



LigoWave

LigoPTP 7.6x

User Guide

Revision 1.3
August 1, 2022

Copyright

© 2022 LigoWave

This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of LigoWave.

Notice

LigoWave reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LigoWave shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LigoWave.

Trademarks

LigoWave logo is trademark of LigoWave LLC.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

FCC warning

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 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC radiation exposure statement

To comply with FCC RF exposure requirements in section 1.1307, a minimum separation distance of 3.9 feet is required between the antenna and all occupational persons, and a minimum separation distance of 8.7 feet is required between the antenna and all public persons.

CE mark warning



This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

RED compliance statement

This equipment complies with all the applicable requirements of the Radio Equipment Directive 2014/53/EU of the European Parliament and the Council of 16 April 2014 on Radio Equipment (RED). The RED Directive repeals and replaces the R&TTE Directive 1999/5/EC.

Safety

This equipment is compliant with the latest EN IEC 62368-1:2020+A11:2020 safety standard, designed with the utmost care for the safety of those who deploy and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU countries not intended for use

None.

Contents

Copyright.....	2
Notice.....	2
Trademarks.....	2
FCC warning.....	3
FCC caution.....	3
FCC radiation exposure statement.....	3
CE mark warning.....	3
RED compliance statement.....	3
Safety.....	3
EU countries intended for use.....	3
EU countries not intended for use.....	3
CONTENTS.....	4
ABOUT THIS GUIDE.....	6
Purpose.....	6
Definitions, acronyms and abbreviations.....	6
DEVICE ACCESS.....	7
First connection via Ethernet.....	7
Windows OS.....	7
MAC OS.....	8
Linux (Ubuntu).....	8
First access to web management interface.....	8
LIGOPTP LINK GUIDED SETUP.....	10
Master's guided setup.....	10
Slave's guided setup.....	15
LIGOPTP CONFIGURATION.....	18
Applying and saving configuration changes.....	18
Status.....	18
Information.....	18
Statistics.....	19
Graphs.....	20
Settings.....	22
Radio configuration.....	22
Network configuration.....	24
IPv4 Configuration.....	24
IPv6 Configuration.....	24
Advanced Settings.....	25
Traffic Management.....	26
Ethernet Traffic Control.....	26
QoS.....	26
Services.....	28
Date & time.....	29
Management.....	30
Wireless management interface.....	30
System Alerts.....	31
SNMP.....	32
WNMS.....	33
Firmware update.....	33
Discovery services.....	34
System logging.....	34

System configuration.....	34
Security.....	35
Advanced settings.....	36
Tools.....	37
Site survey.....	37
Antenna alignment.....	39
Link test.....	40
Maintenance.....	44
Firmware upgrade.....	44
Dual boot firmware images.....	45
Network devices.....	46
Support.....	47
Cloud Controller Configuration.....	47

About This Guide

Purpose

This document provides information and procedures on installation, setup, configuration, and management of the LigoPTP unit.

Definitions, acronyms and abbreviations

The following typographic conventions and symbols are used throughout this document:



Additional information that may be helpful but which is not required.



Important information and warnings that should be observed.

bold

Menu commands, buttons, input fields, links, and configuration keys are displayed in bold

italic

References to sections inside the document are displayed in italic.

code

File names, directory names, form names, system-generated output, and user typed entries are displayed in constant-width type

Device Access

First connection via Ethernet

By default LigoPTP device obtains the IP address from the DHCP server. Follow the steps to access device on different OS:

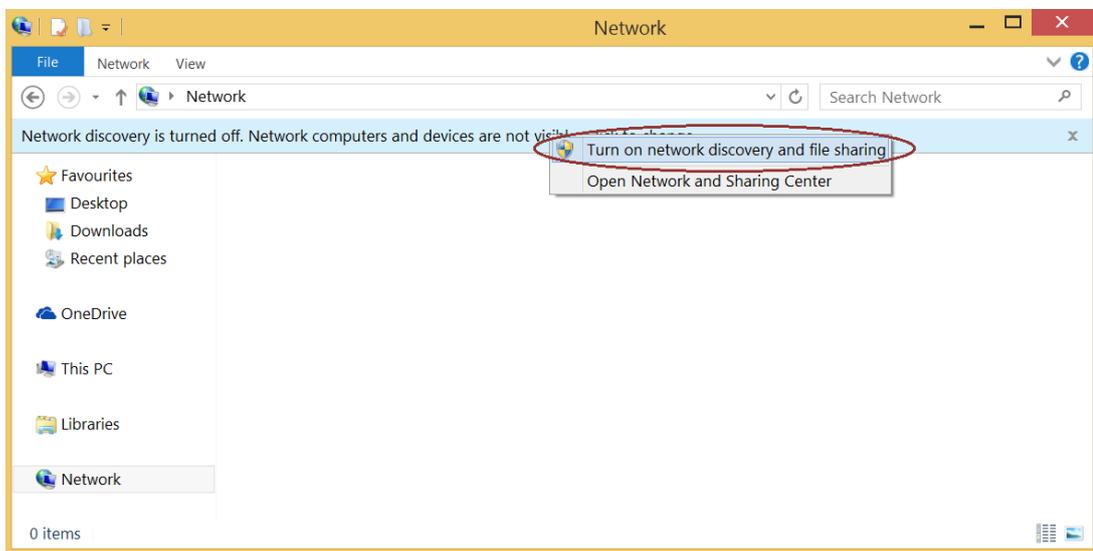


In case the LigoPTP device is unable to obtain IP address from a DHCP server, it fallback to the default static IP 192.168.2.66.

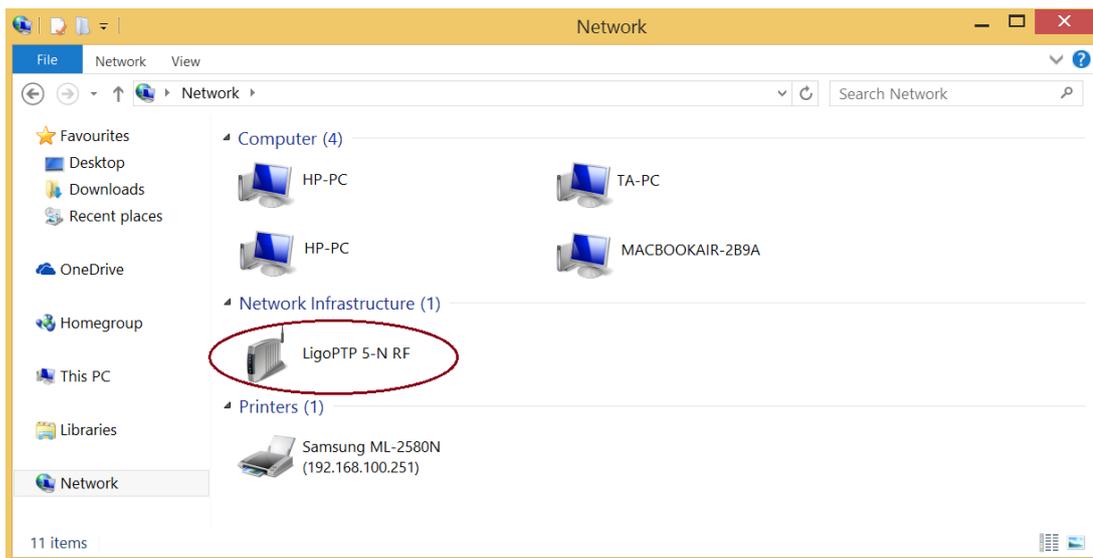
Windows OS

Step 1: Connect your PC directly to the LigoPTP device via Ethernet.

Step 2: Open Windows **Explorer**, click on **Network** drive, and turn on **Network discovery**:



Step 3: Find the required LigoPTP device icon:

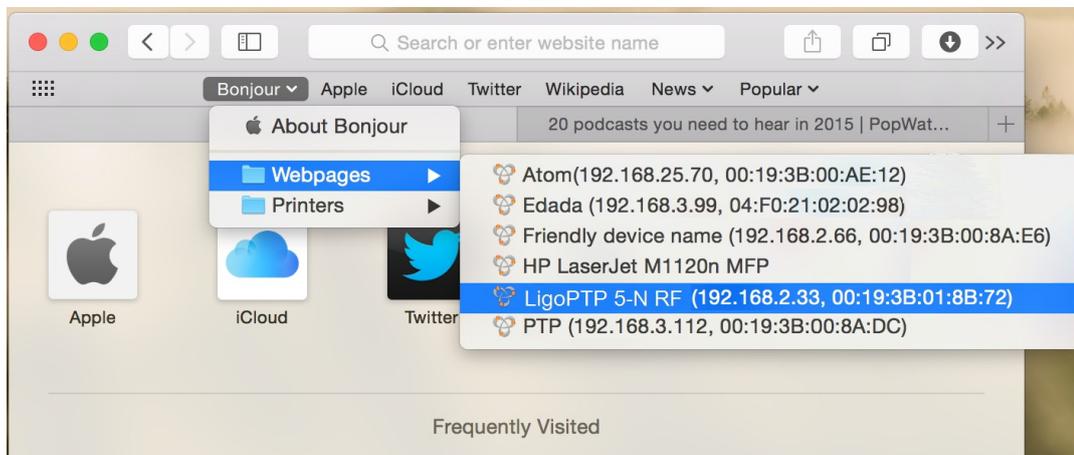


Step 4. Double-click on the device icon – you will be redirected to the device webpage automatically.

MAC OS

Step 1: Connect your PC to the LigoPTP device via Ethernet.

Step 2: Run **Bonjour** application, click on **Webpages** and find the required LigoPTP device name:



Step 3: Click on the selected item and the device web management interface will be loaded on the default web browser.

Linux (Ubuntu)

Step 1: Connect your PC to the LigoPTP device via Ethernet.

Step 2: Open terminal application GNOME Terminal (or Konsole for Kubuntu) and type command "avahi-browse -tr _http._tcp". Find the IP address of the required LigoWave device in the received output:

```

Ubuntu> avahi-browse -tr _http._tcp
+ eth2 IPv4 HP LaserJet 2200 (0001E660DF4D)      Web Site      local
+ eth0 IPv4 NFT 2N (192.168.5.10, 00:19:3B:00:8A:DA)  Web Site      local
= eth2 IPv4 HP LaserJet 2200 (0001E660DF4D)      Web Site      local
  hostname = [NPI60DF4D.local]
  address = [192.168.100.145]
  port = [80]
  txt = []
= eth0 IPv4 NFT 2N (192.168.5.10, 00:19:3B:00:8A:DA)  Web Site      local
  hostname = [NFT-2N-008ADA.local]
  address = [192.168.5.10]
  port = [80]
  txt = []

```

Step 3: Open a web browser and type discovered IP in the address field to open device web management interface.

First access to web management interface

Follow the steps for first connection to the LigoPTP device web management interface:

Step 1. Start your Web browser.

Step 2. Enter the device default IP address **192.168.2.66** in the web browser's IP field. By default, out of the box, or reset to defaults, LigoPTP unit will load the user agreement page. After signing user agreement, choose the LigoPTP unit's operating country. According to the chosen country, the regulatory domain settings may differ. You will be not allowed to select radio channels and RF output power other the permitted values for your chosen country and regulatory domain.



START MODE SETUP FINISH

Product name: LigoPTP Serial number: 0B1B15110000114D
Firmware version: PTP.MA-1.v7.51.10463 (Update) MAC address: 00:19:3B:05:30:B2

START

User agreement

The correct country code must be selected before using the equipment to meet the regulatory requirements for authorized channels, channel width, output power, Dynamic Frequency Selection (DFS) and Automatic Transmit Control (ATC).

Installer or equipment owner takes all responsibility for proper product usage according to the regulatory rules.

Vendor or distributor/reseller is not responsible for illegal wireless equipment operation.

I agree

Operating country:

5 GHz Antenna gain, dBi:



The Antenna Gain value should be set for products with external antenna only.

