Copyright

© 2016 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 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.

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.

R&TTE compliance statement

Safety
This equipment is designed with the utmost care for the safety of those who install 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
CE mark warning .............................................................................................................. 3
R&TTE compliance statement ......................................................................................... 3
Safety ................................................................................................................................. 3
EU countries intended for use .......................................................................................... 3
EU countries not intended for use .................................................................................... 3

### ABOUT THIS GUIDE

Purpose ............................................................................................................................ 5
Definitions, acronyms and abbreviations ....................................................................... 5
Abbreviation list ............................................................................................................... 5

### DEVICE ACCESS

First connection via Ethernet .......................................................................................... 7
Windows OS ....................................................................................................................... 7
MAC OS ............................................................................................................................ 8
Linux (Ubuntu) ................................................................................................................. 8
First access to web management interface ...................................................................... 8

### LIGOWAVE NFT CONFIGURATION

Applying and saving configuration changes ................................................................. 10
Status ............................................................................................................................... 10
Information ...................................................................................................................... 11
Statistics ......................................................................................................................... 12
Wireless .......................................................................................................................... 13
Settings ........................................................................................................................... 15
Network configuration ................................................................................................... 15
IPv4 configuration .......................................................................................................... 15
IPv6 configuration .......................................................................................................... 16
Wireless settings ............................................................................................................ 17
  Advanced radio settings ............................................................................................... 18
  Wireless networks (VAP) settings ................................................................................ 19
  Wireless security .......................................................................................................... 19
  Wireless ACL ............................................................................................................... 21
  Advanced settings ....................................................................................................... 22
Services configuration .................................................................................................... 23
  Date & time ................................................................................................................... 23
  Remote management .................................................................................................... 24
SNMP ............................................................................................................................... 24
WNMS ............................................................................................................................. 25
System configuration ...................................................................................................... 25
  Device settings ............................................................................................................. 26
  System functions ......................................................................................................... 26
  User accounts .............................................................................................................. 27
  Advanced settings ....................................................................................................... 27
Firmware upgrade .......................................................................................................... 28
Tools ................................................................................................................................. 29
Site survey ....................................................................................................................... 29
Support ............................................................................................................................ 30
Troubleshooting ............................................................................................................. 30
System log ...................................................................................................................... 30

### INDEX

........................................................................................................................................ 31
About This Guide

Purpose
This document provides information and procedures on installation, setup, configuration, and management of the LigoWave NFT 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 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.

Abbreviation list

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>ACK</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>AMSDU</td>
<td>Aggregated Mac Service Data Unit</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>ATPC</td>
<td>Automatic Transmit Power Control</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Control Protocol</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>GHz</td>
<td>Gigahertz</td>
</tr>
<tr>
<td>GMT</td>
<td>Greenwich Mean Time.</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical User Interface</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LED</td>
<td>Light-Emitting Diode</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>Mbps</td>
<td>Megabits per second</td>
</tr>
<tr>
<td>MCS</td>
<td>Modulation and Coding Scheme</td>
</tr>
<tr>
<td>MHz</td>
<td>Megahertz</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>MSCHAPv2</td>
<td>Microsoft version of the Challenge-handshake authentication protocol, CHAP.</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication dial In User Service</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector</td>
</tr>
<tr>
<td>RX</td>
<td>Receive</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TTLS</td>
<td>Tunneled Transport Layer Security (EAP-TTLS) protocol</td>
</tr>
<tr>
<td>TX</td>
<td>Transmission</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VAP</td>
<td>Virtual AP</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>WACL</td>
<td>Wireless Access Control List</td>
</tr>
<tr>
<td>WISPr</td>
<td>Wireless Internet Service Provider roaming</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access 2</td>
</tr>
</tbody>
</table>
Device Access

First connection via Ethernet

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

In case the LigoWave NFT 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 LigoWave NFT device via Ethernet.

