INFINITY

NFT series 7.54

User Guide

Revision 1.1
September 4, 2017

LigoWave

Copyright

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

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.

R&TTE compliance statement

This equipment complies with all the requirements of the Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on Radio Equipment and Telecommunication Terminal Equipment and the Mutual Recognition of their Conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

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

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:

i	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

Abbreviation	Description
ACL	Access Control List
ACK	Acknowledgement
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
ATPC	Automatic Transmit Power Control
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MHz	Megahertz

Abbreviation	Description
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NTP	Network Time Protocol
PC	Personal Computer
PSK	Pre-Shared Key
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication dial In User Service
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security (EAP-TTLS) protocol
TX	Transmission
UAM	Universal Access Method
VAP	Virtual AP
VLAN	Virtual Local Area Network
WACL	Wireless Access Control List
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Device Access

First connection via Ethernet

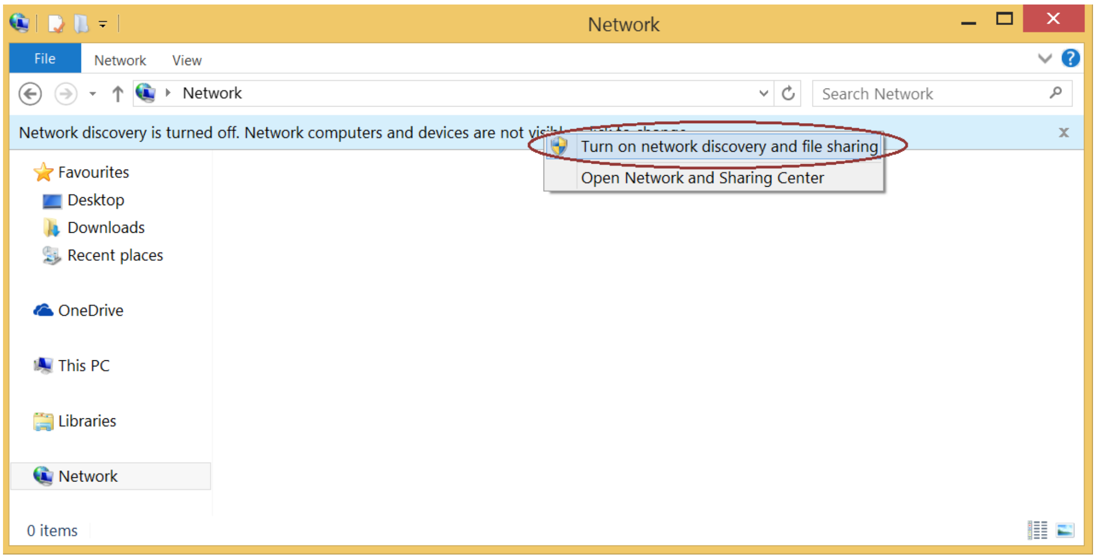
By default LigoWave NFT device obtains the IP address from the DHCP server. Follow the steps to access device on different OS:

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

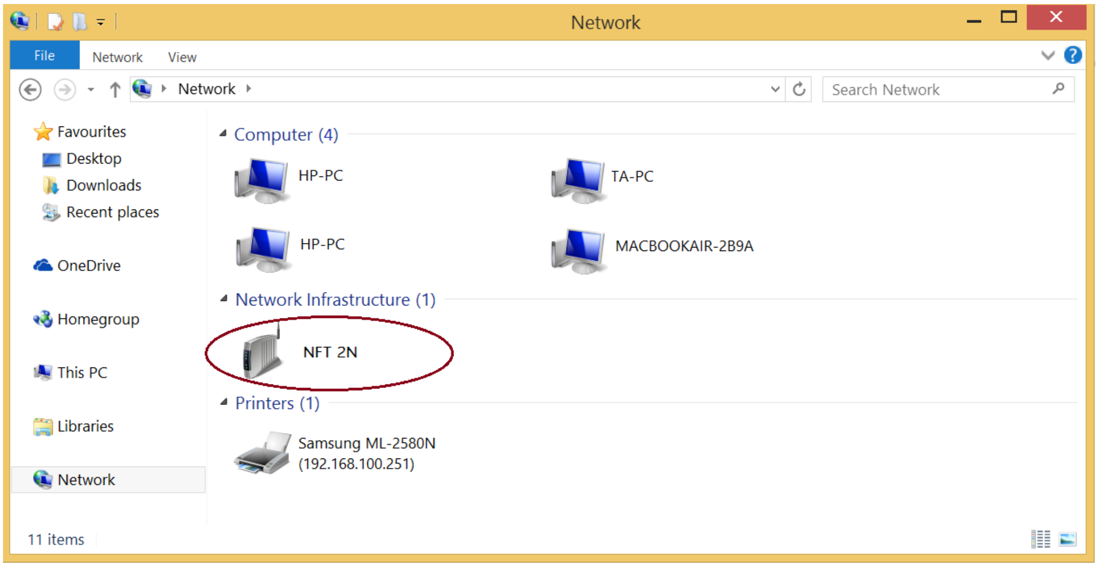
Step 1: Connect your PC directly to the LigoWave NFT device via Ethernet.