Step 3. After successful administrator login, you will see the main page of the device Web management interface. The device now is ready for configuration.

LigoPTP Link Guided Setup

The LigoPTP link consists of two units, one on each end: Master and Slave. If the radio settings of the LigoPTP Master and Slave units are met (and units are properly aligned on installing), the wireless link will automatically establish itself and the traffic will begin to pass between Master and Slave.

After the first login to the LigoPTP web management interface, the setup wizard provides simplified options to help you quickly get your LigoPTP link up and running.

Click **Guided setup** button to start LigoPTP units' installation:

The screenshot shows the LigoWave logo and a progress bar with four steps: START (active), MODE, SETUP, and FINISH. Below the progress bar, the product name is LigoPTP, the firmware version is PTP.MA-1.v7.52.10375 (Update), the serial number is 0B1B15120000002B, and the MAC address is 00:19:3B:04:DA:66. The 'START' section contains a 'User agreement' with a checkbox for 'I agree' (checked), a dropdown for 'Operating country' (set to 'United States'), and a text input for '5 GHz Antenna gain, dBi' (set to '23'). At the bottom right, there are two buttons: 'Manual setup' and 'Guided setup', with the 'Guided setup' button highlighted by a red circle.

Figure 1 – LigoPTP guided setup



To setup LigoPTP unit manually you can cancel this wizard at any time (not recommended).

Master's guided setup

Follow the steps to setup LigoPTP link from the Master unit's side. With this wizard, the administrator is able to setup Master unit as well as scan the air, find the Slave unit, assign required settings, thus creating the LigoPTP link.

Step 1. Choose the operating mode: choose **Master** and click Next button:



START **MODE** SETUP FINISH

Product name: LigoPTP Serial number: 0B1B15120000002B
Firmware version: PTP.MA-1.v7.52.10375 MAC address: 00:19:3B:04:DA:66

OPERATING MODE

Please choose the operating mode for the current device:

Master Slave Load from file

< Back Next >

Step 2. Specify essential parameters of the Master unit and click Next button:



Note that the Security -> **Password** is for connection security between LigoPTP units as well as password to login to the web management interface. This password on Master and Slave units must match.



— ○ START — ○ MODE — ● SETUP — ○ DISCOVERY — ○ FINISH —

Product name: LigoPTP Serial number: 0B1B15120000002B
Firmware version: PTP.MA-1.v7.52.10375 MAC address: 00:19:3B:04:DA:66

MASTER - SETUP

Friendly name: Location:

Contact information:

Security

Password:

IMPORTANT: this password is used to manage all devices on the same wireless network and is also used to generate wireless connection security passphrase. On all devices in same wireless network it must be the same otherwise wireless link will not work.

Radio settings

Link ID: Channel selection:

Network settings

IP method: ▼ DNS server 1:

IP address: DNS server 2:

Subnet mask:

Default gateway:

Step 3. Connect Slave unit to Master unit as shown in pictures below (choose one of the given connection options) and wait until the Slave units appear in the list if the bottom of the page:



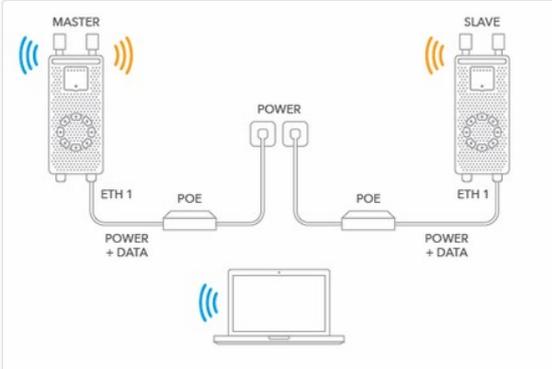
○ START ○ MODE ○ SETUP ● DISCOVERY ○ FINISH

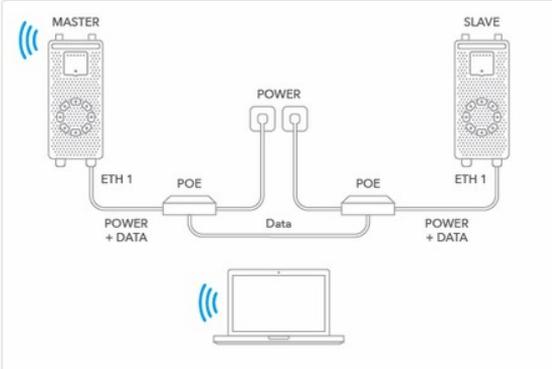
Product name: LigoPTP
Firmware version: PTP.MA-1.v7.52.10375

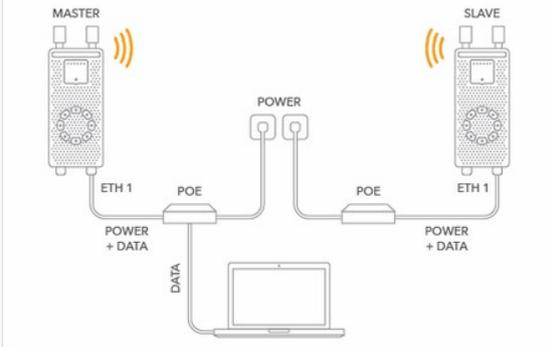
Serial number: 0B1B1512000002B
MAC address: 00:19:3B:04:DA:66

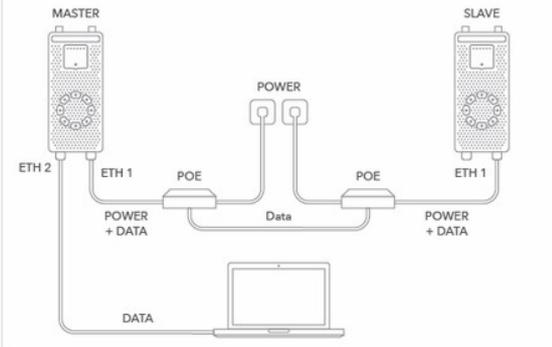
MASTER - DISCOVER DEVICES

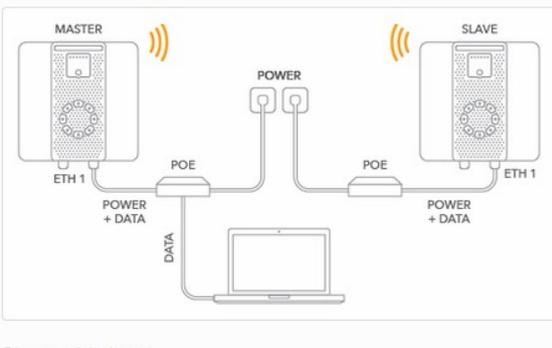
To configure Slave devices automatically connect them as shown on the pictures below and wait until they appear in the list. List is updated automatically. Select Slave device and set its parameters. When finished or want to skip this step press Next button.

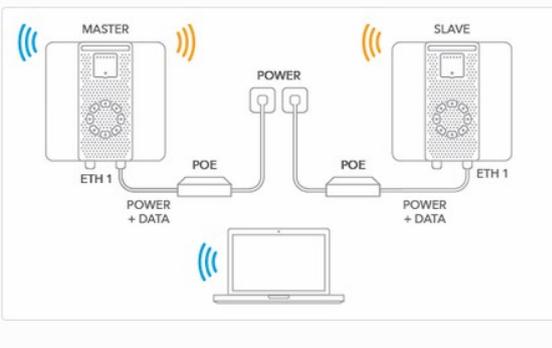












Discovered devices: 1

<input type="checkbox"/>	LigoPTP	SN: 0B1B15110000114D	MAC: 00:19:3B:05:30:B2	Media: wireless
--------------------------	---------	----------------------	------------------------	-----------------

< BackApply configuration



Note that Discovered device list displays remote LigoPTP devices having the default settings only. Already configured devices will not be included in the list.

Step 7. The LigoPTP link is successfully configured. Check parameters of the established LigoPTP link on the Status-> Information page:

The screenshot shows the 'INFORMATION' page in the LigoWave interface. At the top right, a progress bar for 'Link quality (28 %)' is circled in red. Below, the 'Radio' section contains various parameters, with 'Link: LigoPTP' circled in red. A table at the bottom compares 'Remote site' and 'Local site' parameters.

Remote site						Local site
Remote device	Link status	TX power, dBm	TX/RX data rate, Mbps	Noise level, dBm	Signal level, dBm	Signal level, dBm
LigoPTP Slave 00:19:3B:05:30:B2	UP 2 min. 46 sec.	30	6/0	-95/-95	-95 -95	-89 -64



The LigoPTP unit is now running but probably requires additional configuring to conform to your network operational and security requirements. Refer to the next chapter *LigoPTP Configuration* in this manual for the information you need to complete the configuration.

Slave's guided setup

Follow the steps to setup Slave unit. With this wizard the administrator is able to setup Slave unit to scan the air, find and assign the Master unit, thus creating the LigoPTP link.

Step 1. Choose the operating mode: choose **Slave** button and click Next button:

The screenshot shows the 'OPERATING MODE' configuration screen. A progress bar at the top indicates the current step is 'MODE'. The 'Slave' button is highlighted in orange, while 'Master' and 'Load from file' are greyed out. A 'Next >' button is visible at the bottom right.

Step 2. Specify the required settings for the LigoPTP Link and click Apply configuration button:

Product name: LigoPTP
Firmware version: PTP.MA-1.v7.52.10375

Serial number: 0B1B15110000114D
MAC address: 00:19:3B:05:30:B2

SLAVE - SETUP

Friendly name: Location:

Contact information:

Security

Password:

IMPORTANT: this password is used to manage all devices on the same wireless network and is also used to generate wireless connection security passphrase. On all devices in same wireless network it must be the same otherwise wireless link will not work.

Radio settings

Link ID: Channel width (MHz):

Network settings

IP method:

DHCP IP fallback

IP address:

Subnet mask:

Default gateway:

Enter keyword to filter results

LigoPTP
00:19:3B:05:30:B2 | 40 nBm | 5180 MHz
Last updated: 5/16/2019, 3:09:34 PM



Note that the Security -> **Password** is for connection security between LigoPTP units as well as password to login to the web management interface. This password on Slave and Master units must match.



For convenience use search button next to **Link ID** to scan for the Master device

Step 3. Click **Finish** to enable newly assigned settings for Slave unit. After the setup process will be finished, you will be redirected to Login page. Submit a password (assigned on the Step 2) for login to the web management interface.

Product name: LigoPTP **Serial number:** 0B1B15110000114D
Firmware version: PTP.MA-1.v7.52.10375 **MAC address:** 00:19:3B:05:30:B2

FINISH

You have successfully configured Your device.
Password: LigoPTP_password **Operating country:** US

Device

Operating mode: SLAVE **Friendly name:** LigoPTP Slave
Antenna gain, dB: 23 **Location:** Location

Radio

Wireless network ID: LigoPTP **Frequency, MHz:** Auto
Channel width, MHz: 40

Network

IP method: Dynamic

Finish

Step 4. Check parameters of the established LigoPTP link:

Link quality (31%)

INFORMATION

Product name: LigoPTP **Friendly name:** LigoPTP Slave
Serial number: 0B1B15120000002R **Device location:** Location
Firmware version: PTP.MA-1.v7.52.10375 (Update) **Latitude/Longitude:** 0 / 0
System uptime: 45 min. 6 sec. **Height AGL, m:** 0

Radio

Operating mode: SLAVE **TX power, dBm:** 30
Max TX data rate, Mbps: 400 (256-QAM 5/6) **Antenna gain, dBi:** 23
Frequency, MHz: 5180 (5170-5210) **Noise level, dBm:** -95/-95
Channel width, MHz: 40

Link: LigoPTP

Remote site						Local site
Remote device	Link status	TX power, dBm	TX/RX data rate, Mbps	Noise level, dBm	Signal level, dBm	Signal level, dBm
LigoPTP 00:19:3B:05:30:B2	UP 5 min. 36 sec.	31	6/130	-95/-95	-73 -49	-95 -95



The LigoPTP unit is now running but probably requires additional configuring to conform to your network operational and security requirements. Refer to the next chapter *LigoPTP Configuration* in this manual for the information you need to complete the configuration.

