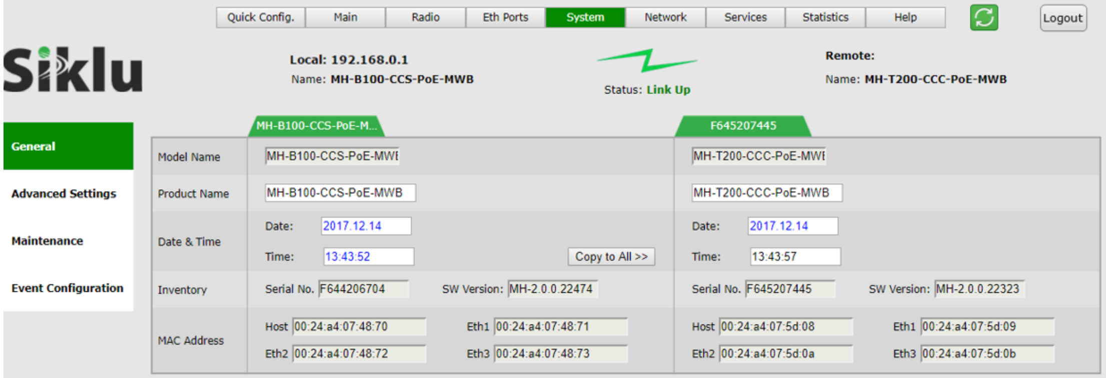
This chapter includes the following topics:

- General Settings
- Advanced Settings
- Maintenance
- Event Configuration

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

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

3.7.1 General Settings



Local: 192.168.0.1
Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:
Name: **MH-T200-CCC-PoE-MWB**

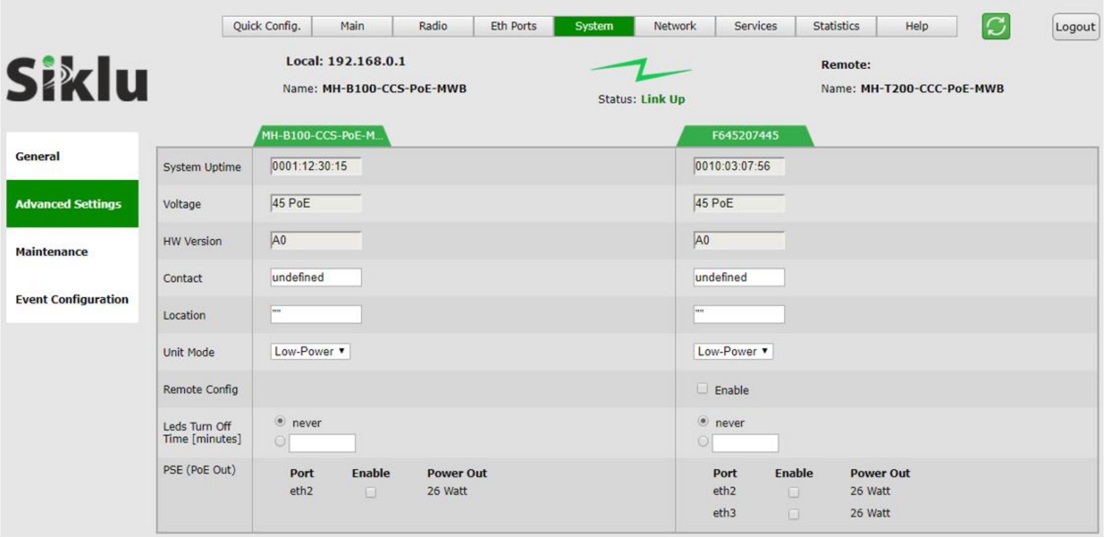
	MH-B100-CCS-PoE-M...	F645207445
Model Name	MH-B100-CCS-PoE-MWI	MH-T200-CCC-PoE-MWI
Product Name	MH-B100-CCS-PoE-MWB	MH-T200-CCC-PoE-MWB
Date & Time	Date: 2017.12.14 Time: 13:43:52	Date: 2017.12.14 Time: 13:43:57
Inventory	Serial No. F644206704 SW Version: MH-2.0.0.22474	Serial No. F645207445 SW Version: MH-2.0.0.22323
MAC Address	Host 00:24:a4:07:48:70 Eth1 00:24:a4:07:48:71 Eth2 00:24:a4:07:48:72 Eth3 00:24:a4:07:48:73	Host 00:24:a4:07:5d:08 Eth1 00:24:a4:07:5d:09 Eth2 00:24:a4:07:5d:0a Eth3 00:24:a4:07:5d:0b

Figure 3-18 System Page: General

This section allows monitoring and configuring the following parameters:

- Model Name – (R/O) Product model.
- Name – Unique name for each system.
- Date & Time – Date [YYYY.MM.DD], Time [HH:MM:SS]
- Inventory – R/O fields. Serial Number and active SW version.
- MAC Address – R/O fields for each port.

3.7.2 Advanced Settings



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

	MH-B100-CCS-PoE-M...	F645207445
System Uptime	0001:12:30:15	0010:03:07:56
Voltage	45 PoE	45 PoE
HW Version	A0	A0
Contact	undefined	undefined
Location	""	""
Unit Mode	Low-Power ▾	Low-Power ▾
Remote Config		☐ Enable
Leds Turn Off Time [minutes]	● never ○	● never ○
PSE (PoE Out)	Port: eth2, Enable: ☐, Power Out: 26 Watt	Port: eth2, Enable: ☐, Power Out: 26 Watt Port: eth3, Enable: ☐, Power Out: 26 Watt

Figure 3-19 System Page: Advanced Settings

This section allows monitoring and configuring the following parameters:

- System Uptime – R/O field. Time elapsed from last power on.
- Voltage – R/O field. Input voltage and indication of PoE input.
- HW Version – R/O field.
- Contact – user configurable info (default – blank).
- Location – user configurable info (default – blank " ").
- Unit Mode – Normal or Low-Power. Use Low-Power for bench testing only, when distance between radios is up to few meters.
- Remote Config (Terminal Unit only) – when enabled, TU will obtain its configuration from the BU (refer to TU Auto-Provisioning feature).
- Leds Turn Off Time – when value entered (in minutes), the radio Leds will turn off automatically after the set time (up to 6000 minutes). To turn on the Leds, reboot the radio. If left blank, Leds will not turn off automatically (default).
- PSE (PoE Out) – for supporting models only.
- Remote Config (Terminal Unit only) – enable auto-provisioning of TUs by BU. Default: Distabled.

3.7.3 Maintenance

3.7.3.1 File Transfer

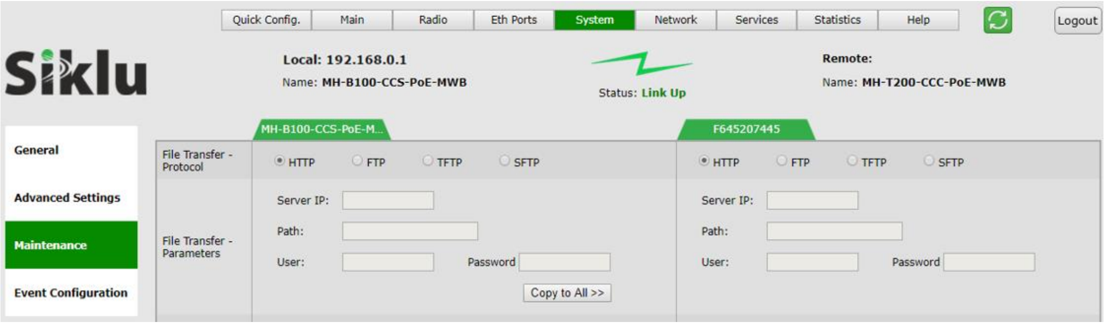


Figure 3-20 System Page: Maintenance – File Transfer

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 anonymous user defined.

Note: The simplest and recommended way to transfer files is using HTTP file transfer.

3.7.3.2 SW Upgrade

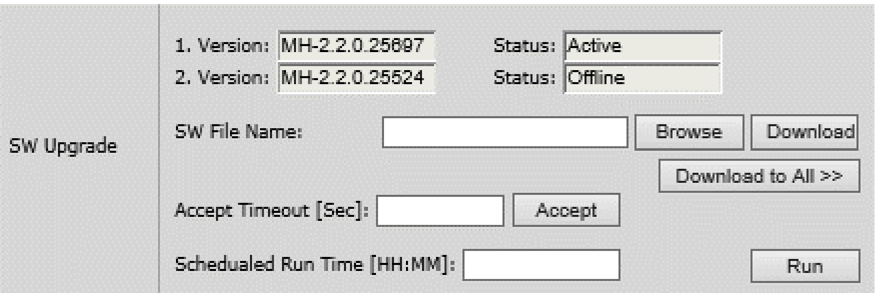

1. Version: MH-2.2.0.25697 Status: Active
2. Version: MH-2.2.0.25524 Status: Offline

Figure 3-21 System Page: Maintenance – SW Upgrade

The 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 (optional).

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

The software may be downloaded 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.
- Scheduled Run Time [HH:MM] – enter time of day (hours:minutes) that the SW upgrade will be performed (and the reboot). Allows sending upgrade command to the radio that will be scheduled to a later hour (maintenance window out of working hours).

  It is important that you set correct system time and date on your network for a scheduled run time.

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

Click **`Upgrade`** to activate the downloaded software. If you have specified time for the upgrade (Scheduled Run Time [HH:MM]), the software will be activated at this time. If you have not specified such time, the downloaded software will be activated immediately.

Note that this action will result in system reboot.

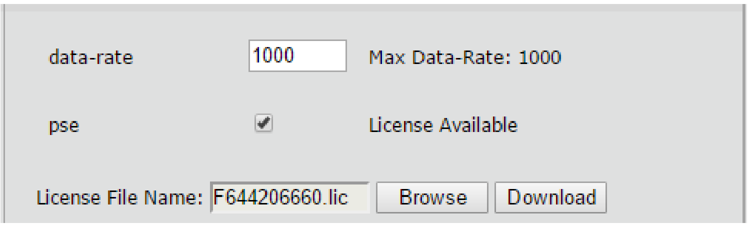
Click **`Accept`** to accept the new SW.

Note:

Always upgrade both sides (all remote Terminal Units).

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

3.7.3.3 Licensing



data-rate: 1000 — Max Data-Rate: 1000

pse: ☑ — License Available

License File Name: F644206660.lic

Figure 3-22 System Page: Maintenance – Licensing

Available licenses:

- Data rate (capacity) – BU: 500Mbps or 1800Mbps, TU: 100Mbps or 1000Mbps).
- PSE – PoE out (13W, 26 or 53W, according to product specs). PSE license available by default.

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 system supports temporary license that is available for 30 days. Once enabled, a countdown timer will run as long as the system is powered up. When timer expires, the system will reboot and come up with data rate /functionality based on the available license.

The temporary license can be enabled/disabled for each license component individually.

Caution: Use temporary license with caution and do not forget to apply permanent license. If the 30 day expire before adding permanent license, link might go down or some essential functionality, controlled by license, will be disabled, what might impair service.

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 **Browse** and **Download** to select and download a new license file. As the license file name is always *<system_serial_number>.lic*, it will be displayed as the License File Name.

The **Permission** field indicates rate/functionality availability based on the license file.

Use the **Config** field to set up the desired rate or to enable/disable functionality.

The **Status** field indicates rate/functionality base on license (Permission), configuration (Config) and temporary license activation.

Note:

Enabling license components will introduce a momentary service disruption.

3.7.3.4 Scripts

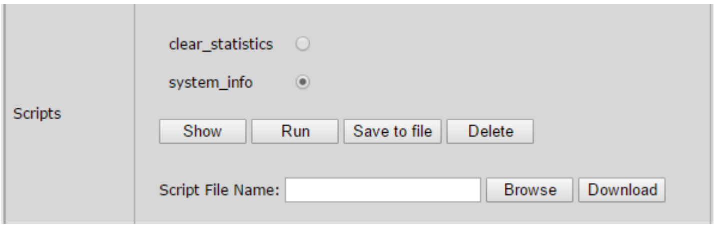


Figure 3-23 System Page: Maintenance – Scripts

The MultiHaul™ 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.