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

![Network Discovery](image)

**Step 3:** Find the required LigoWave NFT device icon:

![Device Icon](image)

**Step 4.** Double-click on LigoWave NFT device icon – you will be redirected to the device webpage automatically.
MAC OS

**Step 1:** Connect your PC to the LigoWave NFT device via Ethernet.

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

![Bonjour Application](image)

**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 LigoWave NFT 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 (0001E6860DF4D) Web Site local
+ eth0 IPv4 NFT 2N (192.168.5.10, 00:19:38:00:8A:DA) Web Site local
+ eth2 IPv4 HP LaserJet 2200 (0001E6860DF4D) Web Site local
hostname = [NPI60DF4D.local]
address = [192.168.100.145]
port = [80]
txt = []
...= eth0 IPv4 NFT 2N (192.168.5.10, 00:19:38:00:8A:DA) Web Site local
hostname = [NFT.2N-088ADA.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

The default administrator login settings are:

- **Login:** admin
- **Password:** admin01

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

**Step 1.** Start your Web browser.
Step 2. Enter the device IP address in the web browser’s IP field and specify default login settings **admin/admin01**.

The initial login screen looks as follow:

![Login Screen]

Step 3. **Confirm the user agreement.** According to the chosen country the regulatory domain settings may differ. You are not allowed to select radio channels and RF output power values other the permitted values for your country and regulatory domain.

**Operating Country**

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:** United States

2.4 GHz Antenna gain, dBi: 3

5 GHz Antenna gain, dBi: 3

Change Cancel

Step 4. After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.
LigoWave NFT Configuration

This document contains product's powerful web management interface configuration description allowing setups ranging from very simple to very complex.

Applying and saving configuration changes

There is one general button containing three actions 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.

It is not required to press **Save changes** in every Web GUI tab. The device remembers all changes made in every tab and after action button is used, all changes will be applied.

Status

After login, the main Web management page displays Status Information page. The header of Web management page displays main information about device: Firmware version, Product name, Uptime, CPU load, Ethernet port(s) status, Connected client count.

![Status Information](image)

Figure 1 - Web Management Interface
Information

The Information page displays a summary of status information of your device. It shows important information for the LigoWave NFT operating mode, radio and network settings.

The Information page of a dual-band device is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

Wireless (AP) – table displays general VAP (Virtual AP) information: SSID, Security type, SSID Broadcast status, VLAN and number and connected clients.

Network – displays a short summary about current network configuration.

Click the refresh icon, on the upper right corner, to update information.
Statistics

The **Statistics** sections id divided into two sections and displays network interface counters and traffic graphs of wired and wireless interfaces:

### Interface counters

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC address</th>
<th>Tx data</th>
<th>Rx data</th>
<th>Tx packets</th>
<th>Rx packets</th>
<th>Tx errors</th>
<th>Rx errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>ath0</td>
<td>00:19:3b:02:3b:5b0</td>
<td>20.05 MB</td>
<td>667.05 MB</td>
<td>161.13 k</td>
<td>5.53 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>eth0 (ssid)</td>
<td>00:19:3b:02:3b:5b2</td>
<td>1.16 GB</td>
<td>544.15 MB</td>
<td>66.16 M</td>
<td>163.08 M</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2.4 GHz (Radio 1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ath0 (2G)</td>
<td>00:19:3b:02:3b:5b0</td>
<td>2.50 GB</td>
<td>210.67 MB</td>
<td>5.40 M</td>
<td>1.10 M</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>ath4 (2G-F)</td>
<td>12:19:3b:02:3b:5b0</td>
<td>573.88 MB</td>
<td>798.45 MB</td>
<td>12.96 M</td>
<td>4.60 M</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>ath2 (guest)</td>
<td>02:19:3b:02:3b:5b0</td>
<td>139.55 MB</td>
<td>5.49 KB</td>
<td>429.99 k</td>
<td>21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5 GHz (Radio 2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ath5 (5G-F)</td>
<td>12:19:3b:02:3b:5b1</td>
<td>3.38 GB</td>
<td>238.28 MB</td>
<td>56.52 M</td>
<td>36.28 M</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>ath1 (5G)</td>
<td>00:19:3b:02:3b:5b1</td>
<td>1.46 GB</td>
<td>3.39 GB</td>
<td>30.27 M</td>
<td>24.38 M</td>
<td>0</td>
<td>9.11 k</td>
</tr>
<tr>
<td>ath3 (guest)</td>
<td>02:19:3b:02:3b:5b1</td>
<td>42.57 MB</td>
<td>0</td>
<td>153.65 k</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 3 – Network Statistics: Interface counters**

- **Interface counters** – displays table of interface statistics. The SSID name is displayed in the brackets near the radio interface (and VAPs).
- **MAC address** – displays the MAC address of the particular interface.
- **Tx data** – displays the transmitted data.
- **Rx data** – displays the received data.
- **Tx packets** – displays the number of transmitted packets.
- **Rx packets** – displays the number of received packets.
- **Tx errors** – displays the number of the TX errors.
- **Rx errors** – displays the number of the RX errors.