LigoPTP Configuration

Applying and saving configuration changes

The four buttons appear right after the configuration changes were made on the GUI, located on the right top corner of the WEB GUI allowing managing device configuration:



-  **Save changes** – if pressed new configuration settings are applied instantly and written to the permanent device memory.
-  **Test changes** – if pressed the device will start operating with newly set configuration settings for 3 minutes. During this test time, the administrator is able to gauge if device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings administrator have lost connection with the device), the device automatically reverts back configuration to an old one.
-  **Discard changes** – if pressed parameter changes are discarded. It should be noted that if Save changes is pressed it is not possible to discard changes.
-  **Logout** – if pressed, the user will be redirected to the Login page.



It is not necessary to **Save changes** at every Web GUI tab. The device remembers all changes made in every tab and any after action button is used, all the changes will be applied or rejected.

Status

After login, the main Web management page displays Status Information page. The header of Web management page displays Link quality and Ethernet port(s) status:



Figure 2 – Web Management Interface



Information

Use the Status Information menu to check the current status of the LigoPTP unit and established link (this is the default page when accessing the device's web management interface). The Information page displays generic information and status of the LigoPTP unit. The page divided into four main categories: System, Radio, Link and Network. The System section displays the identification information of the LigoPTP unit. The Radio section presents main wireless settings. The Link table describes the LigoPTP link (Local and Remote site) connectivity parameters. The Network section displays a short summary about network configuration (IPv4 and IPv6).

The information in the page can be updated using Refresh  icon.

INFORMATION



Product name: LigoPTP 5-N RapidFire	Friendly name: Testlab
Serial number: 0B1B151200000029	Device location: Vilnius
Firmware version: PTP.MA-1.v7.51-8750 (Update)	Latitude/Longitude: 10 / 10
System uptime: 3 hours 45 min. 55 sec.	Height AGL, m: 30

Radio

Operating mode: MASTER	TX power, dBm: 10
Max TX data rate, Mbps: 866.7 (256-QAM 5/6)	Antenna gain, dBi: 0
Frequency, MHz: 5220 (5180-5260)	Noise level, dBm: -95/-95
Channel width, MHz: 80	

Link: Autoteslab2

Remote site						Local site
Remote device	Link status	TX power, dBm	TX/RX data rate, Mbps	Noise level, dBm	Signal level, dBm	Signal level, dBm
Testlab 00:19:3B:04:DA:66	UP 1 hour 43 min. 24 sec.	10	866/866	-95/-95	-54 -52	-56 -51

Network

IP method: Static	IPv6 method: Disabled
MAC address: 00:19:3B:05:31:34	
IP address: 192.168.199.1	
Subnet mask: 255.255.255.0	
Default gateway: 192.168.199.100	
DNS server 1: --	
DNS server 2: --	

Figure 3 – Device Information Page



If LigoPTP unit operates as Master, the Link table contains possibility to manage remote device's (Slave) configuration. Click on the active link (Friendly name of the remote device) and the dialog box containing Slave's settings will be loaded.



Statistics

The statistics page displays detailed statistics of the PTP link performance. The Statistics page divided into the two sections: Interfaces and W-Jet V statistics.

STATISTICS

Interfaces

Interface	Tx data	Rx data	Tx packets	Rx packets	Tx errors	Rx errors
Wireless	4.01 MiB	3.92 MiB	14.09 k	18.13 k	1	0
ETH1	6.68 MiB	3.39 MiB	55.57 k	30.09 k	0	0
ETH2	281.33 KiB	4.82 KiB	4.34 k	77	0	0

W-Jet V

MAC address	IP address	TX frames	RX frames	TX retry frames, %
00:19:3B:05:31:34 (Local)	192.168.199.1	13.76 k (+12)	18.12 k (+14)	0
00:19:3B:04:DA:66 (Remote)	192.168.199.101	18.12 k	14.07 k	0

Figure 4 –Interface counters

Interfaces

This table contains detailed statistics of Ethernet and Wireless interfaces:

TX data – displays the total number of sent bytes by the Ethernet or Wireless interface of the link.

RX data – displays the total number of received bytes by the Ethernet or Wireless interface of the PTP link.

TX packets – displays the total number of sent packets by the Ethernet or Wireless interface of the PTP link.

RX packets – displays the total number of received packets by the Ethernet or Wireless interface of the PTP link.

TX errors – displays the total number of sent corrupted packets by the Ethernet or Wireless interface of the PTP link.

RX errors – displays the total number of received corrupted packets by the Ethernet or Wireless interface of the PTP link.

W-JET V

W-Jet V is advanced proprietary wireless protocol that combines special techniques to achieve superior performance and reliability even over long distances. This table displays statistical counters of the PTP link communication protocol.

MAC address – displays MAC addresses of the Local and Remote units.

IP address – displays IP addresses of the Local and Remote units.

TX frames – number of transmitted data frames. The number in brackets (+xx) displays the data change since the last page refresh.

RX frames – number of transmitted data frames. The number in brackets (+xx) displays the data change since the last page refresh.

TX retry frames % – the percentage of attempts to retransmit data frames. The number in brackets (+xx) displays the data change since the last page refresh.



Graphs

The Graphs page contains device statistics in graphic diagrams and is used for device monitoring.

This page displays graphic diagrams of the following statistics: Signal level, Wireless and Ethernet Throughput, Wireless and Ethernet PPS, CPU load, and Memory usage. Data is displayed in real time, and can be shown in hourly, daily, weekly or monthly intervals as well.



Hovering mouse cursor over the diagram line will display the exact value of the particular counter.

Signal strength diagram displays signal change of the Local and Remote PTP units at the chosen period:

Signal level (last 15 min)

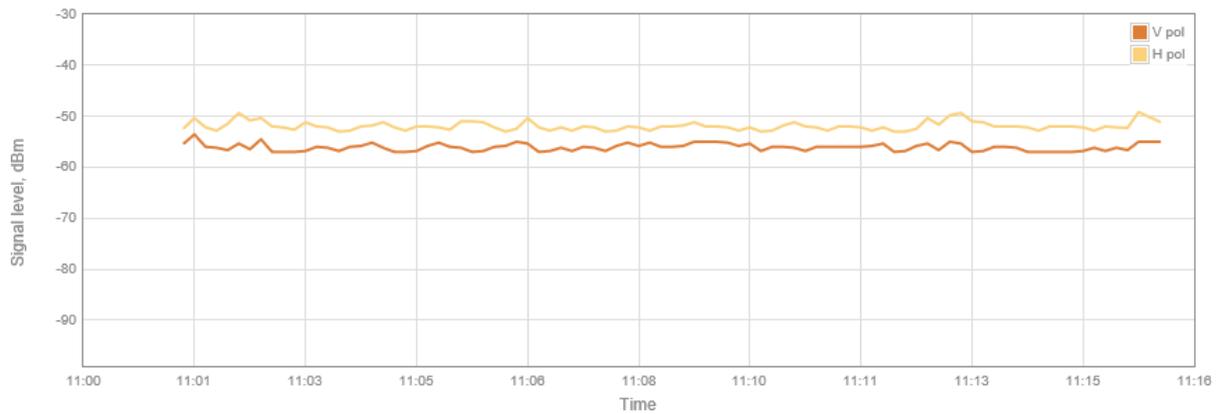
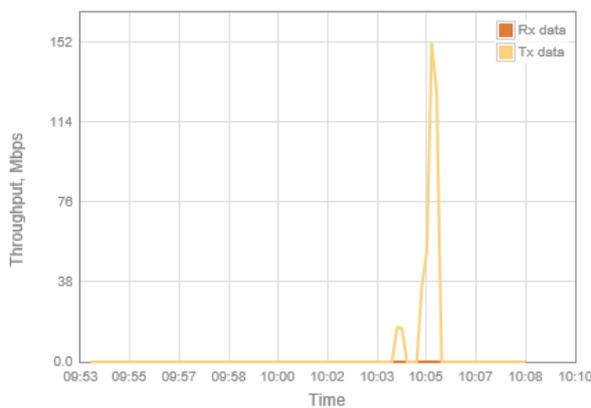


Figure 5 - Signal Strength Graph

Data throughput shows graphical expression of Wireless and Ethernet interfaces throughput statistics of the PTP link in last 15 minutes.

Packets per seconds (PPS) displays graphical expression of Wireless and Ethernet interfaces PPS of the PTP link in last 15 minutes.

Wireless data throughput (last 15 min)



Wireless packets per second (last 15 min)

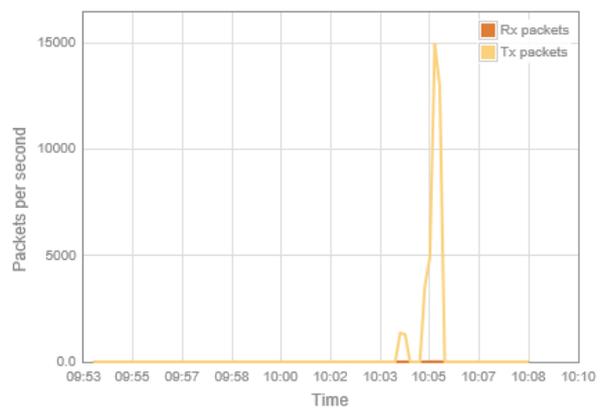
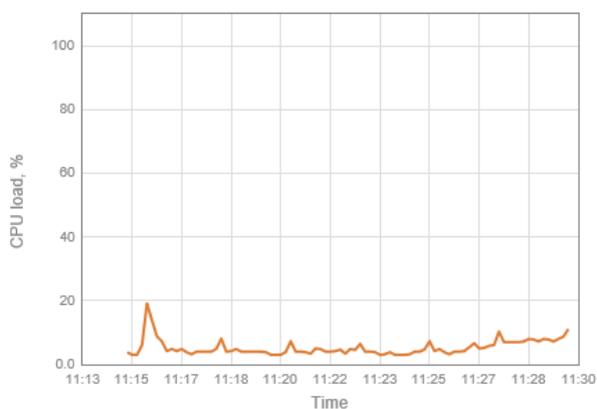


Figure 6 - Data Throughput and PPS (Wireless interface) graphs

CPU load diagram displays device CPU load in selected appropriate time scale.

Memory diagram displays the graph of device memory usage:

CPU load (last 15 min)



Memory usage (last 15 min)

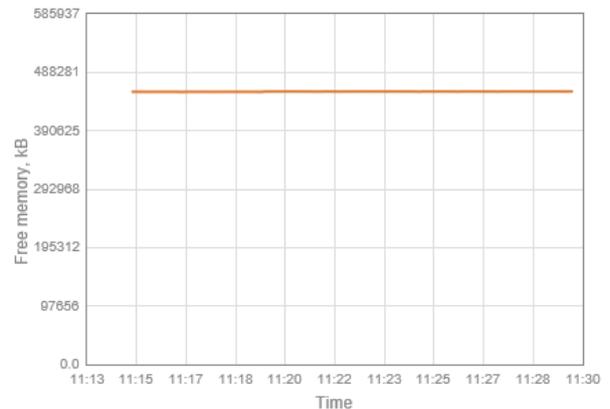


Figure 7 - CPU load and Memory usage graphs

Settings



Figure 8 – Web Management Interface

Radio configuration



Before changing wireless settings manually, please verify that your settings will comply with local government regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations.



The wireless security is hardware accelerated AES-128 encryption on all LigoPTP units. The passphrase of the wireless link security can be changed in **Settings->Security** page.