Note:

Whenever contacting Siklu for support, send the output of this script from all 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/*).

3.7.3.5 Configuration Management

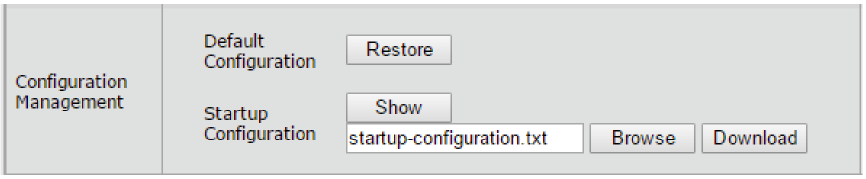


Figure 3-24 System Page: Maintenance – Configuration Management

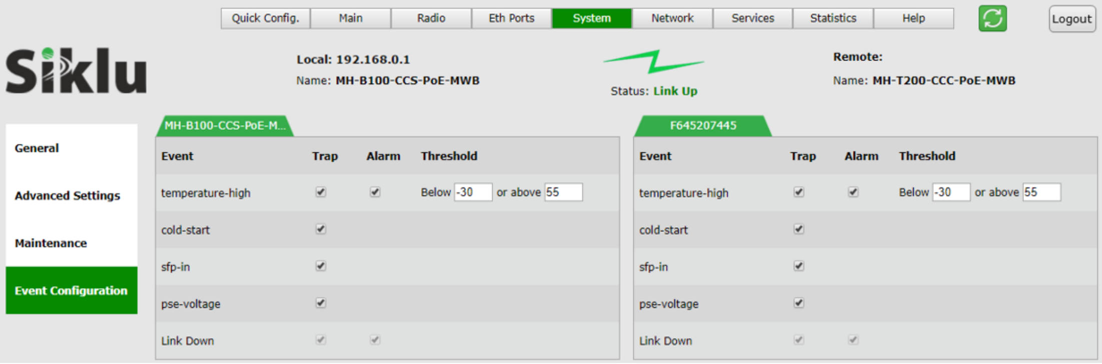
This section allows configuring the following parameters:

- Default Configuration – Click **Restore** to delete current *startup-configuration.txt* file. After reboot, the system will come up with the factory default configuration.
- 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 home directory and will store it in the file system as the new startup-configuration file. After next reboot, the system will come up with the new configuration.

3.7.4 Event Configuration



Event	Trap	Alarm	Threshold
temperature-high	☑	☑	Below -30 or above 55
cold-start	☑		
sfp-in	☑		
pse-voltage	☑		
Link Down	☑	☑	

Event	Trap	Alarm	Threshold
temperature-high	☑	☑	Below -30 or above 55
cold-start	☑		
sfp-in	☑		
pse-voltage	☑		
Link Down	☑	☑	

Figure 3-25 Network Page: Event Configuration

The system 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.

- **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** Some events have configurable thresholds for alarm raise/clear and for sending traps. The threshold hysteresis can be defined (to avoid toggling alarms).

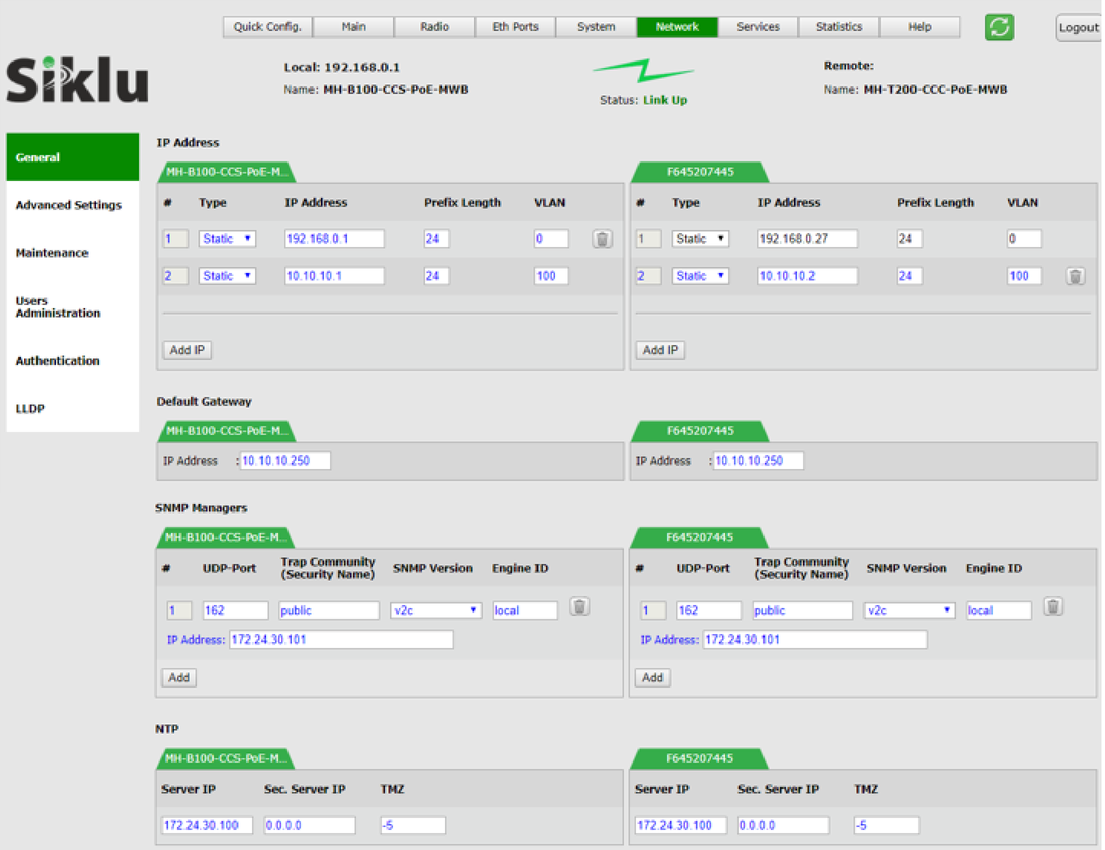
3.8 Network Configuration and Monitoring

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
- Authentication (802.1x)

3.8.1 General Settings



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

IP Address

MH-B100-CCS-PoE-M...

#	Type	IP Address	Prefix Length	VLAN
1	Static	192.168.0.1	24	0
2	Static	10.10.10.1	24	100

F645207445

#	Type	IP Address	Prefix Length	VLAN
1	Static	192.168.0.27	24	0
2	Static	10.10.10.2	24	100

Default Gateway

MH-B100-CCS-PoE-M...

IP Address : 10.10.10.250

F645207445

IP Address : 10.10.10.250

SNMP Managers

MH-B100-CCS-PoE-M...

#	UDP-Port	Trap Community (Security Name)	SNMP Version	Engine ID
1	162	public	v2c	local

IP Address: 172.24.30.101

F645207445

#	UDP-Port	Trap Community (Security Name)	SNMP Version	Engine ID
1	162	public	v2c	local

IP Address: 172.24.30.101

NTP

MH-B100-CCS-PoE-M...

Server IP	Sec. Server IP	TMZ
172.24.30.100	0.0.0.0	-5

F645207445

Server IP	Sec. Server IP	TMZ
172.24.30.100	0.0.0.0	-5

Figure 3-26 Network Page: General

This section allows monitoring and configuring the following parameters:

- IP Address

The system supports up to four IP addresses that can be associated with different VLANs. IP addresses may also be acquired by DHCP.

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

- Default Gateway

When entering the IP of the default gateway, it is translated to a static route (#1). Setting and viewing static routes is available via the Command Line Interface only.

Note that changes to the IP address settings will require reconnecting using the new IP address.

- SNMP Managers

Up to five managers that will receive SNMP traps can be configured (SNMPv2c or SNMPv3).

  - # - Index (1-5)
  - IP Address – Destination IP Address
  - UDP Port – port number for sending traps
  - Security Name (community)
  - SNMP Ver – SNMP version (SNMPv2c or SNMPv3)
  - Engine ID – Used for SNMPv3

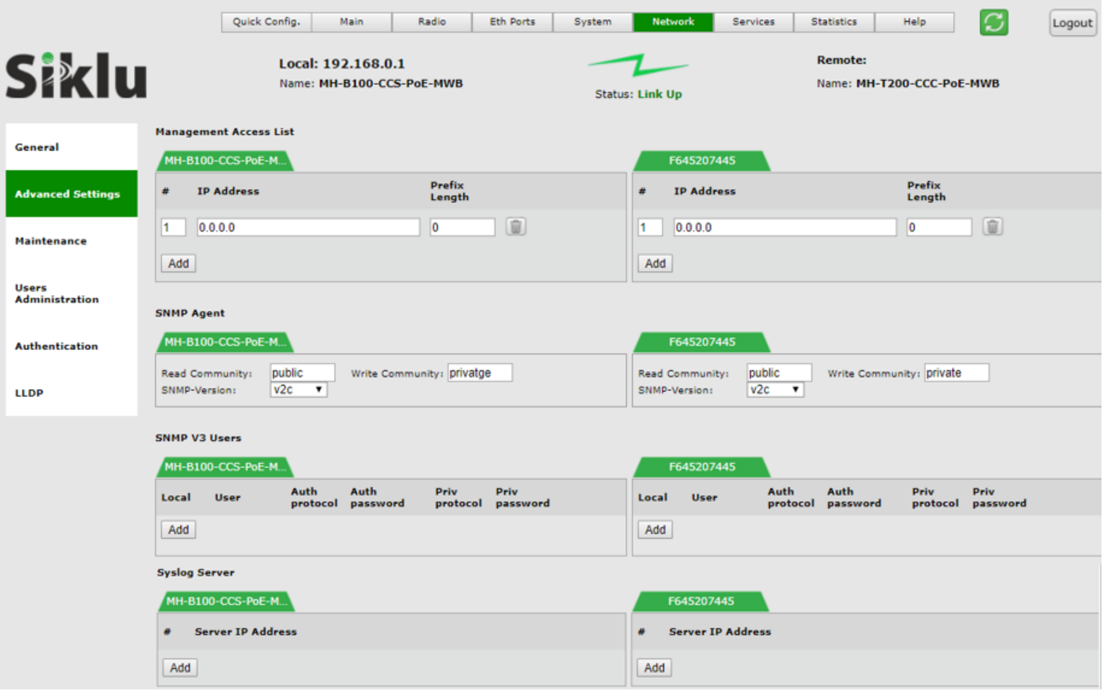
    For SNMPv3 configuration, refer to the *SNMPv3 Users Configuration* section under *System Administration* chapter of this manual.

- NTP

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of network elements over packet-switched, variable-latency data networks. The system 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 defi4ned.

  - 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 displayed.

3.8.2 Advanced Settings



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB
Status: Link Up
Remote:
Name: MH-T200-CCC-PoE-MWB

Management Access List

MH-B100-CCS-PoE-M...

#	IP Address	Prefix Length
1	0.0.0.0	0

F645207445

#	IP Address	Prefix Length
1	0.0.0.0	0

SNMP Agent

MH-B100-CCS-PoE-M...
Read Community: public
Write Community: privatge
SNMP-Version: v2c

F645207445
Read Community: public
Write Community: private
SNMP-Version: v2c

SNMP V3 Users

MH-B100-CCS-PoE-M...

Local	User	Auth protocol	Auth password	Priv protocol	Priv password

F645207445

Local	User	Auth protocol	Auth password	Priv protocol	Priv password

Syslog Server

MH-B100-CCS-PoE-M...

#	Server IP Address

F645207445

#	Server IP Address

Figure 3-27 Network Page: Advanced Settings

This section allows monitoring and configuring the following parameters:

- Management Access List

List of authorized 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.

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

- SNMP Agent

SNMP Agent properties (SNMP passwords).

  - 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.