The wired and wireless interface graphs display real-time data traffic.
The Wireless page displays the receive/transmit statistics between AP and successfully associated wireless clients (click Counters tab, if necessary to view information of connected clients in Rx/Tx numerical expressions):
Figure 5 – Access Point's Wireless Statistics

The Wireless page of a dual-band device is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

In case the access point has more than one wireless interface (VAPs), the appropriate number of tables with information about connected wireless clients will be displayed.

Station – displays MAC address and Friendly name of the successfully connected wireless client.

IP address – displays wireless client IP address.

Signal – indicates the signal strength of the access point main and auxiliary antennas that the station communicates with displayed dBm.

Tx/Rx rate – displays transmit/receive data rates in Mbps.

Tx/Rx CCQ, % - displays the wireless Client Connection Quality (CCQ), the value in percent that shows how effective the bandwidth is used regarding the theoretically maximum available bandwidth.

Protocol – displays the protocol at which the access point communicates with the particular station.

Link uptime – displays the duration of the particular session.

Kick selected – select to end the connection to this station.

Click the refresh icon, on the upper right corner, to update statistics.
Network configuration

The Settings | Network Configuration page allows you to control the network LAN configuration of the device.

IPv4 configuration

**NETWORK CONFIGURATION**

**IPv4 configuration**

<table>
<thead>
<tr>
<th>IP method: Static</th>
<th>DNS server 1: 192.168.100.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address: 192.168.2.66</td>
<td>DNS server 2:</td>
</tr>
<tr>
<td>Subnet mask: 255.255.255.0</td>
<td>Secondary IP:</td>
</tr>
<tr>
<td>Default gateway: 192.168.2.1</td>
<td>IP address: 192.168.2.250</td>
</tr>
<tr>
<td></td>
<td>Subnet mask: 255.255.255.0</td>
</tr>
</tbody>
</table>

*Figure 6 – IPv4 LAN Settings*

**Management VLAN** – select to enable a VLAN tagging for management traffic. Access to the AP for management purposes can further be limited using VLAN tagging. By defining Management VLAN, the device 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 device interfaces are configured with a specific VLAN ID value, only management frames that matching configured VLAN ID will be accepted by device.

When you specify a new management VLAN, your HTTP connection to the device will be lost. For this reason, you should have a connection between your management device and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN router.
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 must be specified manually.
- **Dynamic** – the IP address for this device will be assigned from the DHCP server. 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 device

**Subnet mask** – specify a subnet mask for device.

**Default gateway** – specify a gateway IP address for device.

**DNS server** – specify the Domain Naming Server.

**Secondary IP** – specify the alternative IP address and the netmask for LigoWave NFT unit management.

### IPv6 configuration

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

![Network Configuration](image)

**IPv4 configuration**

- **IP method**: Static
- **IP address**: 192.168.2.06
- **Subnet mask**: 255.255.255.0
- **Default gateway**: 192.168.2.1
- **DNS server 1**: 192.168.100.2
- **DNS server 2**: 
- **Secondary IP**
- **IP address**: 192.168.2.250
- **Subnet mask**: 255.255.255.0

**IPv6 configuration**

- **IPv6 method**: Static
- **IPv6 address**: fc00:0:a0:2:42
- **IPv6 prefix length**: 64
- **IPv6 default gateway**: fc00:0:a0:2:1
- **IPv6 DNS server 1**: 
- **IPv6 DNS server 2**: 

*Figure 7 – IPv6 LAN Settings*
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 must 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.