Use the **Configuration | Wireless** menu to set up radio settings for the PTP link:

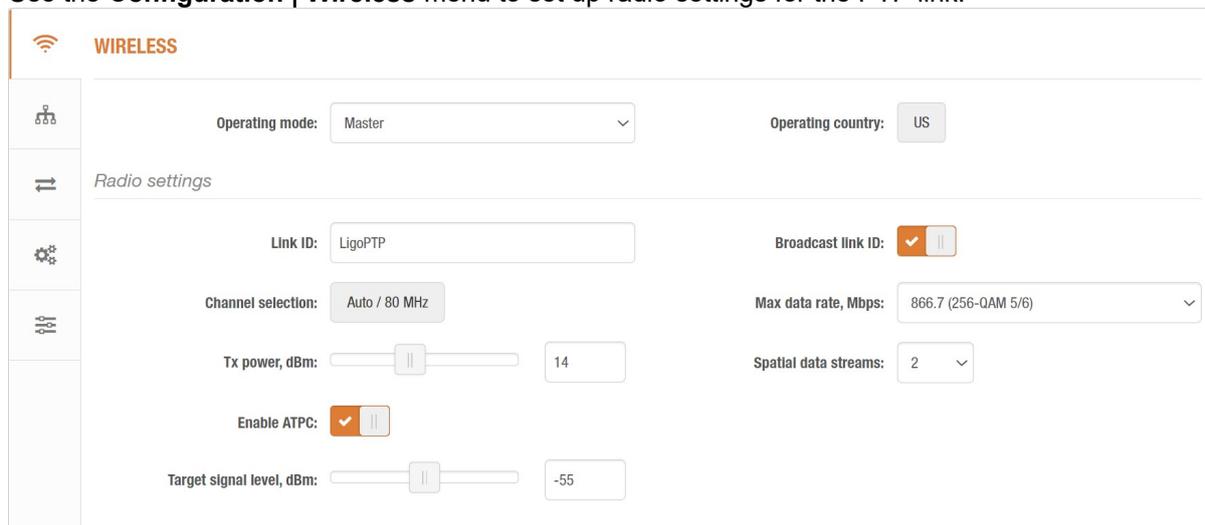


Figure 9 - Wireless settings

Operating mode – specify the operating device role to create PTP link:

- **Master** – the controlling unit of the PTP link.
- **Slave** – in this mode, the PTP unit that connects to the Master unit, creating the PTP link.

Operating country – displays LigoPTP unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. Initially country is selected on the first step of the LigoPTP unit’s installation, though can be updated if required.

Link ID – specify the wireless network name, for a LigoPTP link identification.



For PTP link establishment both units (Master and Slave) of a link must have exactly the same **Link ID**.

Broadcast link ID – enables or disables the broadcasting of the link ID. Disabling Link ID Broadcast makes LigoPTP unit invisible for all wireless clients.



If unit operates as **Slave**, there is possibility to scan for LigoPTP Master's Link ID automatically:

Link ID:

The scan results will appear in the Search SSID table.

Tx power – set the radio transmit power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. The transmit power level that is actually used is limited to the maximum value allowed by your country's regulatory agency.

ATPC – select to enable Automatic Transmit Power Control (ATPC). If enabled, LigoPTP radio will continuously communicate with remote unit's radio in order to adjust transmitter power automatically.

Target signal level – specifies the desired optimal signal level, in dBm, that ATPC would try to keep.

Max data rate, Mbps – choose the maximum data rates in Mbps at which LigoPTP should transmit packets. LigoPTP will attempt to transmit data at the highest data rate set and if there is an interference encountered, the device will step down to the next lower data rate automatically.

Spatial data streams – allows to switch between 2 streams (MIMO 2x2) and single-stream operation. In single-stream mode, data bits are duplicated and sent over two antenna ports at the same time, improving the chances for link establishment in rapidly-changing interference-prone environment or helping to troubleshoot potential antenna or RF cabling issues.

Channel selection – select the channel(s) at which the LigoPTP units will communicate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows LigoPTP unit to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is the least occupied. The table displays detailed information about each channel:

CHANNEL

Channel width (MHz):

<input checked="" type="checkbox"/>	Channel	TX limit, dBm	EIRP limit, dBm	DFS/ATPC required
<input checked="" type="checkbox"/>	31 (5155 MHz)	30	53	No
<input checked="" type="checkbox"/>	32 (5160 MHz)	30	53	No
<input checked="" type="checkbox"/>	33 (5165 MHz)	30	53	No
<input checked="" type="checkbox"/>	34 (5170 MHz)	30	53	No
<input checked="" type="checkbox"/>	35 (5175 MHz)	30	53	No
<input checked="" type="checkbox"/>	36 (5180 MHz)	30	53	No
<input checked="" type="checkbox"/>	37 (5185 MHz)	30	53	No
<input checked="" type="checkbox"/>	38 (5190 MHz)	30	53	No
<input checked="" type="checkbox"/>	39 (5195 MHz)	30	53	No
<input checked="" type="checkbox"/>	40 (5200 MHz)	30	53	No

Figure 10 - Channel Selection

Channel width – select the width of the radio channel. The LigoPTP supports 5 MHz, 10 MHz, 20 MHz, 40 MHz and 80 MHz radio channel widths.



Slave operating mode has only channel width selection. Slave unit inherits channel from Master unit automatically.



Network configuration

The **Settings | Network** menu allows you to control the LigoPTP unit's IPv4 and IPv6 network configuration.

IPv4 Configuration

NETWORK CONFIGURATION

IPv4 settings

IP method:	Static <input type="button" value="v"/>	DNS server 1:	<input type="text"/>
IP address:	10.0.94.140	DNS server 2:	<input type="text"/>
Subnet mask:	255.255.255.0		
Default gateway:	10.0.94.200		

IPv6 settings

IPv6:

Advanced settings

Figure 11 – Network Configuration: IPv4



When assigning IP address make sure that the chosen IP address is unused and belongs to the same IP subnet as your wired LAN, otherwise you will lose the connection to the device from your current PC. If you enable the DHCP client, the browser will lose the connection after saving, because the IP address assigned by the DHCP server is not predictable.

IP method – specify IP reception method: IP addresses can either be retrieved from a DHCP server or configured manually:

- **Static** – the IP address will be specified manually.
- **Dynamic** – the DHCP server will assign the IP address for LigoPTP unit. If DHCP server is not available, the device will try to get an IP. If has no success, it will use pre-configured fallback IP address. The fallback IP settings can be changed to custom values.

IP address – specify IP address for LigoPTP unit.

Subnet mask – specify a subnet mask for device.

Default gateway – specify a gateway IP address for device.

DNS server – specify primary and/or secondary the Domain Naming Server.

Secondary IP – specify the alternative IP address and the netmask for LigoPTP unit management.

IPv6 Configuration

Click on the **IPv6** slide to enable IPv6 configuration:

NETWORK CONFIGURATION

IPv4 settings

IP method:	Static <input type="checkbox"/>	DNS server 1:	<input type="text"/>
IP address:	10.0.94.10	DNS server 2:	<input type="text"/>
Subnet mask:	255.255.255.0		
Default gateway:	10.0.94.200		

IPv6 settings

IPv6:	<input checked="" type="checkbox"/>		
IPv6 method:	Static <input type="checkbox"/>	IPv6 DNS server 1:	<input type="text"/>
IPv6 address:	fc00::c0:a8:2:42	IPv6 DNS server 2:	<input type="text"/>
IPv6 prefix length:	64		
IPv6 default gateway:	fc00::c0:a8:2:1		

Advanced settings

Figure 12 - Network Configuration: IPv6

IPv6 method – specify IPv6 reception method: IPv6 addresses can either be retrieved from a DHCPv6 server or configured manually:

- **Dynamic stateless IP** – the DHCPv6 client only obtains network parameters other than IPv6 address
- **Dynamic stateful IP** – the DHCPv6 clients require IPv6 address together with other network parameters (e.g. DNS Server, Domain Name, etc.).
- **Static** – the IPv6 address will be specified manually.
 - **IPv6 address** – specify the **IPv6 Address** for the interface.
 - **IPv6 prefix length**– enter the **Prefix Length** for the address.
 - **IPv6 default gateway** – specify IPv6 address for default gateway.
 - **IPv6 DNS server** – specify the Domain Naming Server IPv6 addresses.

Advanced Settings

Advanced settings

Management VLAN ID:

Enable STP:

Management VLAN – click on the check box to enable a VLAN tagging for management traffic. Access to the LigoPTP unit for management purposes can further be limited using VLAN tagging. By defining Management VLAN, unit will only accept management frames that have the appropriate Management VLAN ID. All other frames using any management protocol will be rejected.

Management VLAN ID – specify the VLAN ID [2-4095]. When a specific VLAN ID value is assigned for LigoPTP network interface, only management frames that matching configured VLAN ID will be accepted by device.



When you specify a new management VLAN, your connection to the device will be lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN router.

Enable STP – Starts IEEE 802.1D Spanning Tree Protocol on all bridged interfaces.



Traffic Management

The **Services** menu is divided in two sections:

- Ethernet traffic control
- QoS (available on Master only)

Ethernet Traffic Control

Configure the Ethernet traffic control on both Ethernet ports:

TRAFFIC MANAGEMENT

Traffic control on Ethernet ports

Enable speed limit: Incoming speed, Mbps

Note: speed limit is applied on both ports ETH1 + ETH2

Figure 13 – Traffic control on Ethernet ports.

Enable speed limit – slide to enable speed limitation on both Ethernet ports.

Incoming speed – use slide, or specify manually the maximum speed in Mbps on incoming traffic.

QoS



QoS functionality is available only if device is operating as Master.

LigoPTP units support L2 (802.1p) and L3 (DSCP) QoS. In layer 2 QoS data is prioritized according to VLANs while in layer 3 according to IP addresses. Both types of QoS can run together or independently and traffic can be mapped into 4 different queues for each type applying strict or WRR policies. Having QoS on your link allows you to prioritize mission critical data and real time data that requires more capacity and higher PPS rate. Max capacity for each of the queues is calculated according to the wireless link, dynamically.

QoS

Policy: Precedence:

Enable L2 802.1p:

802.1p Queue	802.1p Queue	802.1p Queue	802.1p Queue
0 <input type="text" value="1"/>	2 <input type="text" value="2"/>	4 <input type="text" value="3"/>	6 <input type="text" value="4"/>
1 <input type="text" value="1"/>	3 <input type="text" value="2"/>	5 <input type="text" value="3"/>	7 <input type="text" value="4"/>

Enable L3 DSCP:

DSCP Queue	DSCP Queue	DSCP Queue	DSCP Queue
0 <input type="text" value="1"/>	16 <input type="text" value="2"/>	32 <input type="text" value="3"/>	48 <input type="text" value="4"/>
1 <input type="text" value="1"/>	17 <input type="text" value="2"/>	33 <input type="text" value="3"/>	49 <input type="text" value="4"/>
2 <input type="text" value="1"/>	18 <input type="text" value="2"/>	34 <input type="text" value="3"/>	50 <input type="text" value="4"/>
3 <input type="text" value="1"/>	19 <input type="text" value="2"/>	35 <input type="text" value="3"/>	51 <input type="text" value="4"/>
4 <input type="text" value="1"/>	20 <input type="text" value="2"/>	36 <input type="text" value="3"/>	52 <input type="text" value="4"/>
5 <input type="text" value="1"/>	21 <input type="text" value="2"/>	37 <input type="text" value="3"/>	53 <input type="text" value="4"/>
6 <input type="text" value="1"/>	22 <input type="text" value="2"/>	38 <input type="text" value="3"/>	54 <input type="text" value="4"/>
7 <input type="text" value="1"/>	23 <input type="text" value="2"/>	39 <input type="text" value="3"/>	55 <input type="text" value="4"/>
8 <input type="text" value="1"/>	24 <input type="text" value="2"/>	40 <input type="text" value="3"/>	56 <input type="text" value="4"/>
9 <input type="text" value="1"/>	25 <input type="text" value="2"/>	41 <input type="text" value="3"/>	57 <input type="text" value="4"/>
10 <input type="text" value="1"/>	26 <input type="text" value="2"/>	42 <input type="text" value="3"/>	58 <input type="text" value="4"/>
11 <input type="text" value="1"/>	27 <input type="text" value="2"/>	43 <input type="text" value="3"/>	59 <input type="text" value="4"/>
12 <input type="text" value="1"/>	28 <input type="text" value="2"/>	44 <input type="text" value="3"/>	60 <input type="text" value="4"/>
13 <input type="text" value="1"/>	29 <input type="text" value="2"/>	45 <input type="text" value="3"/>	61 <input type="text" value="4"/>
14 <input type="text" value="1"/>	30 <input type="text" value="2"/>	46 <input type="text" value="3"/>	62 <input type="text" value="4"/>
15 <input type="text" value="1"/>	31 <input type="text" value="2"/>	47 <input type="text" value="3"/>	63 <input type="text" value="4"/>

Figure 14 – QoS Configuration

QoS policy – choose the Strict or WRR prioritize method:

- **Strict** – with this scheduling the higher priority queues are transmitted before transmitting any from the lower priority queues. The value of this type of scheduling is that high priority packets are always handled before low priority packets which is required for voice or video data.