- SNMPv3 Users

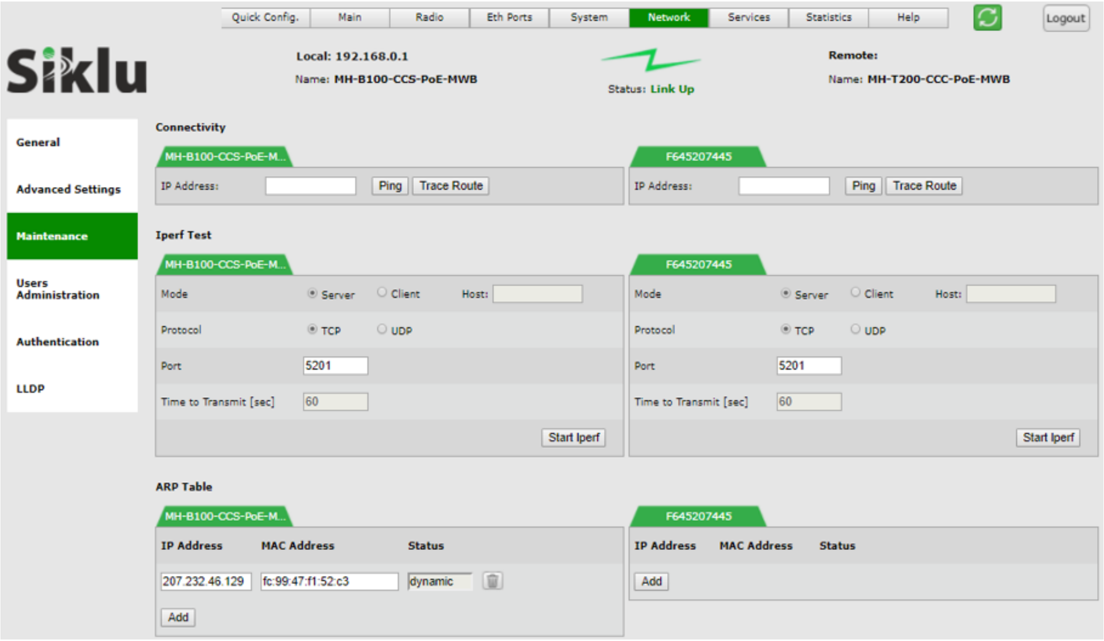
For SNMPv3 configuration, refer to the *SNMPv3 Users Configuration* section under *System Administration* chapter of this manual.

- Syslog Server

When set, all system's event and alarms will be sent to the Syslog server.

Syslog servers listens on Port 514.

3.8.3 Maintenance



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

Connectivity

MH-B100-CCS-PoE-M...
IP Address:

F645207445
IP Address:

Iperf Test

MH-B100-CCS-PoE-M...
Mode: ● Server ○ Client Host:
Protocol: ● TCP ○ UDP
Port: 5201
Time to Transmit [sec]: 60

F645207445
Mode: ● Server ○ Client Host:
Protocol: ● TCP ○ UDP
Port: 5201
Time to Transmit [sec]: 60

ARP Table

MH-B100-CCS-PoE-M...

IP Address	MAC Address	Status
207.232.46.129	fc:99:47:f1:52:c3	dynamic

F645207445

IP Address	MAC Address	Status

Figure 3-28 Network Page: Maintenance

This section allows monitoring and configuring the following parameters:

- Connectivity

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

- Iperf Test

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

  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.

  You may test a cluster of BU and multiple TUs by setting a server on the BU side and independent clients on each TU.

  Pop-up screen will display the results.

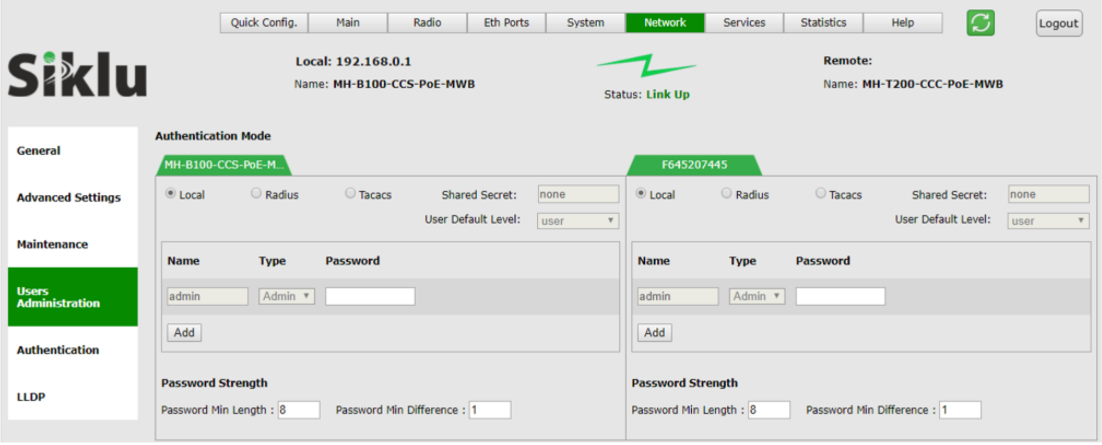
  Typical internal Iperf results are 1.4-1.5 Gbps aggregate (total).

  Remember that max data-rate per TU is 1Gbps.

- 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.

3.8.4 Users Administration



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB
Status: Link Up
Remote:
Name: MH-T200-CCC-PoE-MWB

Authentication Mode

MH-B100-CCS-PoE-M...

● Local ○ Radius ○ Tacacs Shared Secret: none
User Default Level: user

Name	Type	Password
admin	Admin	

Password Strength
Password Min Length : 8 Password Min Difference : 1

F645207445

● Local ○ Radius ○ Tacacs Shared Secret: none
User Default Level: user

Name	Type	Password
admin	Admin	

Password Strength
Password Min Length : 8 Password Min Difference : 1

Figure 3-29 Network Page: Users Administration

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.

This section allows monitoring and configuring the following parameters:

- Users

The system 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 with the different typed. 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/Tacacs configuration, refer to the *Radius/Tatacs Configuration* section under *System Administration* chapter of this manual.

- Password Strength

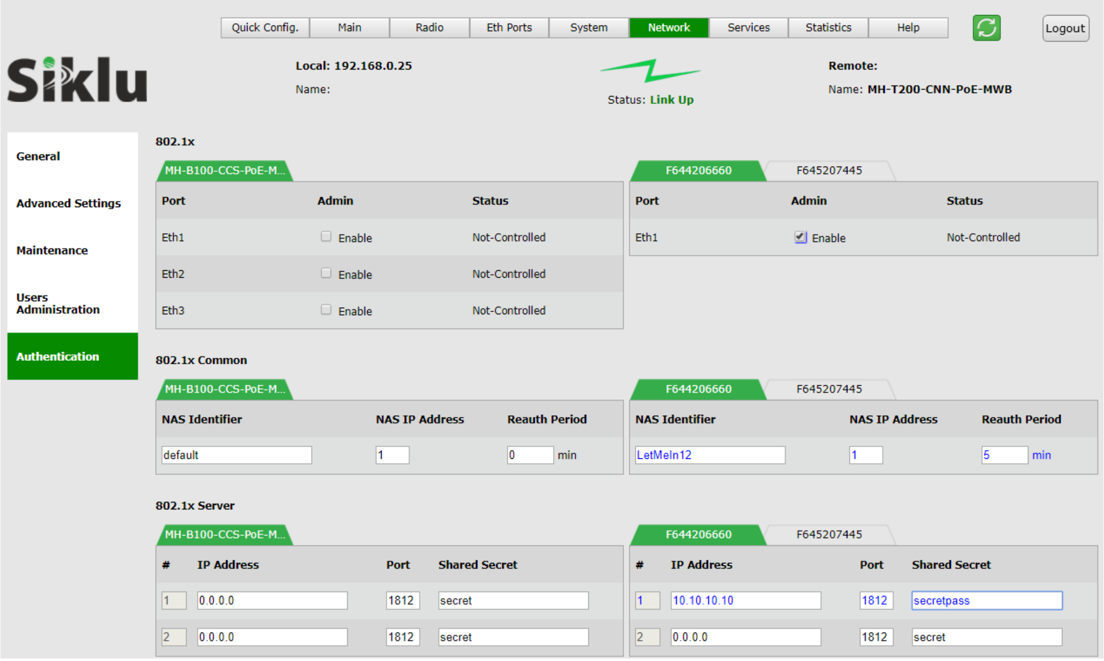
Minimal password requirements for password strength enforcement.

- ○ 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.

3.8.5 Authentication (802.1x)

IEEE 802.1X is an IEEE Standard for port-based Network Access Control. It allows authentication of connected devices with 802.1x server.

Once enabled on a TU line port, the radio will block the port unless the device connected to the port (supplicant) sends 802.1x connection requests that can be validate on the 802.1x authentication server.



Local: 192.168.0.25
Name:

Status: Link Up

Remote:
Name: MH-T200-CNN-PoE-MWB

802.1x

MH-B100-CCS-PoE-M...

Port	Admin	Status
Eth1	☐ Enable	Not-Controlled
Eth2	☐ Enable	Not-Controlled
Eth3	☐ Enable	Not-Controlled

F644206660 | F645207445

Port	Admin	Status
Eth1	☑ Enable	Not-Controlled

802.1x Common

MH-B100-CCS-PoE-M...

NAS Identifier	NAS IP Address	Reauth Period
default	1	0 min

F644206660 | F645207445

NAS Identifier	NAS IP Address	Reauth Period
LetMeIn12	1	5 min

802.1x Server

MH-B100-CCS-PoE-M...

#	IP Address	Port	Shared Secret
1	0.0.0.0	1812	secret
2	0.0.0.0	1812	secret

F644206660 | F645207445

#	IP Address	Port	Shared Secret
1	10.10.10.10	1812	secretpass
2	0.0.0.0	1812	secret

Figure 3-30 Network Page: Authentication (802.1x)

802.1x Settings and Status

- Enable the port you want to authenticate.
- Status: (R/O) Not-controlled (disabled), Controlled-Opened (managed and traffic port is opened, meaning authentication performed successfully). Controlled-Closed (managed and traffic port is closed, meaning authentication not performed or failed).

802.1x Common Settings

This information will be sent to the authenticator when 802.1x packets received.

- NAS Identifier – Identifier of the authenticator.
- NAS IP Address – IP index (1 to 4) to identify the IP address (one of the 4 IP addresses of the radio) the authentication request will use.
- Reauth Period – (minutes). Re-authentication period. If other than 0, the radio will perform re-authentication every set number of minutes and will close the port if authentication fails.

  If value is set to 0, the port will remain open after a successful authentication till the next reboot of the radio.

802.1x Server

Up to 2 authentication servers can be defined.

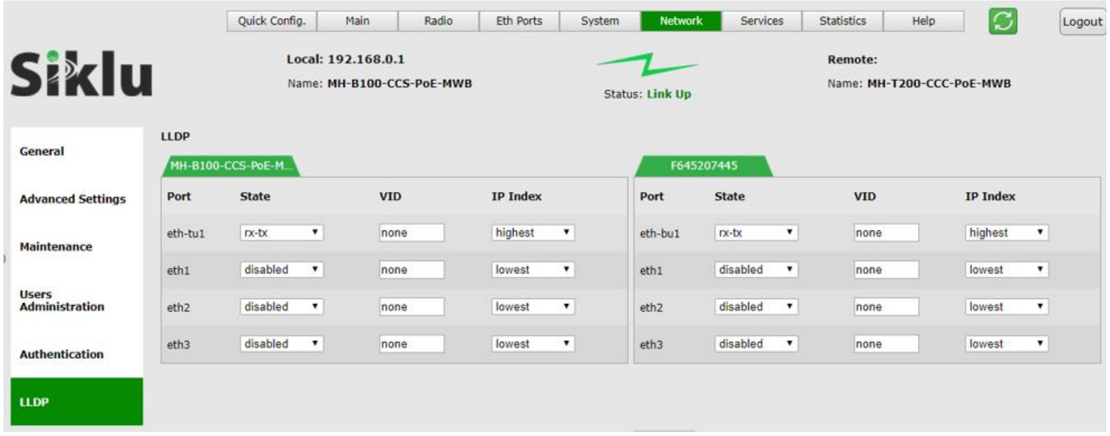
- IP Address – of the authentication server.
- Port – Port number to be used (default 1812).
- Shared Secret – password for the authentication.