### Wireless settings

Before changing radio settings manually 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 page of the LigoWave NFT device web management is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate wireless settings:

**WIRELESS CONFIGURATION**

![Operating country: US](image)

**2.4 GHz (Radio 1)**

- **Enable radio**: use slide to enable or disable
- **IEEE mode**: 802.11b/g/n
- **Channel**: Auto / 40 MHz
- **Tx power (dBm)**: 10

**Advanced radio settings**

**Wireless networks (AP)**

<table>
<thead>
<tr>
<th>Network SSID</th>
<th>Security</th>
<th>Management</th>
<th>Broadcast SSID</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2.4</strong></td>
<td>WPA/WPA2 Enterprise</td>
<td>Enabled</td>
<td>Yes</td>
<td>--</td>
</tr>
</tbody>
</table>

*Figure 8 – Wireless Configuration*

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

**Enable radio** – use slide to enable or disable particular LigoWave NFT radio.

**IEEE mode** – specify the wireless network mode, depending on radio [802.11a, 802.11n, 802.11a/n].
**Tx power (dBm)** – set the unit’s transmitting 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. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

**Channel** – displays the channel at which the AP is operating, or indicates that autochannel function is used. Click on the **Channel** button and the channel selection window will be displayed:

![Channel Selection Window]

**Channel width** – select the width of the operating radio channel. The LigoWave NFT supports 20, 40 Lower and 40 Upper channel widths.

**Channel table** – select the channel(s) at which the NFT AP will operate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows AP 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 least occupied. The table displays detailed information about each channel: TX limit, EIRP limit and DFS or ATPC.

**Advanced radio settings**

Advanced parameters allow configuring the device to get the best performance/capacity of the link:

![Advanced Radio Settings]

**AMSDU** – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased. Available only on 802.11n or 802.11a/n IEEE modes.

**BA window size** – specify BA (Block ACK) window size in frames [1-64].

**RTS/CTS** – specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.
Wireless networks (VAP) settings

Each LigoWave NFT unit supports up to eight (8) VAPs peer radio.

The **Wireless Networks** table allows to configure the principal wireless radio parameters as well as create another 8 wireless networks (Virtual APs) in addition per radio. All VAPs may be active at the same time meaning that client devices can associate to the access point using any of the VAPs.

**Wireless Networks (AP)**

<table>
<thead>
<tr>
<th>Network SSID</th>
<th>Security</th>
<th>Management</th>
<th>Broadcast SSID</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>X3</td>
<td>WPA/WPA2 Enterprise</td>
<td>Enabled</td>
<td>Yes</td>
<td>–</td>
</tr>
</tbody>
</table>

*Figure 11 - Wireless Settings*

Click on the icon for editing, or click on **Add virtual AP** button to create a new VAP:

**WIRELESS AP SETTINGS**

- **SSID**: LigoWave AP
- **Broadcast SSID**

*Security settings*

- **Security**: Open

*WACL*

- **Advanced settings**

*Figure 12 – Wireless AP Settings*

**SSID** – specify the SSID of the wireless network.

**Broadcast SSID** – enables or disables the broadcasting of the SSID.

For detailed information about security settings and WACL refer at the respective sections **Wireless security** and **Wireless ACL**.

**Wireless security**

The wireless security settings will be used by the wireless stations for association, thus wireless station security settings must conform the settings configured on the AP that station is associated with.

Each VAP of the LigoWave NFT supports following authentication/encryption methods:
- **Open** – no encryption.
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals.
- **Enterprise WPA/WPA2** – RADIUS server based authentication (requires configured RADIUS server).

**Open**

By default there is no encryption enabled on the LigoWave NFT device:

![Security settings](image)

*Figure 13 – Wireless Security: Open with RADIUS MAC Authentication Enabled*

**WPA/WPA2 Personal**

To setup WPA/WPA2 Personal encryption, need to select appropriate security type and specify the passphrase:

![Security settings](image)

*Figure 14 – Wireless Security: Personal WPA/WPA2 Security*

**Passphrase** – specify WPA or WPA2 passphrase [8-63 characters].

**WPA/WPA2 Enterprise for Access Points**

LigoWave NFT has possibility to configure WPA/WPA2 Enterprise encryption with RADIUS authentication. Properly configured AP will accept wireless stations requests and will send the information to configured RADIUS server for client authentication.

![Security settings](image)
The properly configured RADIUS server is required for **WPA/WPA2 Enterprise** encryption.

**Auth. server IP/Port** – specify the IP address and the port of the authentication RADIUS server where the authentication requests will be sent to.