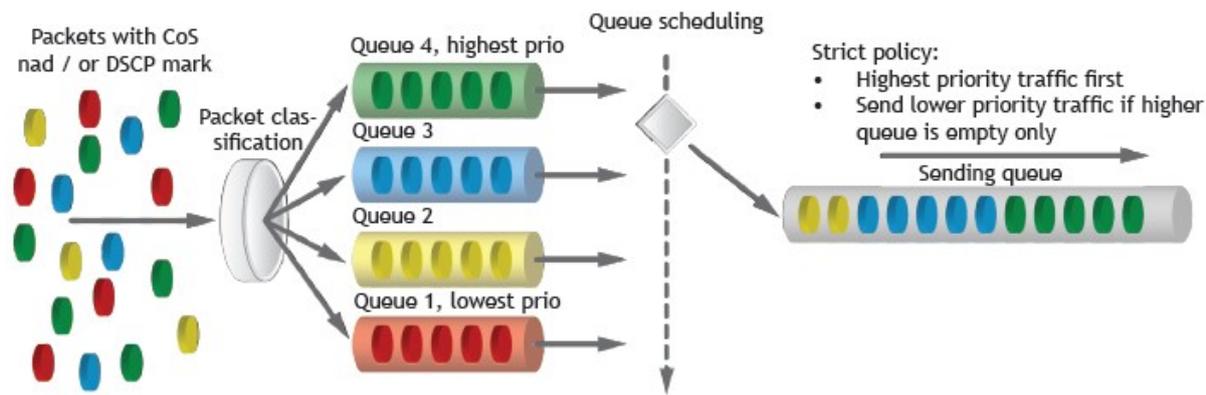


Figure 15 - QoS Policy: Strict

- **WRR** - with this scheduling, a set number of packets from each queue is transmitted, in a round robin algorithm. The higher queue's priority, more packets are transmitted in as the algorithm cycles through the queues in turn. This method guarantees that every queue receives some attention from the port for transmitting packets.

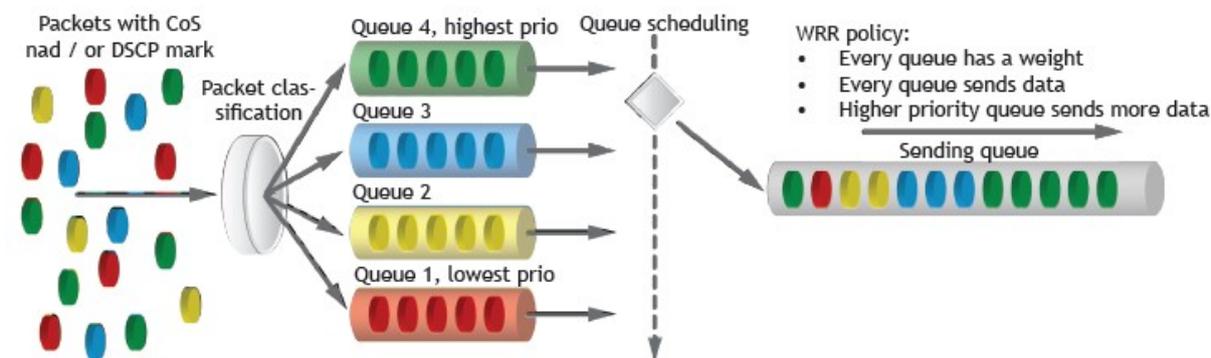


Figure 16 - QoS Policy: WRR

QoS mapping precedence – select the QoS mapping priority either L2 (802.1p) or L3 (DSCP). This option is available only if both types of QoS are enabled.

802.1p settings – enable L2 QoS and specify the priority queue [0-4] for each CoS value (0-7).

DSCP settings – enable L3 QoS and specify the priority queue [0-4] for each DSCP value (0-63).



The queue 1 has the lowest; queue 4 has the highest priority.

DSCP to 802.1p mapping – allows to rewrite 802.1p tags based on DSCP values for VLAN-aware traffic leaving corresponding ETH port



Services

The **Services** menu is divided into further subsections:

- Date & time
- Management
- Wireless management interface
- System alerts

- SNMP
- WNMS
- Firmware update
- Discovery services
- System logging

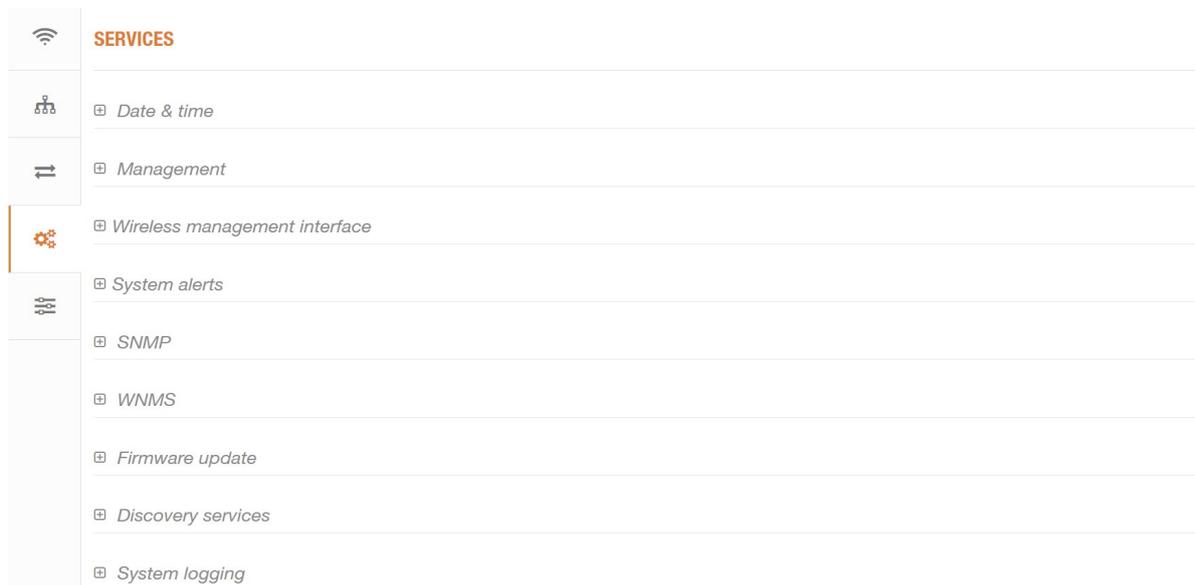


Figure 17 - Services Menu

Date & time

Use this section to manage the system time and date on the device automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the device.

The NTP (Network Time Protocol) client synchronizes the clock of the device with the defined time server. Choose NTP from the configuration menu, select your local time zone and enter NTP server address in order to use the NTP service.

▢ *Date & time*

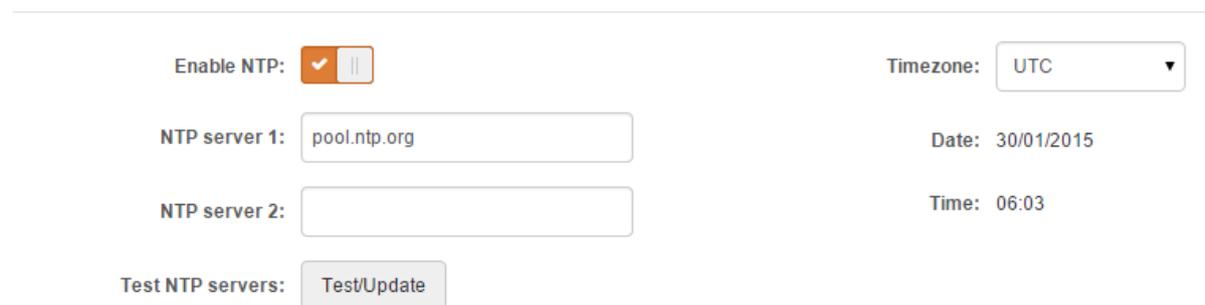


Figure 18 – Date&time: NTP Configuration

Enable NTP – select this option as enabled to configure NTP.

Timezone – select the timezone. Time zone should be specified as a difference between local time and GMT time.

NTP server – specify the trusted NTP server IP or hostname for time synchronization.

Test NTP servers - click this button to check if the specified servers responses successfully.

To adjust the clock settings manually, disable NTP option and specify the following settings on the right side:

☐ Date & time

Enable NTP:

Timezone: UTC

Date (DD/MM/YYYY): 01/05/2014

Time (HH:MM): 00:00

Figure 19 – Date&time: Manual Configuration

Enable NTP – disable this option to set date&time manually.

Timezone – select the timezone. Time zone should be specified as a difference between local time and UTC time.

Date – specify the new date value in format DD/MM/YYYY

Time – specify the time in format HH:MM.

Management

Use this menu to manage access to the LigoPTP via SSH and HTTP:

☐ Management

Enable HTTP:

HTTP port: 80

Enable SSH:

SSH port: 22

Note: HTTPS protocol is always enabled

Figure 20 – Remote Management Configuration

Enable HTTP – select this option to enable or disable management through insecure HTTP.

HTTP port – specify HTTP port. Standard HTTP port is 80.

Enable SSH – enable or disable SSH access to device.

SSH port – specify the SSH service port. By default SSH port is 22.

Wireless management interface

Configure the additional management interface for easy access to the device’s web management interface after newly installed (or rebooted) LigoPTP unit. After successful start, the LigoPTP unit will switch on remote wireless management interface.



LigoPTP unit’s remote wireless management interface is accessible only via HTTPS and SSH via IP: 192.168.111.1. That network is not connected to the transit network traffic and is not reachable from outside.

☐ Wireless management interface

Enable interface:

Activity interval (min):

SSID: LigoWave-mg-12AC3D

Security: WPA/WPA2 Personal

Passphrase: *****

Figure 21 - Management interface configuration

SSID – assign the SSID for remote wireless management interface. Default

Security – choose the security options for remote wireless management access.

Passphrase – specify passphrase for WPA/WPA2 Personal security.

Activity interval – specify interval of remote wireless management interface activity. If no user logs into the LigoPTP web management interface, then, after specified inactivity period, the remote wireless access mode will be switched off automatically. (Default: 5 minutes).

System Alerts

LigoPTP unit is able to send external alerts via SNMP Traps when pre-configured conditions are met or other system events or errors are encountered.

System alerts

Enable system alerts:

System check interval, s:

Wireless link status change:

Ethernet link status change:

RSSI level lower than:

Device reboot:

System uptime:

Uptime send interval, min:

Noise level greater than, dBm:

RX drop greater than, %:

TX retry greater than, %:

Ping delay, ms:

Ping host/IP address:

SNMP traps settings

Manager address:

Manager port:

Trap community:

Use inform:

Retry count:

Retry timeout, s:

Figure 22 - System Alerts Configuration

Enable system alerts – select to enable alert notifications on the system.

System check interval – specify interval in seconds at which the device will send notifications of unexpected system behavior.