3.8.6 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 radio to discover other network elements that are connected to it, including the discovery of third-party network elements, and enables easier integration of MultiHaul™ links in an LLDP supported networks.



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

LLDP

MH-B100-CCS-PoE-M...

Port	State	VID	IP Index
eth-tu1	rx-tx	none	highest
eth1	disabled	none	lowest
eth2	disabled	none	lowest
eth3	disabled	none	lowest

F645207445

Port	State	VID	IP Index
eth-bu1	rx-tx	none	highest
eth1	disabled	none	lowest
eth2	disabled	none	lowest
eth3	disabled	none	lowest

Figure 3-31 Network Page: LLDP (Configuration)

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

To configure LLDP

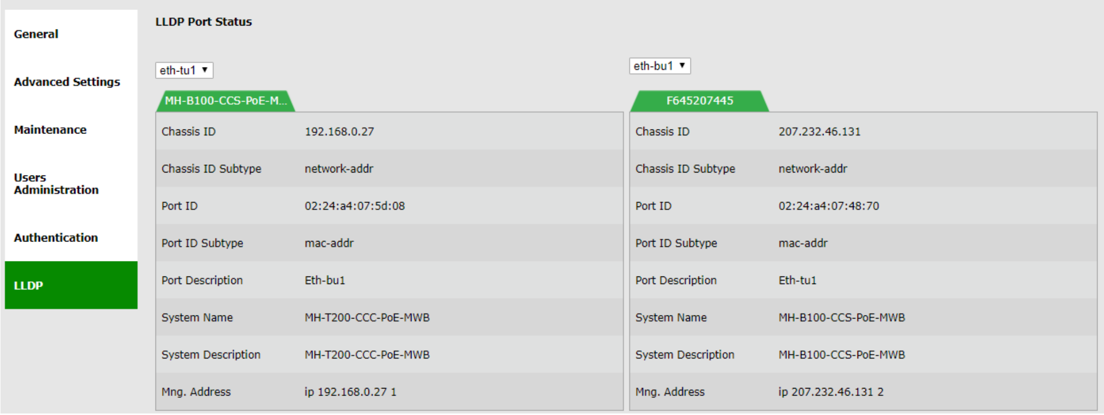
- Port – Eth1-Eth3, Eth-tu1…
- Admin – enabling LLDP on the port. Select **rx-tx** to enable LLDP. Note that you may work with uni-directional LLDP by selecting **rx** or **tx** only.
- VID – VLAN ID that LLDP messages will be sent on. Default is **none** (untagged).
- IP Index – Lowest, Highest or IP index (1-4). The IP address the system will respond with in the LLDP information reply. Default is **Lowest**.

Note:

By default, LLDP is disabled on the radio port and on all line Ethernet ports).

When LLDP is disabled on all ports (including radio ports), LLDP packets will pass transparently over the radio.

To monitor LLDP status



LLDP Port Status

eth-tu1

MH-B100-CCS-PoE-M...

Chassis ID	192.168.0.27
Chassis ID Subtype	network-addr
Port ID	02:24:a4:07:5d:08
Port ID Subtype	mac-addr
Port Description	Eth-bu1
System Name	MH-T200-CCC-PoE-MWB
System Description	MH-T200-CCC-PoE-MWB
Mng. Address	ip 192.168.0.27 1

eth-bu1

F645207445

Chassis ID	207.232.46.131
Chassis ID Subtype	network-addr
Port ID	02:24:a4:07:48:70
Port ID Subtype	mac-addr
Port Description	Eth-tu1
System Name	MH-B100-CCS-PoE-MWB
System Description	MH-B100-CCS-PoE-MWB
Mng. Address	ip 207.232.46.131 2

Figure 3-32 Network Page: LLDP (Port Status)

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.

3.9 Services Configuration and Monitoring

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

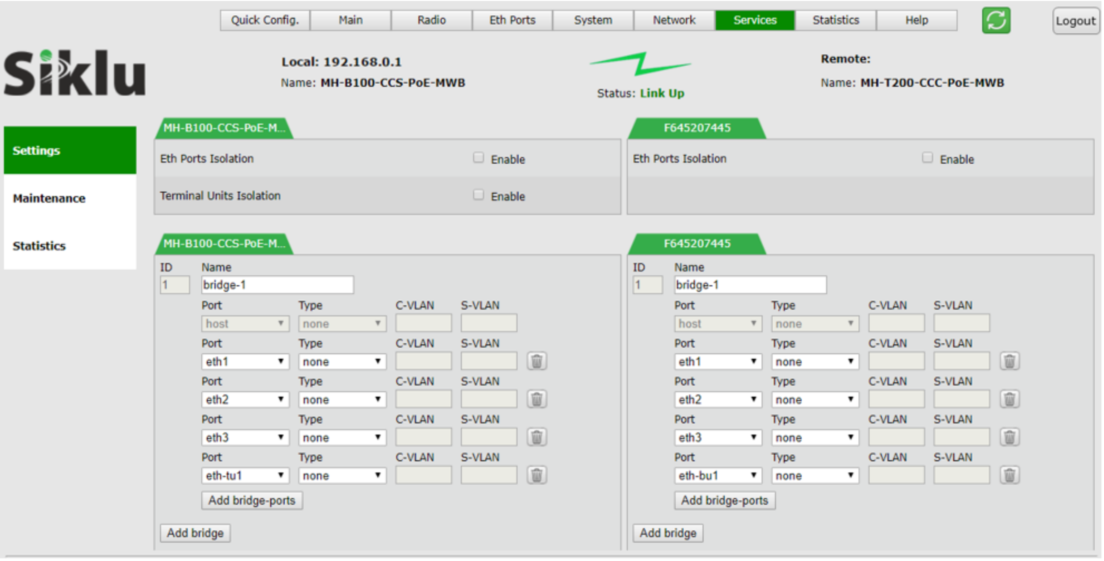
The bridge architecture of the MultiHaul™ radios allows defining 802.1q and 802.1ad services, including adding VLAN, removing VLANs and VLAN translation.

Up to 100 bridges can be defined and ports (line ports and radio ports) may be attached to the bridge as customer port (C-VLAN), provider port (S-VLAN) or Provider Bridge port (Q-in-Q).

Ports may be added, deleted or edited on specific bridges.

Bridge port types:

- None – all traffic, regardless of VLANs.
- C-VLAN – traffic with single C-VLAN (customer port)
- S-VLAN – traffic with single S-VLAN (provider port)
- Q-in-Q – traffic with C-VLAN and S-VLAN



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

MH-B100-CCS-PoE-M...

Eth Ports Isolation ☐ Enable
Terminal Units Isolation ☐ Enable

F645207445

Eth Ports Isolation ☐ Enable

MH-B100-CCS-PoE-M...

ID: 1 Name: bridge-1

Port	Type	C-VLAN	S-VLAN
host	none		
eth1	none		
eth2	none		
eth3	none		
eth-tu1	none		

F645207445

ID: 1 Name: bridge-1

Port	Type	C-VLAN	S-VLAN
host	none		
eth1	none		
eth2	none		
eth3	none		
eth-bu1	none		

Figure 3-33 Services Page: Settings

Important notes:

1) Traffic egressing a tagged port (C-VLAN, S-VLAN or Q-in-Q) that came in from a port set to None, the C/S VLAN is added on top of any existing VLAN.
2) Once bridge-port created user can modify its ether-type: C-VLAN/S-VLAN and its pcp-priority (P-bit override).
3) Each bridge-port can participate only in one bridge.

4) Each bridge has separate forwarding-database.
5) Bridge #1 is dedicated for the Host (management) configuration and cannot be deleted. There is no need to define management VLAN on the bridge itself. You do that by adding VLAN on the IP address settings.

3.9.1 Global Settings

- Terminal units Isolation – when checked, packets coming from one TU and received by BU will not be transmitted to any other TU, isolation the traffic of each TU from neighboring TUs.
- Eth Ports Isolation – when checked, packets coming from one port of the radio will not be transmitted to any other ports of the TU (only towards the radio ports and the management host), isolation the traffic of each Eth port from other Eth ports.

Note:

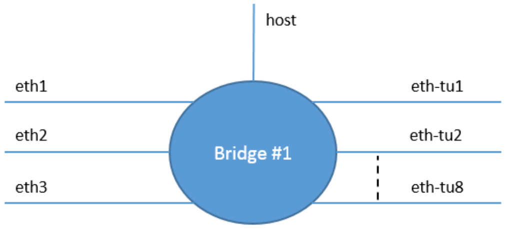
Enabling "Terminal Units Isolation" or "Eth Ports Isolation" will override bridge configuration.

3.9.2 Bridge Models

- **Default Bridge (Transparent)**

The default bridge (bridge #1) implements IEEE 802.1d Transparent Bridge. In this mode, all traffic (both tagged and untagged) is transparently forwarded between all ports and over the radio ports.

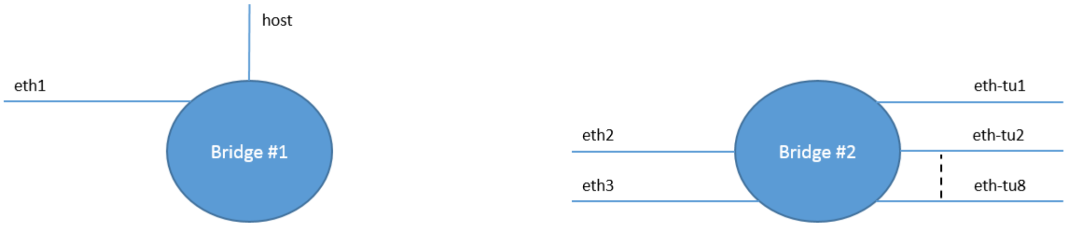
Use the default bridge configuration if you have no intention to restrict management to specific port (aka out-of-band management) or allow specific VLANs on ports.



- **Out-of-Band Management**

For cases where you want to restrict management to a specific port without carrying it over the radio.

In this example Bridge #1 will be used for management coming from port eth1and second bridge will be created to carry the traffic of the other ports (transparent bridge between all ports but eth1 and host).

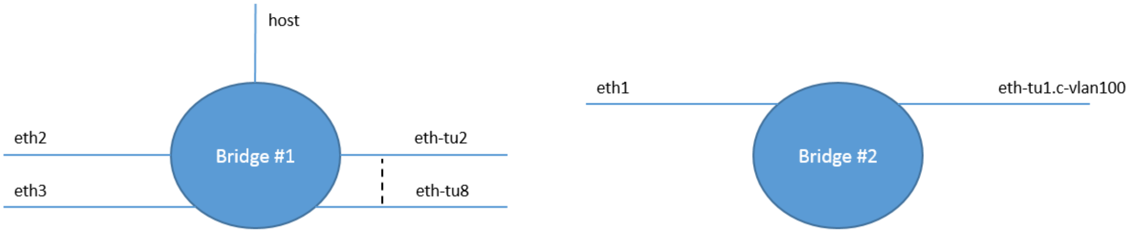


- **Access Port to Customer Port (PVID)**

For cases where you want to add C-VLAN to all traffic coming from specific port and carry it to specific radio interface.

In this example Bridge #2 will be used to tag all incoming traffic from port eth1 and transmitted with C-VLAN 100 over eth-tu1 radio interface.

Bridge #1 will implement transparent bridge on all other ports (transparent bridge between all ports but eth1 and eth-tu1).

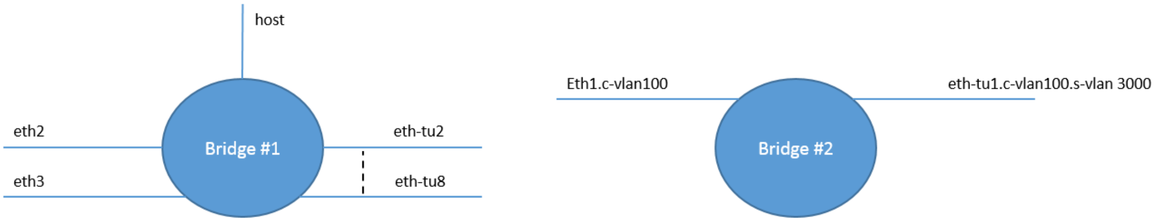


- **Customer Port to Provider Port**

For cases where you want to add S-VLAN to traffic coming from specific port with specific C-VLAN and carry it to specific radio interface.