**Auth. server key** – enter the key for the authentication on specified RADIUS server.

**Accounting server** – use slide to enable accounting RADIUS server, if required.

**Acc. server IP/Port** – specify the IP address and the port of the accounting RADIUS server where the accounting stats will be sent to.

**Acc. server key** – enter the key for the authentication on specified accounting RADIUS server.

**Wireless ACL**

Access Control provides the ability to limit associations wirelessly, based on MAC address, to an AP by creating an Access Control List (ACL) on each wireless interface (including VAPs).

**MAC filter policy** – define the main VAP policy:

- **Open** – no rules applied.
- **Allow MAC in the list** – only listed MAC clients can connect to the VAP (white list).
- **Deny MAC in the list** – only listed MAC clients can NOT connect to the VAP (black list).

To add new rule, click the **Add** button, specify MAC address and click verification icon ✅.

To remove the rule, click the delete icon ✗ next to required record.

To edit the rule, click the pencil icon ✒ next to required record.
**Advanced settings**

**WIRELESS AP SETTINGS**

- **SSID:** LigoWave AP
- **Broadcast SSID:**

**Security settings**

- **Security:** Open

**WACL**

**Advanced settings**

- **Client isolation:**
- **Max connected clients:** 126
- **Min client signal (dBm):** -100
- **Map to data VLAN ID:** 10
- **Management over wireless:** Enabled

*Figure 17 – VAP Advanced Settings*

**Client isolation** – select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) and Access Point Repeater mode.

**Max connected clients** - specify the maximum number of associated wireless clients on the AP radio.

**Min client signal (dBm)** - if enabled, the AP will drop the connection for clients that have signal level below configured threshold.

**Map to data VLAN ID** – specify the VLAN ID for traffic tagging on particular VAP interface. The Station devices that associate using the particular SSID will be grouped into this VLAN.

**Management over wireless** – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to LigoWave NFT.
Services configuration

Use Services menu is divided into further five sections:

- Date & time
- Remote management
- SNMP
- WNMS

Figure 18 - 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 location time zone and enter NTP server in order to use the NTP service.

Figure 19 – 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:

**Date & time**

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.

**Remote management**

Use this menu to manage access to the LigoWave NFT via SSH and Telnet:

Remote management

Enable SSH – enable or disable SSH access to device.
SSH port – specify the SSH service port. By default SSH port is 22.
Enable telnet – enable or disable telnet access to device.
Telnet port – specify the telnet port. By default SSH port is 23.

**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.

Enable SNMP – specify the SNMP service status.
R/O community – specify the read-only community name for SNMP version 1 and version 2c. The read-only community allows LigoWave NFT unit manager to read values, but denies any attempt to change values.
**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.

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

**System configuration**

System menu allows you to manage main LigoWave NFT settings and perform main system actions (reboot, restore configuration, etc.). The section is divided into further sections:

- Device settings
- System functions
- User accounts
- Advanced settings

---

*Figure 23 - System Menu*
Device settings

**Device settings**

- **Friendly device name**: specify name of the LigoWave NFT that will be used to identify the unit.
- **Contact information**: specify the name of the contact person, such as a network administrator, for the LigoWave NFT.
- **Device location**: describe the location of the device.
- **Longitude**: specify the longitude coordinates of the device [specific decimal format, e.g. 54.869446].
- **Latitude**: specify the latitude coordinates of the device [specific decimal format, e.g. 23.891058]. Both coordinates helps indicate accurate location of the device.

System functions

**System functions**

- **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 manually configure each device through the web interface.
- **Restore configuration**: click to upload an existing configuration file to the device. After the configuration file is uploaded, the new configuration will be effective after the **Save changes** button is pressed.
- **Reboot device**: reboot device with the last saved configuration.
- **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 LigoWave NFT devices have **physical reset button**, located close to device’s Ethernet port. This button is able to perform following functions:
- **Reboot device** - press and hold this button for 1s.
- **Reset device to factory defaults** – press and hold the button for 5s and release it. When the reset process will start, device LEDs will start to blink.
User accounts

For security reasons it is recommended to change the default administrator username and password as soon as possible.