System alert types:

Wireless link status change – system will send notification on Wireless link status change.

Ethernet link status change – system will send notification on Ethernet link status change.

RSSI level lower than – system will send notification when RSSI drops below specified value. Default: -60dBm

Device reboot – system will send notification about unexpected or administrator-initiated device reboot.

System uptime – system will send notification about unit’s uptime at preset time intervals.

Uptime send interval – set the time interval, at which the information about device uptime will be send.

Noise level greater than – system will send notification when signal noise will reach value greater than specified. Default: -90 dBm.

RX drop greater than – system will send notification when percentage of RX dropped packets become higher than specified value. Default: 15%.

TX retry greater than – system will send notification when percentage of TX retries becomes higher than specified value. Default: 15%.

Ping delay – if enabled, system will send continuously ping requests to the host, specified below, and in case ping response delay exceeds preset interval (Default: 1000ms), the notification will be sent.

Ping host/IP address – specify the host where the Ping requests will be sent to.

SNMP Traps Settings

Manager address – specify the IP address or hostname of SNMP Trap receiver.

Manager port – specify the port number of the Trap receiver. Default port number is 162.

Trap community - specify the SNMP community string. This community string acts as password between SNMP manager and device. By default, Trap community string is "public".

Use inform – select to wait for an acknowledgment from SNMP manager that the trap was received.

Retry count – specifies maximum number of times to resend an inform request [1-10]. Default: 5.

Retry timeout – specifies number (in seconds) to wait for an acknowledgment before resending request [1-10]. Default: 1.

SNMP

SNMP is the standard protocol that is widely used for remote network management over the Internet. With the SNMP service enabled, the device will act as SNMP agent.

☐ SNMP

Enable SNMP:

Version: v3

R/O username: private

R/O password: *****

Security level: DES encryption (authPriv)

Privacy password: *****

Auth. algorithm: MD5

Figure 23 – SNMP Service Settings

Enable SNMP – starts SNMP service.

Version – select SNMP version number (Version 1/2c or Version 3 are supported).

R/O community or R/O username – specify the read-only community name for SNMP version 1 and version 2c, or SNMP username for SNMP v3. The read-only community allows LigoPTP unit manager to read values, but denies any attempt to change values.

R/O password – specify the password for SNMP Version 3 user.

Security level – choose between authNoPriv and authPriv SNMP v3 Privacy mode with DES. Note that auth mode is always on for SNMP v3, protected with MD5 signature.

Privacy password – specify DES passphrase for authPriv mode SNMP v3.

WNMS

Wireless Network Management System (WNMS) is a centralized monitoring and management system for wireless network devices. The communication between managed devices and the WNMS server is always initiated by the WNMS client service running on every device.

WNMS

The screenshot shows the 'WNMS Agent Settings' configuration page. It includes a toggle switch for 'Enable WNMS agent' which is turned on. Below it is a text input field for 'Server/Collector URL' containing the value 'http://192.168.101.56'. At the bottom, there is a 'Test connection' button with a 'Test' label.

Figure 24 – WNMS Agent Settings

Enable WNMS agent – select to enable WNMS agent.

Server/Collector URL – specify the URL of the WMS server to which that heartbeat notifications will be send.

Test connection - click this button to check if the specified server responses successfully.

Firmware update

LigoPTP unit can be configured to automatically check for new firmware versions and update it from official support website or locally-provided server via HTTP or FTP protocols. That feature is independent from other network-management services. It is disabled by default.

Firmware update

The screenshot shows the 'Firmware Update Service Settings' configuration page. It features a toggle switch for 'Enable auto update' which is turned on. Below this are several configuration fields: 'Source' (a dropdown menu set to 'Custom'), 'Protocol' (a dropdown menu set to 'HTTP'), 'Server address' (a text input field containing '10.10.1.1'), 'Path' (a text input field containing '/firmware'), and 'Period, hours' (a text input field containing '24').

Figure 25 – Firmware Update Service Settings

Enable auto update – starts the auto-update service.

Source – choose between Official support website or custom user-defined server.

Protocol – choose HTTP (anonymous) or FTP transport for updates.

Username – specify FTP username for the custom server.

Password – specify FTP password for the custom server.

Server address – specify the address of the local update server. Note that the Official server address cannot be changed.

Path – specify the local path to the firmware folder on server.

Period – specify the frequency (in hours) to check for updates.

Discovery services

LigoPTP supports mDNS/Bonjour, SSDP and CDP/LLDP protocols to be discovered by neighboring devices and applications in wired and wireless networks to ease network troubleshooting and to verify network integrity.

Discovery services

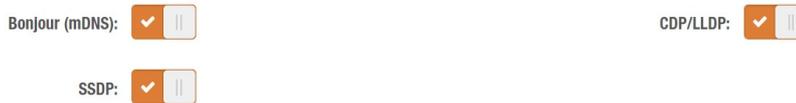


Figure 26 – Discovery Services

System logging

LigoPTP supports SYSLOG to keep the event logs in local RAM and to send the events to a remote SYSLOG server. Local logging is always on and cannot be disabled.

System logging

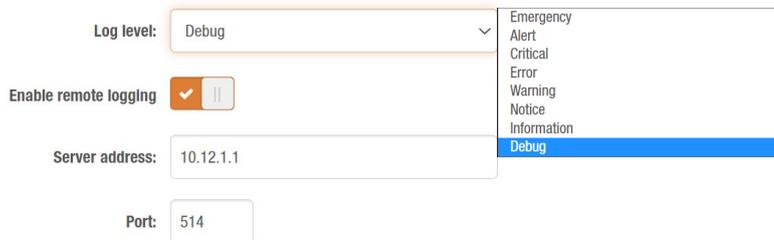


Figure 27 – System logging settings

Log level – choose event detail level, from highest (Debug all events) to lowest (Emergency only).

Enable remote logging – starts sending message to a remote destination.

Server address – specify the IP address of the remote SYSLOG server.

Port – choose destination UDP port on SYSLOG server.



System configuration

System menu is divided into further three sections:

- Device settings
- Security
- Advanced settings

SYSTEM

Friendly name: Latitude:

Location: Longitude:

Contact information: Height AGL, m:

Security

Public status page:

Allow reset to defaults:
(Hardware button behaviour)

Advanced settings

Figure 28 - System Menu

Friendly name – specify name of the LigoPTP that will be used to identify the unit.

Device location – describe the location of the LigoPTP unit.

Contact information – specify the name of the contact person, such as a network administrator, for the LigoPTP.

Longitude – specify the longitude coordinates of the device [specific decimal format, e.q. 54.869446].

Latitude – specify the latitude coordinates of the device [specific decimal format, e.q. 23.891058].

Both coordinates helps indicate accurate location of the device.

Height AGL – specify altitude above ground level in meters.

Security



For security reasons set the password for administrator login and the LigoPTP wireless link as soon as possible.

Security

Password:

Reset button

Public status page:

Allow reset to defaults:

Figure 29 – Security settings



The hardware accelerated AES-128 encryption is used for user access to the device and LigoPTP wireless link protection.

Password – click button to change password that is used to manage access to LigoPTP unit, and LigoPTP wireless link connection.

SET PASSWORD

IMPORTANT: this password is used to manage all devices on the same wireless network and is also used to generate wireless connection security passphrase. On all devices in same wireless network it must be the same otherwise wireless link will not work.

New password

Verify password

New password – enter the new administrator password for user authentication.

Verify password – re-enter the new password to verify its accuracy.



The only way to gain access to the web management if you forget the administrator password is to reset the unit to factory default settings.

Public status page –enable or disable the permission for non-authenticated users to view the Status page.

Allow reset to default – use slide to enable or disable resetting LigoPTP unit using external hardware reset button.

Advanced settings

⊟ *Advanced settings*

LED:

LED timeout, min:

ETH1 port speed:

ETH2 port:

ETH2 port speed:

PoE passthrough to ETH2:

Figure 30 – Advanced device configuration settings

LED – choose LED operation mode:

- **Always off** – LED indication will be always disabled.
- **Always on** – LED indication will be always enabled.
- **Auto off** – LED will be disabled after specified timeout.

ETH port speed – select the ETH1 and/or ETH2 ports speed:

- Auto
- 100Mbps Full Duplex
- 100Mbps Half Duplex
- 10Mbps Full Duplex
- 10Mbps Half Duplex

PoE passthrough to ETH2 – if enabled, the ETH2 interface becomes as PoE source device.



Never connect a **NON-PoE** device to ETH2 interface without verifying that PoE passthrough is **DISABLED!** It is end-user responsibility to always check voltage limits and wiring diagram of the PoE devices used, as they may vary. Irreversible damage may happen instantly in case of miswired or mismatched PoE type used.



ETH2 port acts as Passive PoE source, so DC power will be supplied immediately, without any negotiation protocol. The voltage (up to 57VDC) and remaining power budget are the same as supplied by PoE injector module used, minus losses in the wiring and power consumed by LigoPTP unit itself.

Tools



Figure 31 – Web Management Interface top panel



Site survey

The Site Survey tool shows overview information for wireless networks in a local geographic area. Using this test, an administrator can scan for working wireless devices, check their operating protocol, frequency, bandwidth and see signal/noise levels listed in the table or represented graphically.

To perform the Site Survey test currently, click **Update** button:

SITE SURVEY

Note: results are provided by automatic monitoring in background using dedicated interface

Update

Site	MAC address	Link ID	Protocol	Signal, dBm	Noise, dBm	Freq, MHz	Bandwidth, MHz
remote	44:F0:21:10:08:27	lab2-AR	W-Jet V	-39	-95	5155	5

Last scan: 2015-05-12 16:28:10

Graphical site survey representation

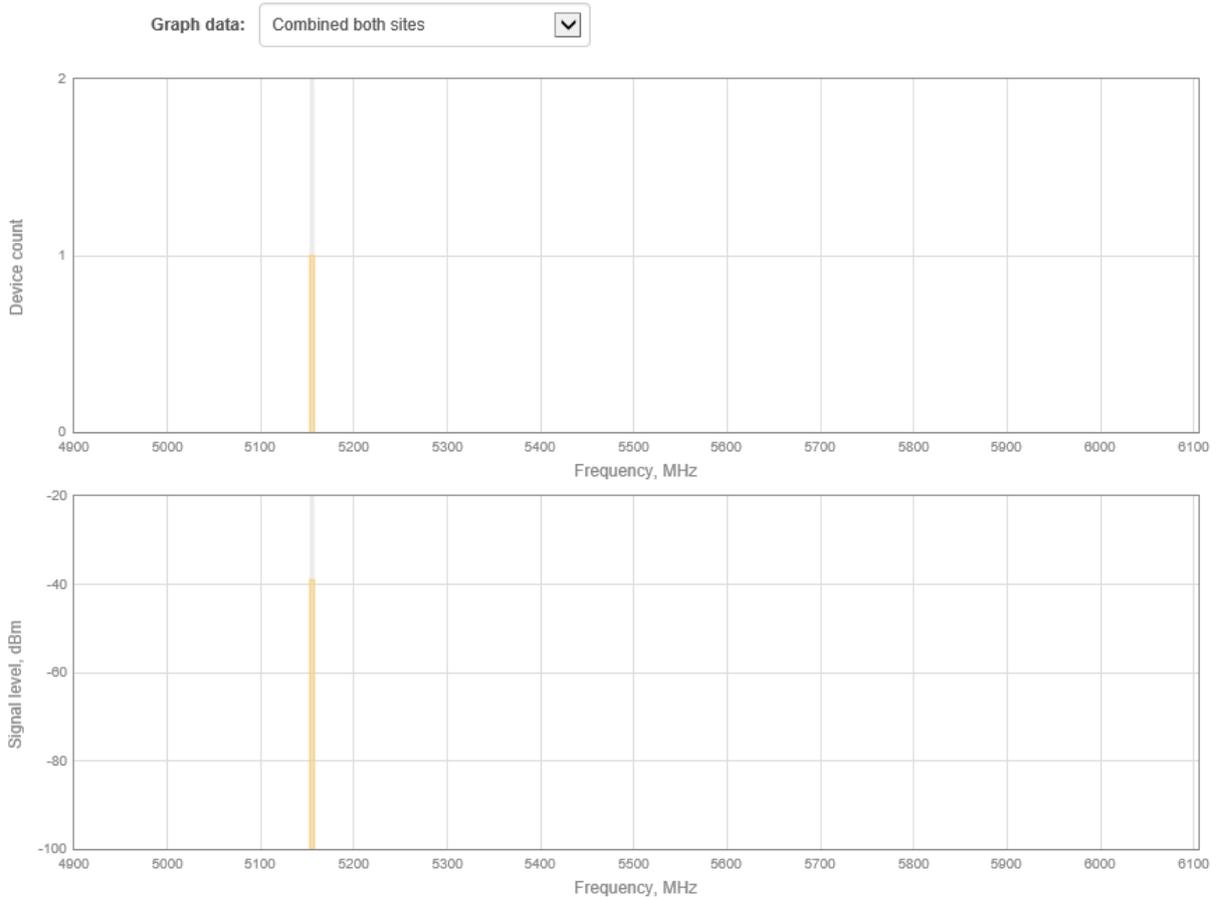


Figure 32 – Site Survey Results

Graph data – choose what data to be displayed in the graphs:

- Only local site
- Only remote site
- Combined both sites



The option **Graph data** will be hidden if Master received no data from Slave unit or unit is operating as Slave.