In this example Bridge #2 will be used to tag incoming traffic with C-VLAN 100 from port eth1 and transmitted with additional S-VLAN 3000 over eth-tu1 radio interface.

Bridge #1 will implement transparent bridge on all other ports (transparent bridge between all ports but eth1 and eth-tu1).

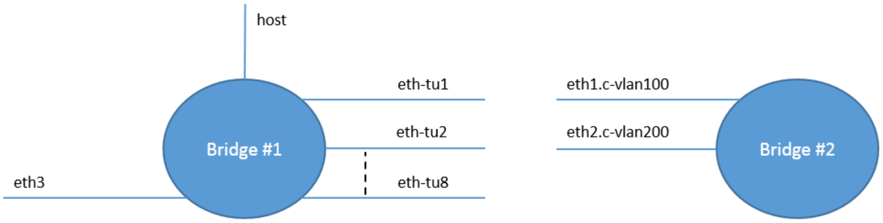


- **VLAN Translation**

For cases where you want to translate incoming VLAN to another VLAN.

In this example Bridge #2 will be used to translate incoming traffic with C-VLAN 100 from port eth1 and transmitted with C-VLAN 200 over port eth2 (and vice-versa).

Bridge #1 will implement transparent bridge on all other ports (transparent bridge between all ports but eth1 and eth2).



- **Terminal Unit Isolation**

For cases where you would like to separate the traffic of different terminal units using VLANs as services in your network are tagged, per user, with different VLANs.

To achieve this goal, a VLAN and a dedicated bridge is configured. Such VLAN will continue to the network and should be terminated/manipulated by customer's network switches/routers.

Note:

Remember that you can enable "Terminal Units Isolation" (System -> Advanced Settings) to separate (isolate) traffic coming from different terminal units.

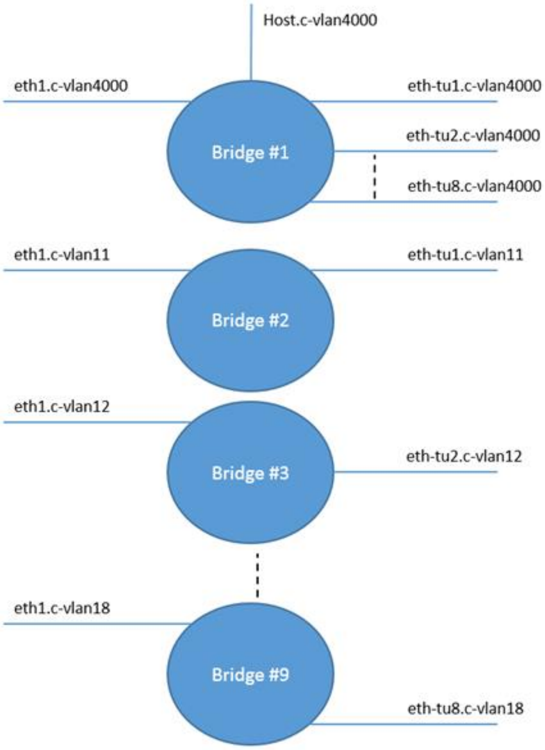
If enables, "Terminal Units Isolation" overrides any bridge configuration.

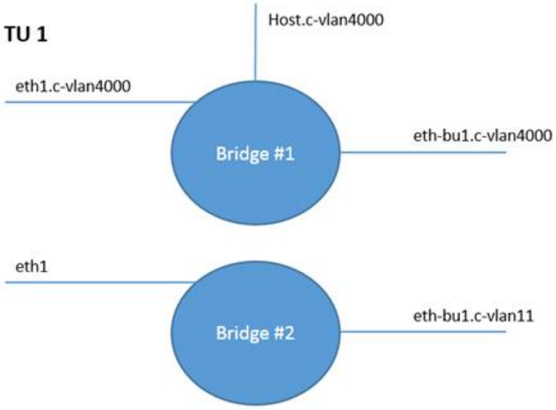
In this example management is carried throughout the network over C-VLAN 4000. TUs 1 to 8 will be tagged with VLAN 11 to 18 respectively. End user's traffic at each TU will remain untagged.

On the BU side, Bridge #1 will be used for management coming from port eth1 over C-VLAN 4000 and will egress with this VLAN to all terminal units and the host.

A separate bridge (Bridges #2 to 9) will be defined to carry VLANs 11 to 18 to the respective terminal units. The reason separate bridge is defined for each VLAN is to assure separation between traffic coming from different TUs.

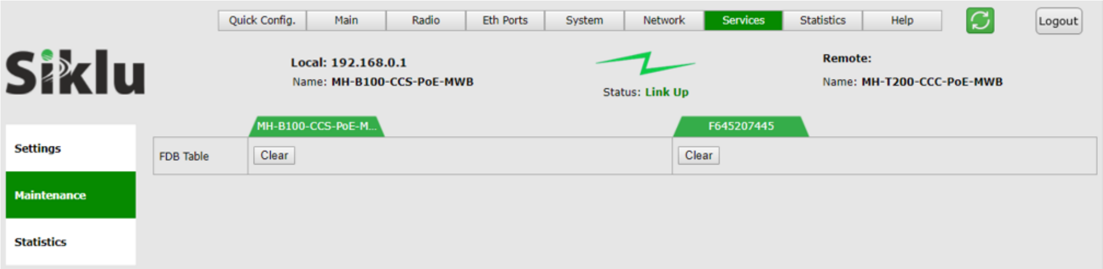
On the terminal unit side, two bridges will be used. Bridge #1 to carry management over C-VLAN 4000. Bridge #2 will be used to tag all other traffic coming on port eth1 on the relevant C-VLAN (C-VLAN 11 for TU 1, up to C-VLAN 18 to TU 8).

<table>
<tr><th>Base Unit</th><th>Terminal Units</th></tr>
<tr><td>


</td><td>


</td></tr>
</table>

3.9.3 Maintenance



Local: 192.168.0.1
Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:
Name: **MH-T200-CCC-PoE-MWB**

Figure 3-34 Services Page: Maintenance

- FDB Table

  Click **Clear** to clear all MAC entries in the Forwarding Database tables.

4 Setup and Monitoring Using the Command Line Interface

This chapter explains how to perform basic configuration tasks using the Command Line Interface (CLI).

The CLI provides 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 1000FD

show eth all statistics
```

- Typical commands:

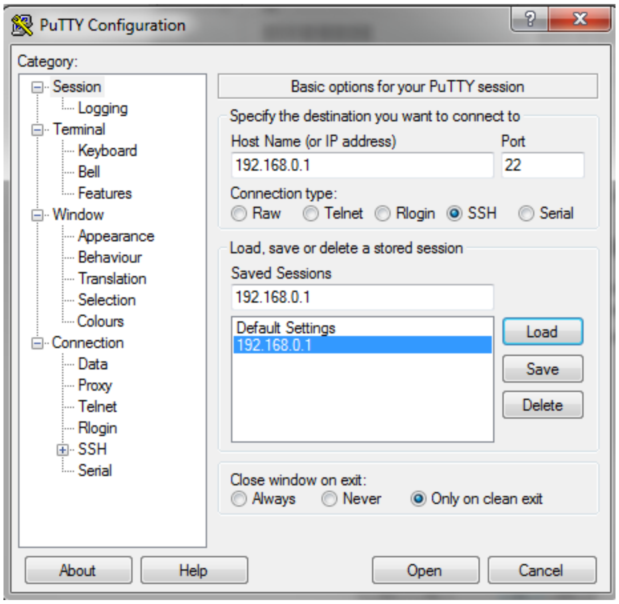
```
Set, show, clear, reset, run, copy
```

- 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.

4.1 Establishing a CLI Session with the ODU

1. Launch 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`.



Host Name (or IP address): 192.168.0.1
Port: 22
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial
Saved Sessions: 192.168.0.1
Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 4-1 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.

3. When prompted, enter the username and password. Default: `admin` and `admin`.

```
login as: admin
MH, S/N: F626500012, Ver:  MH-1.0.0 20211
admin@192.168.0.1's password:
```

4.2 General Configuration Commands: Save, Reset, Rollback

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

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

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

```
Local_Site> reset system
```

Rollback is 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 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.

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

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

4.3 Configuring and Displaying System Information Using the CLI

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

```
Local_Site>show system

MH-B100-CCS-PoE-MWB>show system
system description               : MH-B100-CCS-PoE-MWB
system snmpid                    : .1.3.6.1.4.1.31926
system uptime                    : 0000:01:17:44
system contact                   : undefined
system name                      : MH-B100-CCS-PoE-MWB
system location                  : ""
system voltage                   : 45 poe
system temperature               : 36
system date                      : 2017.12.06
system time                      : 11:40:12
system cli-timeout               : 15
system loop-permission           : enabled
system terminal-units-isolation  : disable
system eth-ports-isolation       : disable
system unit-mode                 : normal
system remote-config             : disable
system leds-turn-off             : never
```

- Description – model description (R/O).
- SnmpID – SNMP ID for Siklu products (R/O).
- Uptime – R/O field. Time elapsed from last power on.
- Contact – text string.
- Name – text string. Enter a unique name to identify your system.

- Location – text string.
- Voltage – input voltage and indication DC or PoE (R/O).
- Temperature – system temperature in C⁰ (R/O).
- Date & Time – Date [YYYY.MM.DD], Time [HH:MM:SS]
- Cli-timeout – timeout for auto-logoff.
- Loop Permission – control the permission to perform system loopbacks.
- Terminal units Isolation (Base Unit only) – when checked, packets coming from one TU and received by BU will not be transmitted to any other TU, isolation the traffic of each TU from neighboring TUs.
- Eth Ports Isolation – when checked, packets coming from one port of the radio will not be transmitted to any other ports of the TU (only towards the radio ports and the management host), isolation the traffic of each Eth port from other Eth ports.
- Unit Mode – Normal or Low-Power. Use Low-Power for bench testing only, when distance between radios is up to few meters. Default: Normal.
- Remote Config (Terminal Unit only) – enable auto-provisioning of TUs by BU. Default: Distabled.
- Leds Turn Off Time – when value entered (in minutes), the radio Leds will turn off automatically after the set time (up to 6000 minutes). To turn on the Leds, reboot the radio. If left blank, Leds will not turn off automatically (default).

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

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

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

```
Local_Site> set system date 2017.12.13 time 15:08:00
```

4.4 Configuring System IP Addresses Using the CLI

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

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

- IP Address – 192.168.0.1
- IP network Prefix – 24

- VLAN – 0 (not defined)
- Default Gateway – 0.0.0.0 (by default, no route is defined).

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

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

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

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

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

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

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

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

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

For example:

```
Local_Site>show ip

ip 1 ip-addr                : 192.168.0.11
ip 1 prefix-len             : 24
ip 1 vlan                   : 0
ip 1 default-gateway        : 0.0.0.0
```

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

```
clear ip <index>
```

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

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

idx   number 1 to 10

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

By default, no route is defined.

To set a static route, use the following command:

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

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

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

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

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

4.5 RF Settings and Provisioning

4.5.1 Base Unit Setup

Use the `show base-unit` command, to display the RF settings of the Base-Unit.

Use the `set base-unit` command, to set the RF settings of the Base-Unit.