Default administrator logon settings are:
Username: admin
Password: admin01

Click Edit button next to user for changing credentials:

**ACCOUNT SETTINGS**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>admin</td>
</tr>
<tr>
<td>Old password</td>
<td>*********</td>
</tr>
<tr>
<td>New password</td>
<td>*********</td>
</tr>
<tr>
<td>Verify password</td>
<td>*********</td>
</tr>
</tbody>
</table>

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.

Advanced settings

**Device discovery** – select to enable LigoWave NFT discovery function. Enable this feature to allow the LigoWave NFT unit discovery within reach of a single multicast packet

**Public status page** – enable or disable the permission for not logged users to view the Status page.
Firmware upgrade

The current version of the device firmware is shown on the upper left corner of the Web interface.

![Firmware Version](image)

Figure 29 – Firmware Version

The device system firmware upgrade is compatible with all 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.

Click the (Update) link near the running firmware name and select the proper firmware image in the Firmware Update pop-up window, then click Upload button:

![Firmware Upload](image)

Figure 30 – Firmware Upload

The new firmware image is uploaded to the controller’s temporary memory. It is necessary to save the firmware into the device permanent memory. Click the Upgrade button:

![Firmware Upgrade](image)

Figure 31 – Firmware Upgrade

**Current version** – displays version of the current firmware.

**Uploaded version** – displays version of the uploaded firmware.

**Upgrade** – 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 could be damaged.
Tools

Site survey

The Site Survey tool shows overview information for wireless networks in a local geographic area on each LigoWave NFT device radio interface. Using this test, an administrator can scan for working wireless devices, check their operating channels, encryption and see signal/noise levels.

To perform the Site Survey test currently, click the **Start scan**:

**SITE SURVEY**

![Figure 32 – Site Survey Results](image)
Support

Troubleshooting

The troubleshooting file contains valuable information about device configuration, routes, log files, command outputs, etc. When using the troubleshooting file, the device quickly gathers troubleshooting information automatically, rather than requiring you to gather each piece of information manually. This is helpful for submitting problems to the support team.

TROUBLESHOOTING

Troubleshooting file:

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

System log

The system log viewer utility provides debug information about the system services and protocols. If the device's malfunction occurs recorded messages can help operators to locate misconfiguration and system errors.

SYSTEM LOG

Click the refresh icon, on the upper right corner, to view current system messages.

Figure 33 – Troubleshooting File Download

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

Figure 34 – Device System Log

Click the refresh icon, on the upper right corner, to view current system messages.
Index

8
802.11a, 17
802.11a/n, 17
802.11n, 17

A
abbreviations, 5
ACK, 5
ACL, 5, 21
AES, 5
aggregation, 18
AMSDU, 5, 18
ATPC, 5, 18
autochannel, 18

B
black list, 21

C
client isolation, 22
configuration backup, 26
configuration file, 26
CPU load, 10

D
default login, 27
device discovery, 27
DFS, 18
DHCP, 5
dynamic stateful, 17
dynamic stateless, 17

E
EAP, 5
ethernet, 10, 22

F
firmware upgrade, 28

G
GMT, 5, 23
graphs, 12

I
IEEE, 5, 17
IP, 5
IP method, 16
IPv4 settings
dynamic IP, 15
static IP, 15
IPv6, 16
IPv6 settings
dynamic IP, 16
static IP, 16
ISP, 5

L
LAN, 5
latitude, 26
LED, 5
longitude, 26

M
MAC, 5
MCS, 5
MSCHAPv2, 6

N
NTP, 6, 23

P
PC, 6
PEAP, 6
physical reset, 26
PSK, 6

R
RADIUS, 6, 21
reboot device, 26
RSSI, 6
RTS threshold, 18
RX errors, 12

S
scan SSID, 29
site survey, 29
SMTP, 6
SNMP, 6, 24
SSH, 6, 24
SSID, 6, 19
syslog, 30
tagging, 22
TCP, 6
threshold, 22
timezone, 23, 24
TKIP, 6
troubleshooting, 30
TTLS, 6
TX errors, 12

U
UDP, 6
uptime, 10, 14
UTC, 24

V
VAP, 6
VLAN, 6, 15
VLAN tagging, 15

W
WACL, 6, 19
white list, 21
WISPr, 6
WLAN, 6
WNMS, 25
WPA, 6, 20
WPA2, 6, 20