Link test



It is recommended to ensure that there is no user traffic on the link before running the **Link test** as results may not be accurate.

Use the Link test tool to check the quality of the established **LigoPTP** link. This tool tests the throughput at selected packet sizes using several iterations.

LINK TEST

Packet size (bytes): 64 / 512 / 1024 / 1600
 Slave device: AutoTest... (00:19:3B:04:DA:66)
 Iterations: 20
 Traffic direction: From Local to Remote

Traffic direction: From Local to Remote Finished: May 13, 2015 11:17:22 AM

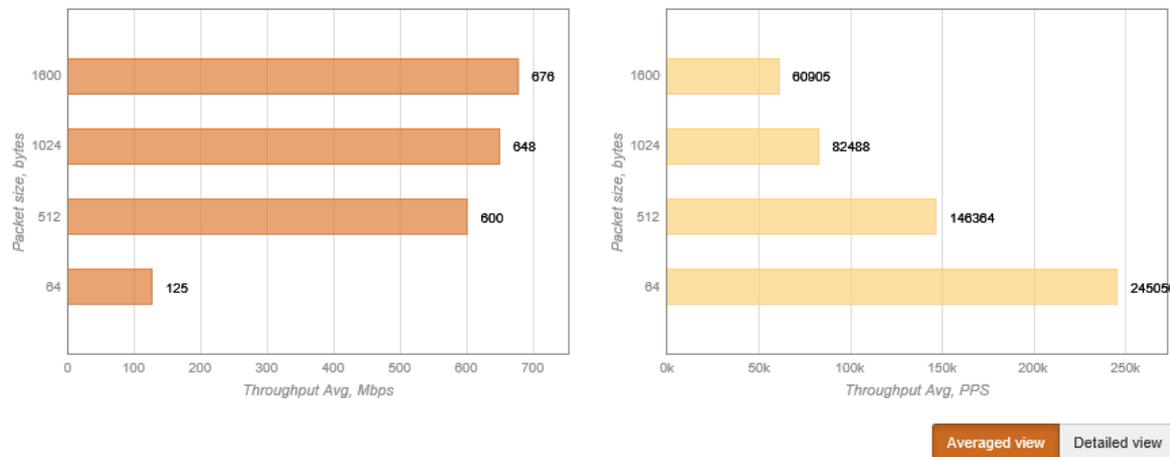


Figure 34 – Linktest Results

Packet size – select packet sizes in bytes at which the test will be performed.

Iterations – select number of test iterations.

Master device – displays information of the Master unit (Slave side) of the established LigoPTP link.

Slave device – displays information of the Slave unit (Master side) of the established LigoPTP link.

Traffic direction – select the traffic direction for the performing test.

Start/Stop – click to start or to stop the throughput test.

Spectrum analyzer

The **Spectrum analyzer** displays detailed information about spectrum usage at LigoPTP unit's receiver. Current, Maximum and Average levels are displayed for each frequency up to 250kHz resolution. Spectrograph screen displays 3D spectrum usage data, where color temperature represents the signal level and its density is proportional to the painted area on the graph. This enables administrator to choose the best available frequency/channel for the link operation. The frequency list depends on the Country at which the unit is operating, and chosen channel width.



Spectrum analyzer may temporary disable wireless link. Spectrum analyzer will stop automatically after full spectrum scan is done.

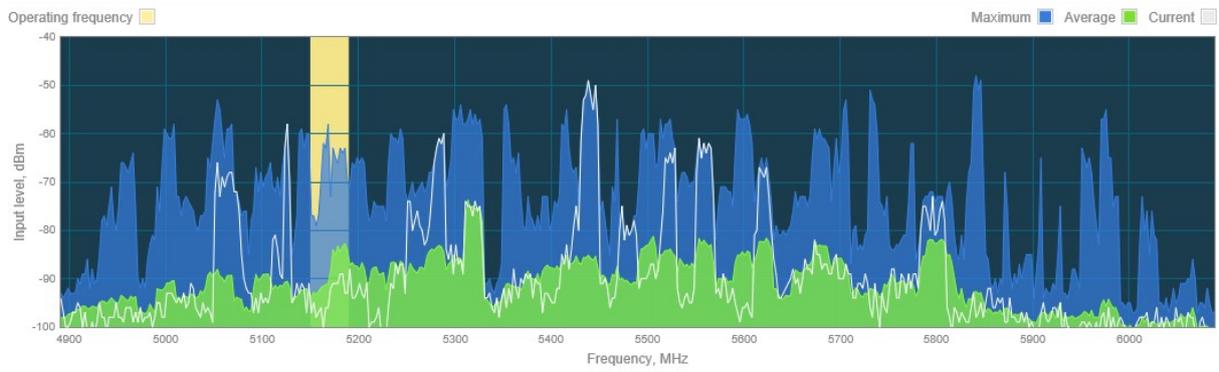
Click **Start** button to perform the test:

SPECTRUM ANALYZER

Caution: starting spectrum analyzer will disable wireless link.



Spectrum realtime



Spectrograph

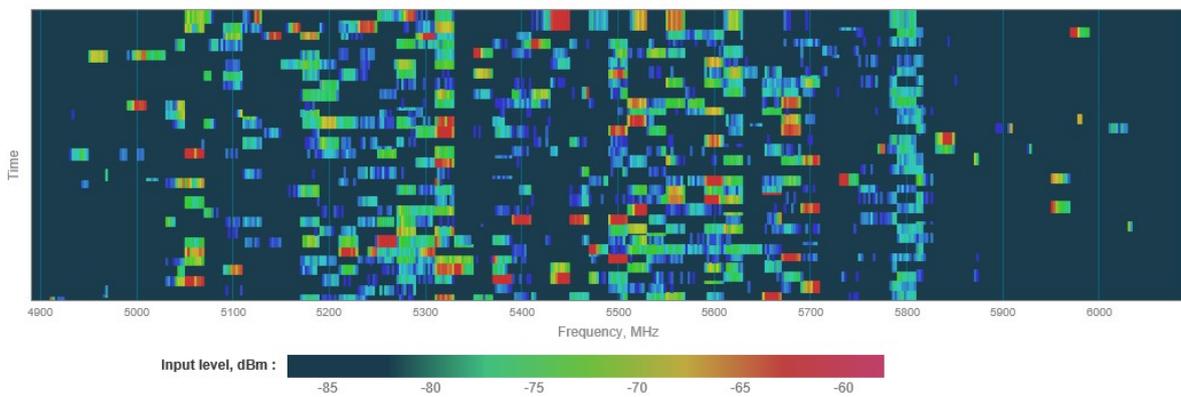


Figure 35 - Spectrum analyzer results



The **highlighted** column represents operating frequency of current LigoPTP link.



Ping & Trace

Use **Ping** tool to discover how long it takes for packets to reach the specified trusted host. The ping results are displayed in the table and graphically:

PING & TRACE

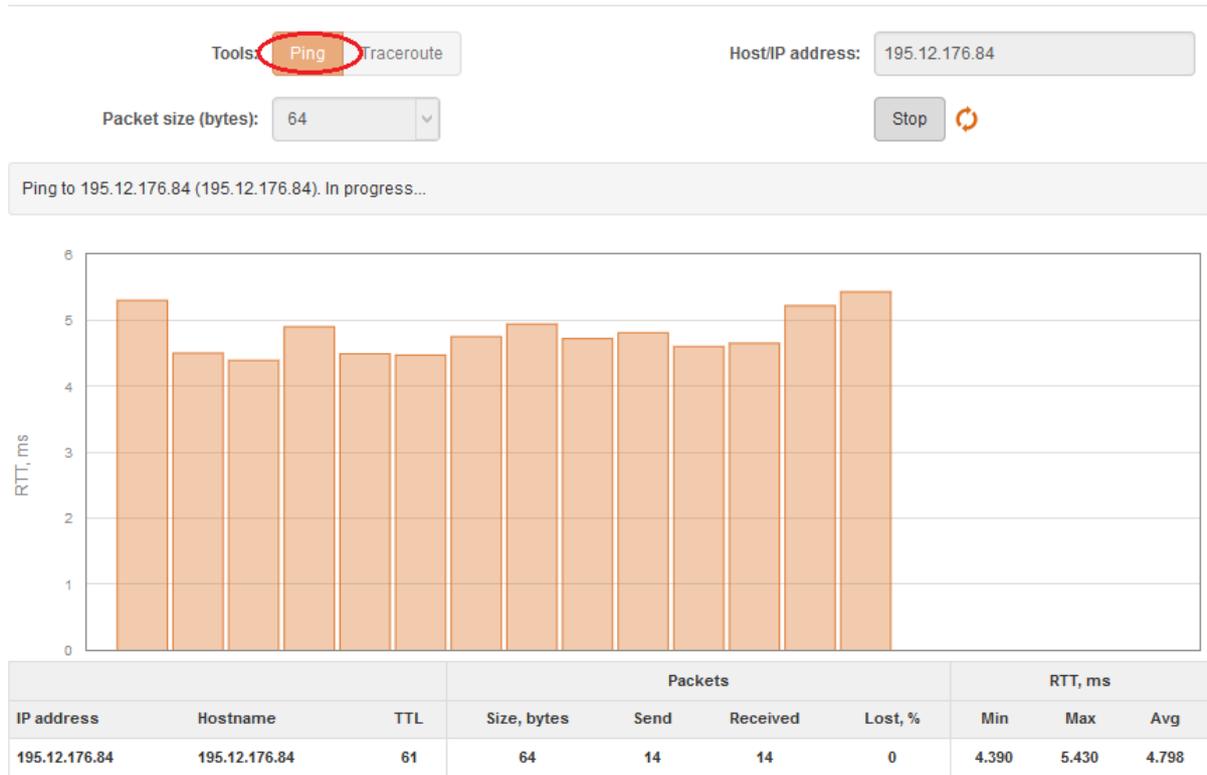


Figure 36 - Ping tool

Host/IP address – specify the host where the Ping requests will be sent to.

Packet size (bytes) – specify the size in bytes of the packet.

Start/Stop – click to start or stop ping tool.

Use **Traceroute** tool to track the route of packets to the destination host from current unit. This is useful when trying to find out why destination is unreachable, as you may be able to see where the connection fails.

PING & TRACE

Tools:

Host/IP address:

Max hops (TTL):



Tracing 195.12.176.84. In progress...