```
Local_Site>show base-unit

base-unit self-mac                   : 00:24:a4:07:48:74
base-unit ssid                       : MultiHaul
base-unit password                   : MultiHaul
base-unit frequency                  : channel-2
base-unit access-control             : by-name
base-unit guest-connection           : enable
base-unit max-terminal-units         : 8
base-unit tx-throughput              : 0
base-unit rx-throughput              : 0
```

- Self-mac – Base Unit's MAC address
- SSID – Service Set Identifier (SSID) of the access point (base-unit). Default: MultiHaul. The BU broadcasts openly its SSID.
- Password – base-unit password used for connection. Default: MultiHaul.
- Frequency – the channel number (channel2 or 3). Default: channel-2.
- Access-control –By-MAC (default) or By-Name. determines if TUs are identified by MAC address or by configured name. Relevant for TU auto-provisioning by BU feature.
- Guest-connection – determines if guest (unmanaged) terminals can be associated with the base unit. If guest-connection is enabled, any TU with the correct SSID and password can connect to the BU.
- Max-terminal-units – max number of TUs that can be connected to the BU (1 to 8). Default: 8 (max).

4.5.2 Terminal Unit Setup

Use the **`show terminal-unit`** command, to display the RF settings of the Terminal-Unit.

Use the **`set terminal-unit`** command, to set the RF settings of the Terminal-Unit.

```
TU1> show terminal-unit

terminal-unit self-mac                   : 00:24:a4:07:47:14
terminal-unit ssid                       : MultiHaul
terminal-unit password                   : MultiHaul
terminal-unit connection-mode            : auto-connect
terminal-unit name                       : F644206660
terminal-unit status                     : connected
terminal-unit frequency                  : channel-2
terminal-unit base-unit mac              : 00:24:a4:07:48:74
terminal-unit tx-mcs                     : 8
terminal-unit rssi                       : -52
terminal-unit signal-quality             : 95
terminal-unit tx-throughput              : 0
terminal-unit rx-throughput              : 0
terminal-unit connect-time               : 0000:01:26:03
```

- Self-mac – Terminal Unit's MAC address

- SSID – Service Set Identifier (SSID) of the Terminal Unit that is used for connection with the Base Unit. Default: MultiHaul.
- Password – base-unit password used for connection. Default: MultiHaul.
- Connection-mode – auto connect or scan-only. Default: auto-connect.
    - Auto connect – TU will connect automatically to BU in case SSID/password match.
    - Scan only – TU will scan and present all visible BUs (without connecting to any of them, even if SSID/password match).
- Name - text string representing the name of the TU as it will be identified by the BU. Default: Serial Number of the TU.
- Status (R/O) – connection status: connected (in case of association to a BU) or scanning (if not associated to a BU).
- Frequency (R/O) – the channel frequency the TU is locked on (determined by the BU).
- Base-unit-mac – the MAC address of the BU connected.
- Tx-mcs – the Adaptive Modulation & Coding Scheme (A-MCS) which is used to transmit the packets. MCS values: 1 to 8 (MCS 10 for very short links). MCS 0 is used to carry control messages only (no data traffic).
- RSSI – Receive Signal Strength Indication (in dBm). Available as long as the TU is connected.
- Signal-quality – the signal’s quality indication. Values: 0 to 100.
- Tx-throughput – the transmitted throughput over the RF interface (in Mbps).
- Rx-throughput – the received throughput over the RF interface (in Mbps).
- Connect-time – time the TU is connected to the BU since last disconnection.

4.5.3 Remote Terminal Units Setup and Monitoring

From the Base Unit you can provision the connected Terminal Units.

Use the **`show remote-terminal-unit`** command, to display the RF settings of the connected TUs (1 to 8) and their settings.

Use the **`set remote-terminal-unit`** command, to set the RF settings of the connected TUs.

```
BU> show remote-terminal-unit

remote-terminal-unit 1 eth-port              : eth-tu1
remote-terminal-unit 1 mac                   : 00:24:a4:07:47:14
remote-terminal-unit 1 name                  : F644206660
```

```
remote-terminal-unit 1 status                : connected
remote-terminal-unit 1 association           : guest
remote-terminal-unit 1 tx-mcs                : 8
remote-terminal-unit 1 rssi                  : -52
remote-terminal-unit 1 signal-quality        : 95
remote-terminal-unit 1 tx-rate-limiter        : up-to-license
remote-terminal-unit 1 rem-tx-rate-limiter    : 300
remote-terminal-unit 1 connect-time          : 0000:01:32:46
```

- Eth-port – name of the RF port that is used to connect to the TU.
- Mac – MAC address of the remote TU.
- Name – text string. Set the name of the remote TU. Default: S/N of the remote TU.
- Status (R/O) – connection status: connected (in case of association to a BU) or scanning (if not associated to a BU).
- Association – guest or managed.
    - Guest – TUs that are connected as ‘guest’ do not require setting on the BU side. An RF port will be created in case TU is connected.

      No services configuration is supported for ‘guest’ TUs (transparent bridge only).
    - Managed – TUs that are set to ‘managed’ reserve their RF port settings and will allow settings of services.

Note: TUs connected as ‘guests’ will be displayed only in case they are connected.

TUs connected as ‘managed’ will be displayed even if they are down.

- Tx-mcs – the Adaptive Modulation & Coding Scheme (A-MCS) which is used to transmit the packets. MCS values: 1 to 8 (MCS 10 for very short links). MCS 0 is used to carry control messages only (no data traffic).
- RSSI – Receive Signal Strength Indication (in dBm). Available as long as the TU is connected.
- Signal-quality – the signal’s quality indication. Values: 0 to 100.
- Tx Rate Limiter – User may set rate limiter to limit the data rate on the radio from BU towards the TU. Value in Mbps. Default is ‘up-to-TU-license’, meaning the rate limiter will be set to the value of the TU configured capacity license (Data Rate set on System->Maintenance->Licensing page).
- Rem-Tx-Rate-Limiter (R/O) – the value of the Tx rate limiter at the remote TU.
- Connect-time – time the TU is connected to the BU since last disconnection.

4.6 Configuring Ethernet Interfaces Using the CLI

The MultiHaul™ radio has up to four fixed Ethernet interfaces:

- **Host** – Management interface
- **Eth1** – ODU interface, port 1
- **Eth2** – ODU interface, port 2
- **Eth3** – ODU interface, port 3

On Base Units, RF interfaces are created when remote TUs are connected or set.

The Ethernet RF interfaces are named Eth-tu1, Eth-tu2…Eth-tu8.

On a Terminal Unit, RF interfaced is available. The Ethernet RF interface is named Eth-bu1.

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

4.6.1 Displaying Interface Status

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

The following is an example of an Ethernet interface (Eth1) status display.

```
Local_Site> show eth eth1

eth eth1 description            : Eth 1
eth eth1 mtu                    : 16384
eth eth1 mac-addr               : 00:24:a4:07:48:71
eth eth1 admin                  : up
eth eth1 operational            : up
eth eth1 last-change            : 0001:03:04:34
eth eth1 name                   : Eth1
eth eth1 alias                  :
eth eth1 eth-type               : 1000fd
eth eth1 eth-act-type           : 1000fd
eth eth1 auto-neg               : enabled
eth eth1 loopback-mode          : disabled
eth eth1 loopback-timeout       : 60
eth eth1 connector-type         : rj45
```

- MTU – R/O field to indicate the Maximum Transmission Unit of the port.
- Mac-addr – MAC address of the port.
- Admin – port enable/disable.

- Operational – port up/down status.
- Last-change – time elapsed since last port status changed.
- Name – text field.
- Alias – text field.
- Eth-type – configured Speed/Duplex: speed (10/100/1000) and duplex (half/full) setting.
    - 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).
- Eth-act-type – actual Speed/Duplex negotiated (if Auto-Neg enabled).
- Auto-neg – Auto negotiation enable/disable.
- Loopback-mode – enable and configure loopback on the port. External (towards the line side) or Internal (towards the radio side) loopback are available, with or without MAC addresses swap.
- Loopback Timeout – in seconds. Loopback will clear when timeout expires.
- Connector-type – RJ45 or SFP based on the physical port.

4.6.2 Configuring Interface Parameters

Use the `set eth` command, followed by the name of the interface to change the default values of an Ethernet interface.

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

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

5 Diagnostics

The MultiHaul™ 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 a MultiHaul™ 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 MultiHaul™ diagnostics features, and offers basic instructions for how to use these features to isolate and resolve operating faults in the ODUs or in the MultiHaul™ network. The chapter includes the following topics:

- Troubleshooting Process
- Alarms
- Loopbacks
- Performance Statistics

5.1 General 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 MultiHaul™ 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 all sides (copy its output to a text file) for efficient service.

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

5.2 MultiHaul™ Recommended Troubleshooting Steps

This is the recommended flow when dealing with problems reported by customers. Please keep in mind that these steps focus on connectivity issues and do not intend to cover all possible scenarios.

Let's review the possible reasons for customer to call for help.

1. No service (no Internet connection)
2. Slow Internet connection
3. Unstable service/Internet connection (disconnections)

What to check:

1. TU is connected.

You can ping it or connect to the BU and see that the TU is connected.

You should also check on the BU that the YU is connected (show remote-terminal-unit).

If TU is not connected, then obviously no service.

2. If no internet, check that the customer is physically connected to the TU (check the active alarms to see that the port is up and connected).

3. Check the log file for disconnection events. This might also explain slow internet connection (and often disconnections).

The BU log (and also the TU log) records all disconnect events and active alarms.

Here is an example of disconnection in the log of the TU:

```
TU>show log

Apr 24 13:46:07 cad: link down eth eth-bu1

Apr 24 13:50:50 cad: link up eth eth-bu1
```

4. You can monitor the throughput (Tx and Rx, in Mbps) on the BU and TU to see if there is an issue.