Hop	IP address	Hostname	Send/Recv	Min, ms	Avg, ms	Max, ms
1	10.0.95.1	10.0.95.1	3/3	0.263	0.378	0.463
2	*	*	3/0	--	--	--
3	82.135.182.3	82-135-182-3.static.zebra.lt	3/3	4.594	4.896	5.231
4	*	*	3/0	--	--	--

Figure 37 - Trace tool

Host/IP address – specify hostname or IP address of the target host.

Max hops (TTL) – specify the maximum number of hops to search for target.

Start/Stop – click to start or stop trace tool.

Maintenance

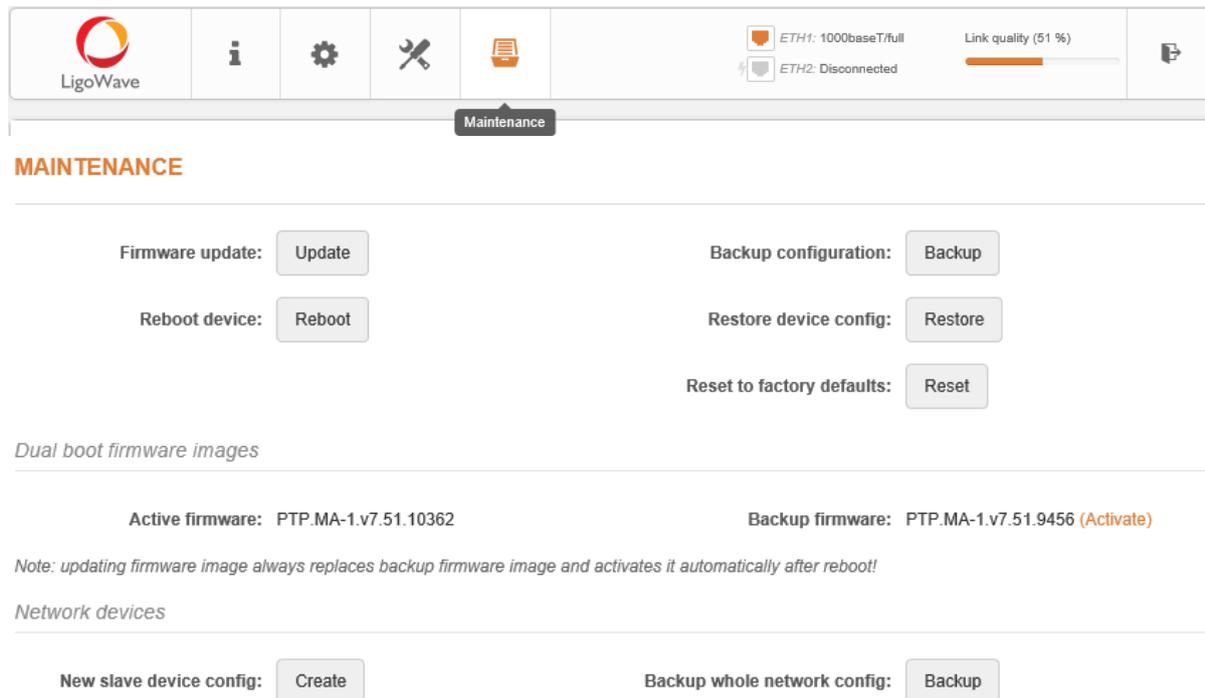


Figure 38 – Maintenance: system functions

Reboot device – click to reboot device with the last saved configuration.

Backup configuration – click to save the current configuration file. The saved configuration file is useful to restore a configuration in case of a device misconfiguration or to upload a standard configuration to multiple devices without the need to configure manually each device through the web interface.

Restore device config – click to upload an existing configuration file to the LigoPTP unit. If unit operates as Master, then there is a possibility to restore Slave’s configuration as well.

Reset device to factory defaults – click to restore unit’s factory configuration.



Resetting the device is an irreversible process. Current configuration and the administrator password will be set back to the factory default.



All LigoPTP devices have physical reset button, located on the back side of the device. This button is able to perform the following functions:

- Activate LED indication** - click once,
- Switch to RSSI or Status indication** – click once,
- Enable WiFi management radio** - hold until 3 Blue LEDs are on,
- Reset device to factory defaults** - hold until all Blue LEDs start to blink.

Firmware upgrade



The firmware upgrade is safe for all existing configuration settings. When the device is upgraded with a newer version or the same version builds, all the system’s configuration will be preserved after the upgrade. During downgrade, however, the new settings that were not supported in the older firmware may be lost or replaced with default values.

Click the **Update** button and select the proper firmware image in the **Firmware Update** pop-up window:

FIRMWARE UPDATE

Select a File to Upload

PTP.MA-1.v7.51.10427.img Browse...

Device	Mode	Current version
PTP master	Master	PTP.MA-1.v7.51.10362
PTP managed	Slave	PTP.MA-1.v7.51.10362

Upload Close

Figure 39 – Firmware Upload

The new firmware image uploaded to the unit’s temporary memory. It is necessary to save the firmware into the device permanent memory. Click the **Upload** button.

After the FW image successfully uploaded, the dialog box displays table with LigoPTP link units. It is now available to choose which devices to upgrade. By default, both devices of the LigoPTP link (Master and Slave) are ready for system firmware upgrade.

FIRMWARE UPDATE

Select a File to Upload

PTP.MA-1.v7.51.10427.img Browse...

New firmware file uploaded: PTP.MA-1.v7.51.10427

<input checked="" type="checkbox"/>	Device	Mode	Current version
<input checked="" type="checkbox"/>	PTP master	Master	PTP.MA-1.v7.51.10362
<input checked="" type="checkbox"/>	PTP managed	Slave	PTP.MA-1.v7.51.10362

Note: master device is updated last!

Update Close

Figure 40 –Firmware Upgrade

Update – click to upgrade device with the uploaded image and reboot the system.



Do not switch off and do not disconnect the device from the power supply during the firmware upgrade process as the device flash memory could be damaged.

Dual boot firmware images

LigoPTP units have factory installed default dual-boot firmware. With a new firmware upgrade, the backup firmware is overwritten each time.

Dual boot firmware images

Active firmware: PTP.MA-1.v7.51.10362

Backup firmware: PTP.MA-1.v7.52-DEVEL.9456 (Activate)

Figure 41 - Dual-boot firmware images

Activate – click link to activate backup firmware. Backup firmware will be activated after reboot.

Network devices

Network devices

New slave device config: Backup whole network config:

Figure 42 – Network device configuration

Backup whole network config – click **Backup** to download configuration files of whole LigoPTP link. The downloaded file will contain two configurations: Master's and Slave's.

New slave device config – click to setup and download a new configuration file for Slave unit. After the **Create** button clicked, the dialog window with some Slave's configuration parameters appears:

NEW SLAVE DEVICE CONFIGURATION

Friendly name:

Location:

Latitude:

Longitude:

Height AGL, m:

IPv4 settings

IP method:

IP address:

Subnet mask:

Default gateway:

Figure 43 – Slave device config setup

Download – click to save a new created configuration file for Slave unit.



Support

The **troubleshooting file** contains valuable information about device configuration, log files, command outputs, etc. Device quickly gathers troubleshooting information automatically, rather than requiring you to gather each piece of information manually. This is helpful for submitting detailed problem description into the support ticket, or keeping “baseline” records after new link deployment.

TROUBLESHOOTING

Troubleshooting file: Download

System Log

Read log

```

May 14 03:08:00 syslogd started: BusyBox v1.21.1
May 14 03:08:00 kernel: [ 3.124968] 5 cmdlinepart partitions found on MTD device armada-nand
May 14 03:08:00 kernel: [ 3.131345] 5 cmdlinepart partitions found on MTD device armada-nand
May 14 03:08:00 kernel: [ 3.137718] Creating 5 MTD partitions on "armada-nand":
May 14 03:08:00 kernel: [ 3.142963] 0x000000000000-0x000000380000 : "u-boot"
May 14 03:08:00 kernel: [ 3.148949] 0x000000380000-0x000000600000 : "u-boot-env"
May 14 03:08:00 kernel: [ 3.155211] 0x000000600000-0x0000002e0000 : "firmware1"
May 14 03:08:00 kernel: [ 3.161399] 0x0000002e0000-0x000000560000 : "firmware2"
May 14 03:08:00 kernel: [ 3.167605] 0x000000560000-0x0000007f0000 : "data"
May 14 03:08:00 kernel: [ 3.173827] UBI: attaching mtd3 to ubi0
May 14 03:08:00 kernel: [ 3.177687] UBI: physical eraseblock size: 131072 bytes (128 KiB)
May 14 03:08:00 kernel: [ 3.183972] UBI: logical eraseblock size: 126976 bytes
May 14 03:08:00 kernel: [ 3.584336] o TX Queue support: 8 Queues * 532 Descriptors
May 14 03:08:00 kernel: [ 3.590010] o GSO supported
May 14 03:08:00 kernel: [ 3.592985] o GRO supported
May 14 03:08:00 kernel: [ 3.595961] o Receive checksum offload supported
May 14 03:08:00 kernel: [ 3.600764] o Transmit checksum offload supported
May 14 03:08:00 kernel: [ 3.605655] o Driver ERROR statistics enabled
May 14 03:08:00 kernel: [ 3.610197]
May 14 03:08:00 kernel: [ 3.611812] o Loading network interface(s)
May 14 03:08:00 kernel: [ 3.616031]
                    
```

Figure 44 – Troubleshooting File Download

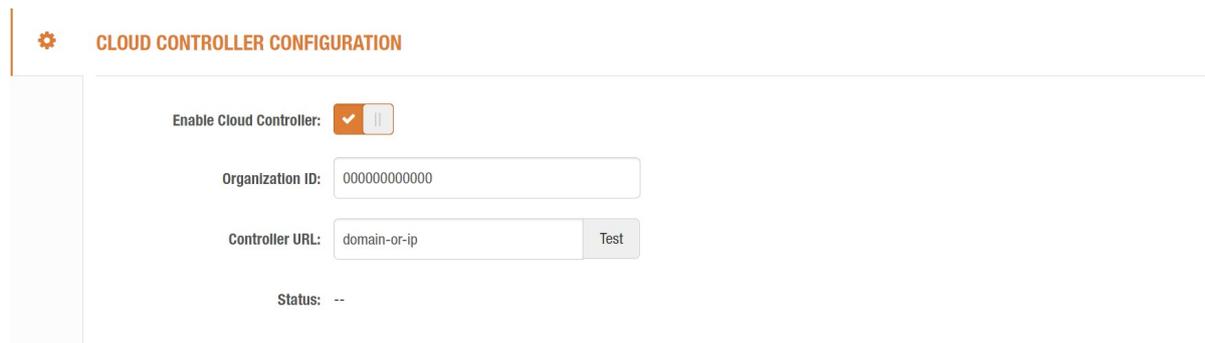
Troubleshooting file – click to download the troubleshooting file. This may take a few minutes to gather information and to complete download.

System log - this viewer utility provides debug information about the system services and protocols. If the device's malfunction occurs, recorded messages can help operators to locate configuration issues and system errors.



Cloud Controller Configuration

LigoPTP units can be managed and monitored on LigoWave Controller. Only one of the management methods, WNMS or Controller, can be enabled. Note that since LigoPTP device is successfully onboarded in Management mode on the Controller, it will become impossible to modify most of its configuration settings locally, without disabling the Controller agent. Configuration changes done and saved from the Controller will not be lost after disabling Controller agent.



CLOUD CONTROLLER CONFIGURATION

Enable Cloud Controller:

Organization ID:

Controller URL:

Status: --

Figure 45 – Cloud Controller Configuration

Enable Cloud Controller – starts Controller agent on the device.

Organization ID - identifies the network on the Controller to which that device belongs.

Controller URL – IP address or URL of the Controller to connect to. Note that IP Default gateway and DNS server must be already configured in the Network settings to reach the Controller.

Test – verify connection to the Controller, test will pass only if Organization ID is correct.

Status - displays current communication status to the Controller.