```
TU>show terminal-unit

terminal-unit self-mac            : 00:24:a4:07:47:14

terminal-unit ssid                : MultiHaul

terminal-unit password            : MultiHaul

terminal-unit connection-mode     : auto-connect

terminal-unit status              : connected

terminal-unit frequency           : channel-2

terminal-unit base-unit mac       : 00:24:a4:07:48:74

terminal-unit tx-mcs              : 7

terminal-unit signal-quality      : 30

terminal-unit tx-throughput       : 0

terminal-unit rx-throughput       : 0

terminal-unit tx-rate-limiter     : 100
```

5. You can monitor the Tx-MCS (modulation) and Signal quality. Typically, should be 8 and min 35, respectively.

6. If issues persist and require an in-depth investigation, you can schedule a maintenance window and run iperf test from the TU to the BU to confirm performance.

5.3 Alarms and Events

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
Reset Cause: "First Time Power On"	System power up after power connection	1) Restoring the power 2) Reset caused by power disruption	Power restored, no corrective actions needed
Reset Cause: "Software 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
Reset Cause: "Restore to Factory Settings"	System power up after user pressed the reset button (for more than 10 seconds), restoring factory defaults	1) User action: reset button pressed for more than 10 seconds causing factory defaults restore	Power restored after user action, no corrective actions needed
Reset Cause: "HW Watchdog Reset"	Internal HW watchdog failure, indicating system fault	System failure	1) Deadlock in SW/HW solved by workaround. no corrective actions needed 2) Replace ODU (if persistent).
Link down	Link down (operational down) on one of the line or radio interfaces	Line interfaces (eth1/2/3): 1) Ethernet cable disconnected or not connected properly. 2) Ethernet interface disabled (admin down). 3) Port settings mismatch 4) Interface HW fault. Radio interfaces (eth-tu, eth-bu): 1) No Line of Sight or rain fading. 2) Mismatch in rf configuration between sides or wrong configuration.	Line interfaces (eth1/2/3): 1) Verify cable terminated and connected properly. 2) Verify port configuration, including auto-neg and speed/duplex. 3) Replace unit. Radio interfaces (eth-tu, eth-bu): 1) Verify antenna alignment and verify clear line of sight. 2) Verify RF configuration. 3) Change channel to verify no interference. 4) Replace ODU.

		3) HW fault.	
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.
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.

5.4 Loopbacks

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

- Line Loopback – Internal loopback is performed on the interface, looping the line egress traffic towards the bridge (radio).
- RF (Radio) Loopback – Internal loopback is performed on the bridge’s RF interface, looping RF egress traffic towards the bridge (line 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.

5.4.1 Loopback Diagram

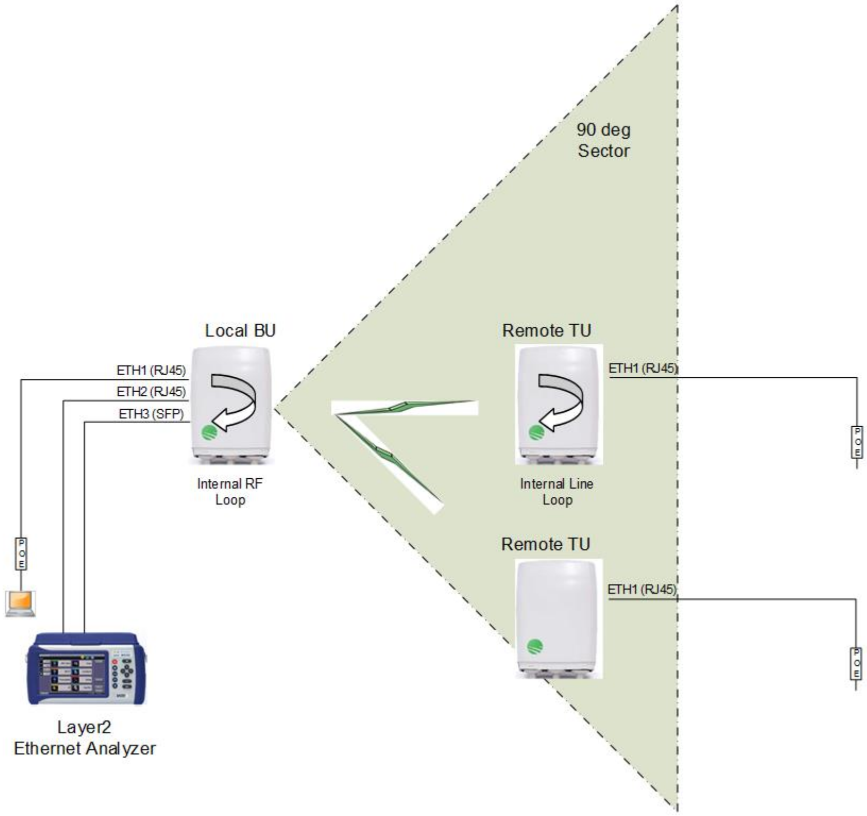


Figure 5-1 Loopbacks Diagram

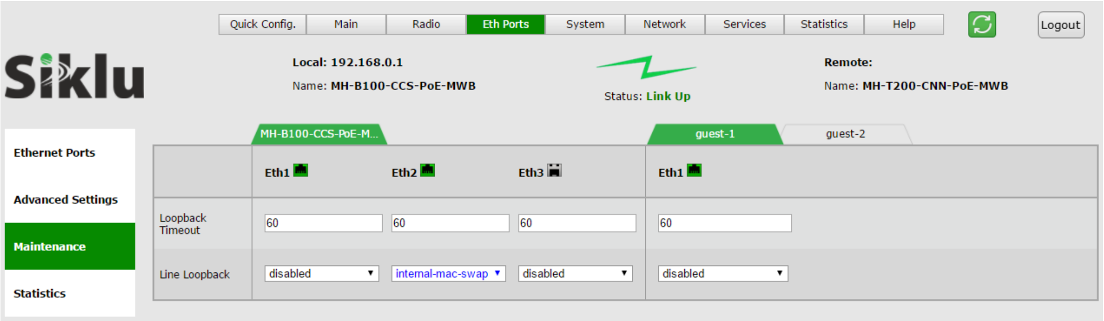
Internal user management and external Radius or TACACS server are supported.

5.4.2 Ethernet Line Loopbacks

The loopback can be applied separately for each one of the line interfaces (Eth1 to Eth3) with MAC Address swapping.

Set the loopback mode for the desired Ethernet port and set the loopback-timeout in seconds (default 60 seconds, up to 24 hours, 0= no timeout).

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



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CNN-PoE-MWB

	Eth1	Eth2	Eth3	Eth1
Loopback Timeout	60	60	60	60
Line Loopback	disabled	internal-mac-swap	disabled	disabled

Figure 5-2 Ethernet Line Loopback

Internal Line Loopback

An Internal loop returns the traffic to be transmitted out of the line port to the bridge. From the bridge the traffic is transmitted over the radio.

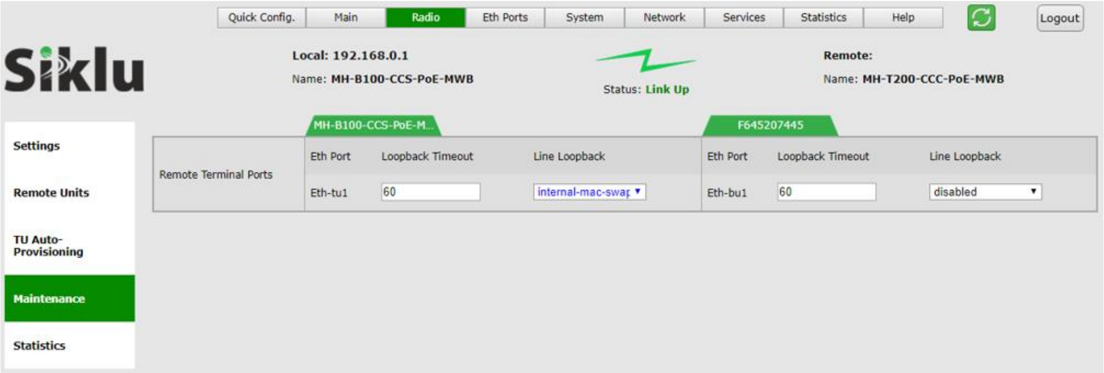
Connect the Ethernet traffic from the Customer’s end-equipment or Ethernet analyzer to the local radio and apply line loopback on remote radio for end-to-end testing. This will allow you to test the connection (cable/fiber) to the local radio, the interface between end-equipment and the local system, both local and remote systems and the radio transmission.

5.4.3 Radio Loopbacks

The loopback can be applied separately for each one of the radio interfaces (on a TU – one radio interface towards the BU, on a BU – up to 8 radio interfaces towards each on the TUs) with MAC Address swapping.

Set the loopback mode for the desired radio interface and set the loopback-timeout in seconds (default 60 seconds, up to 24 hours, 0= no timeout).

Radio loopbacks can be set in the Maintenance section of the Radio page.



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

	Eth Port	Loopback Timeout	Line Loopback	Eth Port	Loopback Timeout	Line Loopback
Remote Terminal Ports	Eth-tu1	60	internal-mac-swap	Eth-bu1	60	disabled

Figure 5-3 Radio Loopback

Internal Radio Loopback

An Internal loop returns the traffic to be transmitted out of the radio port to the bridge. From the bridge the traffic is transmitted to the line interfaces.

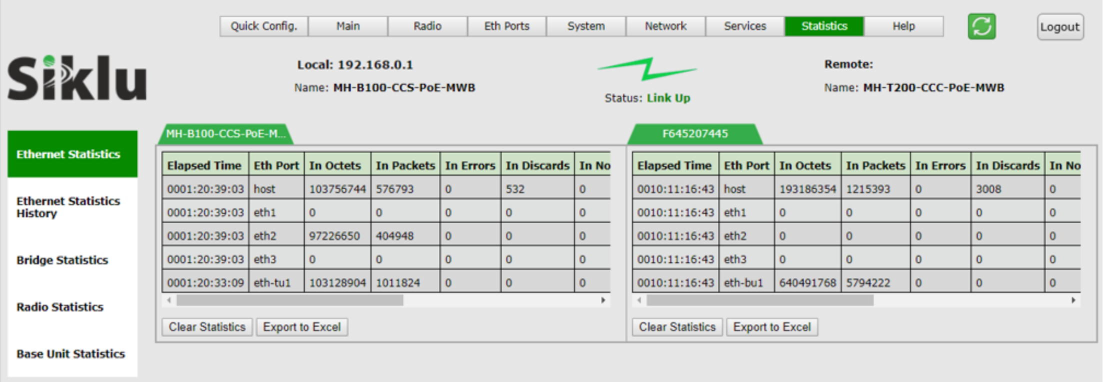
Connect the Ethernet traffic from the Customer's end-equipment or Ethernet analyzer to the local radio and apply radio loopback on local radio for local testing. This will allow you to test the connection (cable/fiber) to the local radio, the interface between end-equipment and the local system and the local radio.

5.5 Statistics

The performance statistics tab is available on each page and gathered on the **Statistics** page.

5.5.1 Ethernet Statistics

Ethernet statistics are presented per port (line interface and radio interface). Cumulative since last cleared or system's reboot.



Local: 192.168.0.1

Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:

Name: MH-T200-CCC-PoE-MWB

MH-B100-CCS-PoE-M...

Elapsed Time	Eth Port	In Octets	In Packets	In Errors	In Discards	In No
0001:20:39:03	host	103756744	576793	0	532	0
0001:20:39:03	eth1	0	0	0	0	0
0001:20:39:03	eth2	97226650	404948	0	0	0
0001:20:39:03	eth3	0	0	0	0	0
0001:20:33:09	eth-tu1	103128904	1011824	0	0	0

F645207445

Elapsed Time	Eth Port	In Octets	In Packets	In Errors	In Discards	In No
0010:11:16:43	host	193186354	1215393	0	3008	0
0010:11:16:43	eth1	0	0	0	0	0
0010:11:16:43	eth2	0	0	0	0	0
0010:11:16:43	eth3	0	0	0	0	0
0010:11:16:43	eth-bu1	640491768	5794222	0	0	0

Figure 5-4 Statistics Page: Ethernet Statistics

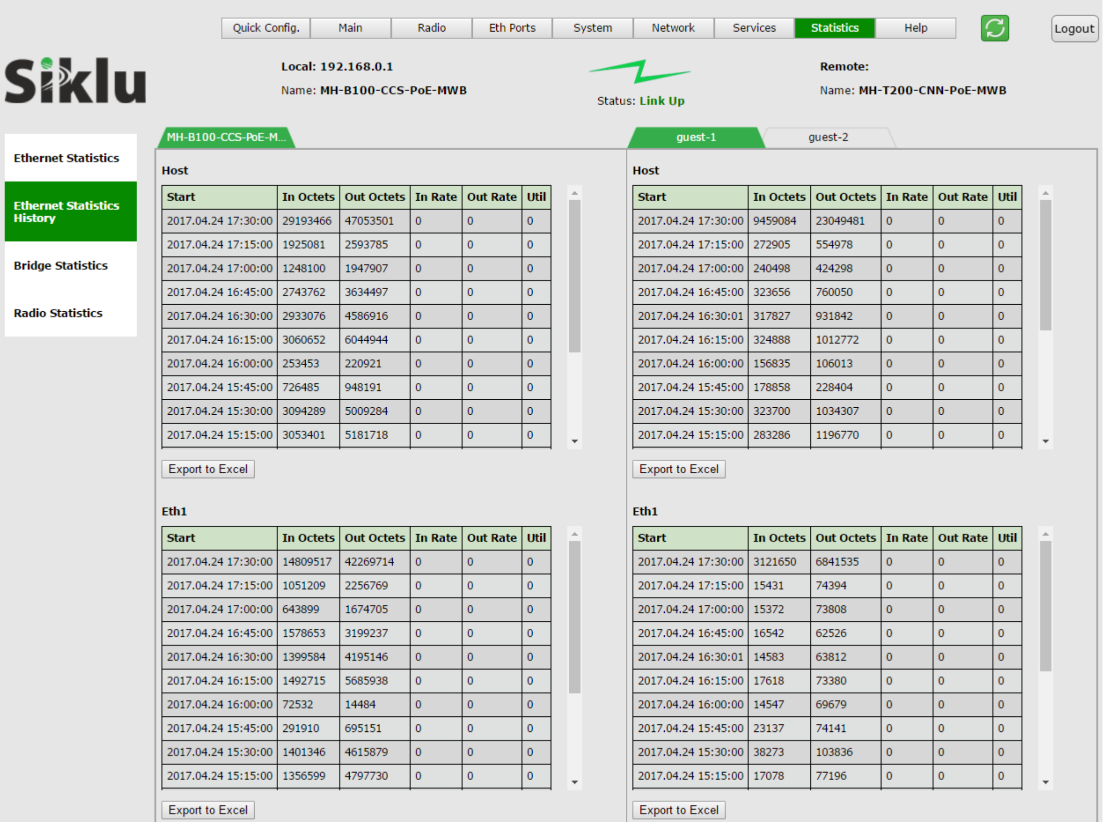
Attribute	Description
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.
Incoming Unicast Packets (in-ucast-pkts)	The number of unicast packets received on the interface.
Discarded Incoming Packets (in-discards)	The number of packets which 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-	The number of unicast packets transmitted out of the

Attribute	Description
pkts)	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.
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.

Statistics may be cleared or exported to Excel.

5.5.2 Ethernet Statistics History

Ethernet statistics are presented per port (line interface and radio interface) and include 96 intervals of 15 minutes (last 24 hours).



Local: 192.168.0.1

Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:

Name: **MH-T200-CNN-PoE-MWB**

Host

Start	In Octets	Out Octets	In Rate	Out Rate	Util
2017.04.24 17:30:00	29193466	47053501	0	0	0
2017.04.24 17:15:00	1925081	2593785	0	0	0
2017.04.24 17:00:00	1248100	1947907	0	0	0
2017.04.24 16:45:00	2743762	3634497	0	0	0
2017.04.24 16:30:00	2933076	4586916	0	0	0
2017.04.24 16:15:00	3060652	6044944	0	0	0
2017.04.24 16:00:00	253453	220921	0	0	0
2017.04.24 15:45:00	726485	948191	0	0	0
2017.04.24 15:30:00	3094289	5009284	0	0	0
2017.04.24 15:15:00	3053401	5181718	0	0	0

Eth1

Start	In Octets	Out Octets	In Rate	Out Rate	Util
2017.04.24 17:30:00	14809517	42269714	0	0	0
2017.04.24 17:15:00	1051209	2256769	0	0	0
2017.04.24 17:00:00	643899	1674705	0	0	0
2017.04.24 16:45:00	1578653	3199237	0	0	0
2017.04.24 16:30:00	1399584	4195146	0	0	0
2017.04.24 16:15:00	1492715	5685938	0	0	0
2017.04.24 16:00:00	72532	14484	0	0	0
2017.04.24 15:45:00	291910	695151	0	0	0
2017.04.24 15:30:00	1401346	4615879	0	0	0
2017.04.24 15:15:00	1356599	4797730	0	0	0

Host

Start	In Octets	Out Octets	In Rate	Out Rate	Util
2017.04.24 17:30:00	9459084	23049481	0	0	0
2017.04.24 17:15:00	272905	554978	0	0	0
2017.04.24 17:00:00	240498	424298	0	0	0
2017.04.24 16:45:00	323656	760050	0	0	0
2017.04.24 16:30:01	317827	931842	0	0	0
2017.04.24 16:15:00	324888	1012772	0	0	0
2017.04.24 16:00:00	156835	106013	0	0	0
2017.04.24 15:45:00	178858	228404	0	0	0
2017.04.24 15:30:00	323700	1034307	0	0	0
2017.04.24 15:15:00	283286	1196770	0	0	0

Eth1

Start	In Octets	Out Octets	In Rate	Out Rate	Util
2017.04.24 17:30:00	3121650	6841535	0	0	0
2017.04.24 17:15:00	15431	74394	0	0	0
2017.04.24 17:00:00	15372	73808	0	0	0
2017.04.24 16:45:00	16542	62526	0	0	0
2017.04.24 16:30:01	14583	63812	0	0	0
2017.04.24 16:15:00	17618	73380	0	0	0
2017.04.24 16:00:00	14547	69679	0	0	0
2017.04.24 15:45:00	23137	74141	0	0	0
2017.04.24 15:30:00	38273	103836	0	0	0
2017.04.24 15:15:00	17078	77196	0	0	0

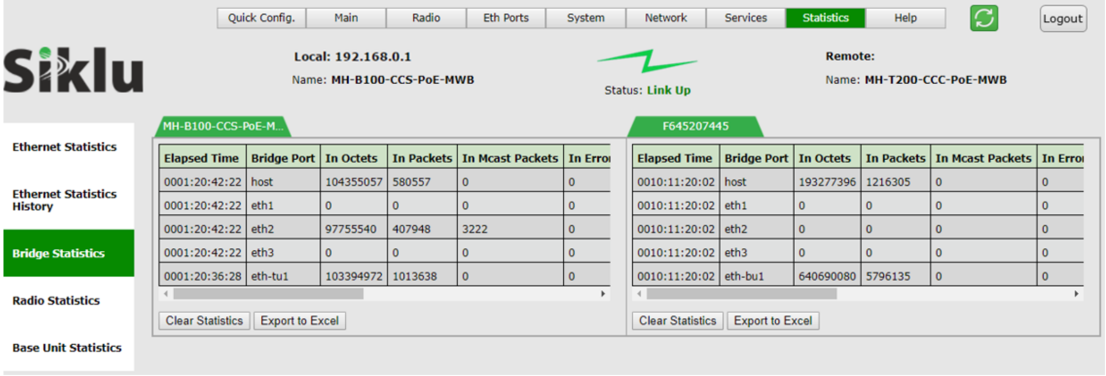
Figure 5-5 Statistics Page: Ethernet Statistics History

Attribute	Description
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.
In Rate	Rx rate in bits
Out Rate	Tx rate in bits

Statistics may be cleared or exported to Excel.

5.5.3 Bridge Statistics

Bridge statistics counters (since last cleared or last power up) are presented per bridge port defined.



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

MH-B100-CCS-PoE-M...

Elapsed Time	Bridge Port	In Octets	In Packets	In Mcast Packets	In Erro
0001:20:42:22	host	104355057	580557	0	0
0001:20:42:22	eth1	0	0	0	0
0001:20:42:22	eth2	97755540	407948	3222	0
0001:20:42:22	eth3	0	0	0	0
0001:20:36:28	eth-tu1	103394972	1013638	0	0

F645207445

Elapsed Time	Bridge Port	In Octets	In Packets	In Mcast Packets	In Erro
0010:11:20:02	host	193277396	1216305	0	0
0010:11:20:02	eth1	0	0	0	0
0010:11:20:02	eth2	0	0	0	0
0010:11:20:02	eth3	0	0	0	0
0010:11:20:02	eth-bu1	640690080	5796135	0	0

Figure 5-6 Statistics Page: Bridge Statistics

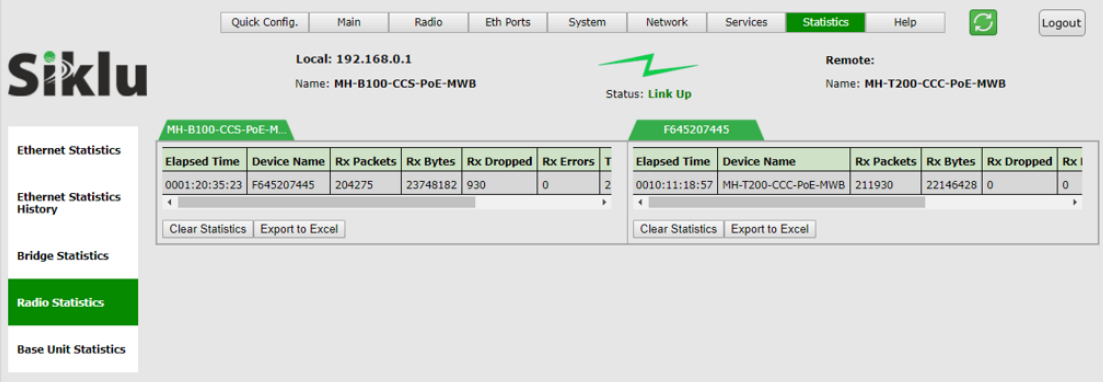
Attribute	Description
Incoming Octets (in-octets)	The total number of octets received on the interface, including framing characters.
Incoming Packets (in-packets)	The total number of packets received on the interface.
Incoming Multicast Packets (in-mcast-pkts)	The number of multicast packets received on the interface.
Erroneous Incoming Packets (in-errors)	The number of received erred packets.
Discarded Incoming Packets (in-discards)	The number of packets which were chosen to be discarded due to RX FIFO full.
Outgoing Octets (out-octets)	The total number of octets transmitted out of the interface, including framing characters.
Outgoing Packets (out-packets)	The total number of packets transmitted out of the interface.
Erroneous Outgoing Packets (out-error-packets)	The number of outbound packets that could not be transmitted because of errors.
Discarded Outgoing Packets (out-discard-packets)	The number of outbound packets which were chosen to be discarded due to excessive collision or excessive deferral.

Note that packets may be dropped due to traffic exceeding the radio link's available bandwidth.

Statistics may be cleared or exported to Excel.

5.5.4 Radio Statistics

Radio statistics counters (since last cleared or last power up) are presented per radio interface and name of TU (device name).



Local: 192.168.0.1

Name: **MH-B100-CCS-PoE-MWB**

Status: **Link Up**

Remote:

Name: **MH-T200-CCC-PoE-MWB**

Elapsed Time	Device Name	Rx Packets	Rx Bytes	Rx Dropped	Rx Errors	T
0001:20:35:23	F645207445	204275	23748182	930	0	2

Elapsed Time	Device Name	Rx Packets	Rx Bytes	Rx Dropped	Rx
0010:11:18:57	MH-T200-CCC-PoE-MWB	211930	22146428	0	0

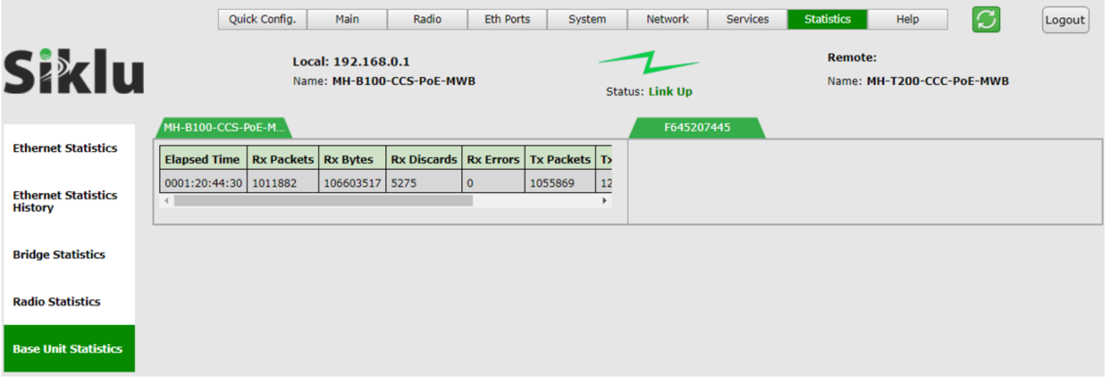
Figure 5-7 Statistics Page: Radio Statistics

Attribute	Description
Rx Packets	The total number of packets received on the radio interface.
Rx Bytes	The total number of bytes received on the radio interface.
Rx Dropped	The total number of packets dropped on receive on the radio interface.
Rx Errors	The total number of error packets received on the radio interface.
Tx Packets	The total number of packets transmitted by the radio interface.
Tx Bytes	The total number of bytes transmitted by the radio interface.
Tx Errors	The total number of transmit errors on the radio interface.

Statistics may be cleared or exported to Excel.

5.5.5 Base Unit Statistics

Cumulative aggregated base statistics counters (since last cleared or last power up).



Local: 192.168.0.1
Name: MH-B100-CCS-PoE-MWB

Status: Link Up

Remote:
Name: MH-T200-CCC-PoE-MWB

Elapsed Time	Rx Packets	Rx Bytes	Rx Discards	Rx Errors	Tx Packets	Tx
0001:20:44:30	1011882	106603517	5275	0	1055869	12

Figure 5-8 Statistics Page: Base Unit Statistics

Attribute	Description
Rx Packets	The total number of packets received on the radio interface.
Rx Bytes	The total number of bytes received on the radio interface.
Rx Dropped	The total number of packets dropped on receive on the radio interface.
Rx Errors	The total number of error packets received on the radio interface.
Tx Packets	The total number of packets transmitted by the radio interface.
Tx Bytes	The total number of bytes transmitted by the radio interface.
Tx Errors	The total number of transmit errors on the radio interface.

Statistics may be cleared or exported to Excel.

---End--