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



Network discovery is turned off. Network computers and devices are not visibl

Step 3: Find the required LigoWave NFT device icon:

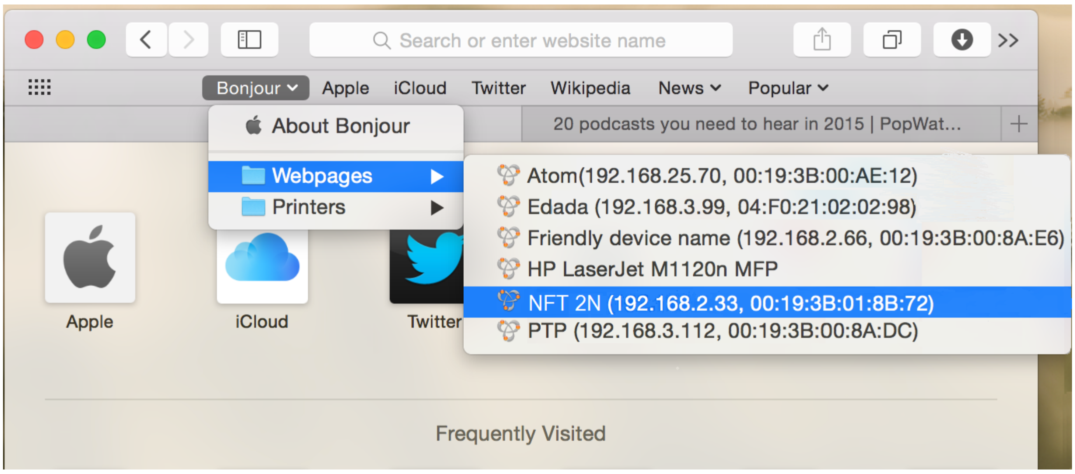


Step 4. Double-click on LigoWave NFT device icon – you will be redirected to the device webpage automatically.

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:

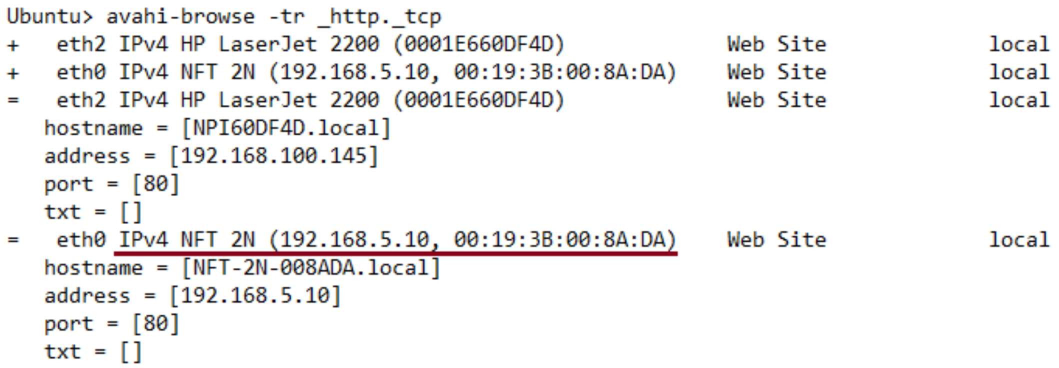

Search or enter website name
Bonjour
Apple
iCloud
Twitter
Wikipedia
News
Popular
About Bonjour
20 podcasts you need to hear in 2015 | PopWat…
Webpages
Printers
Atom(192.168.25.70, 00:19:3B:00:AE:12)
Edada (192.168.3.99, 04:F0:21:02:02:98)
Friendly device name (192.168.2.66, 00:19:3B:00:8A:E6)
HP LaserJet M1120n MFP
NFT 2N (192.168.2.33, 00:19:3B:01:8B:72)
PTP (192.168.3.112, 00:19:3B:00:8A:DC)
Apple
iCloud
Twitter
Frequently Visited

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 (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 ant type discovered IP in the address field to open device web management interface.

First access to web management interface

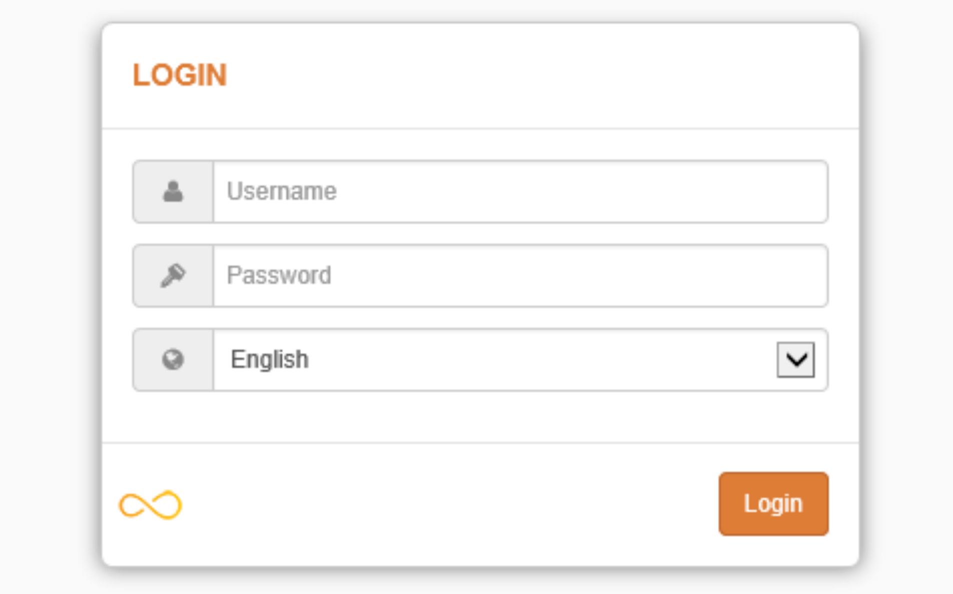
The default administrator login settings are:
Login: **admin**
Password: **admin01**

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

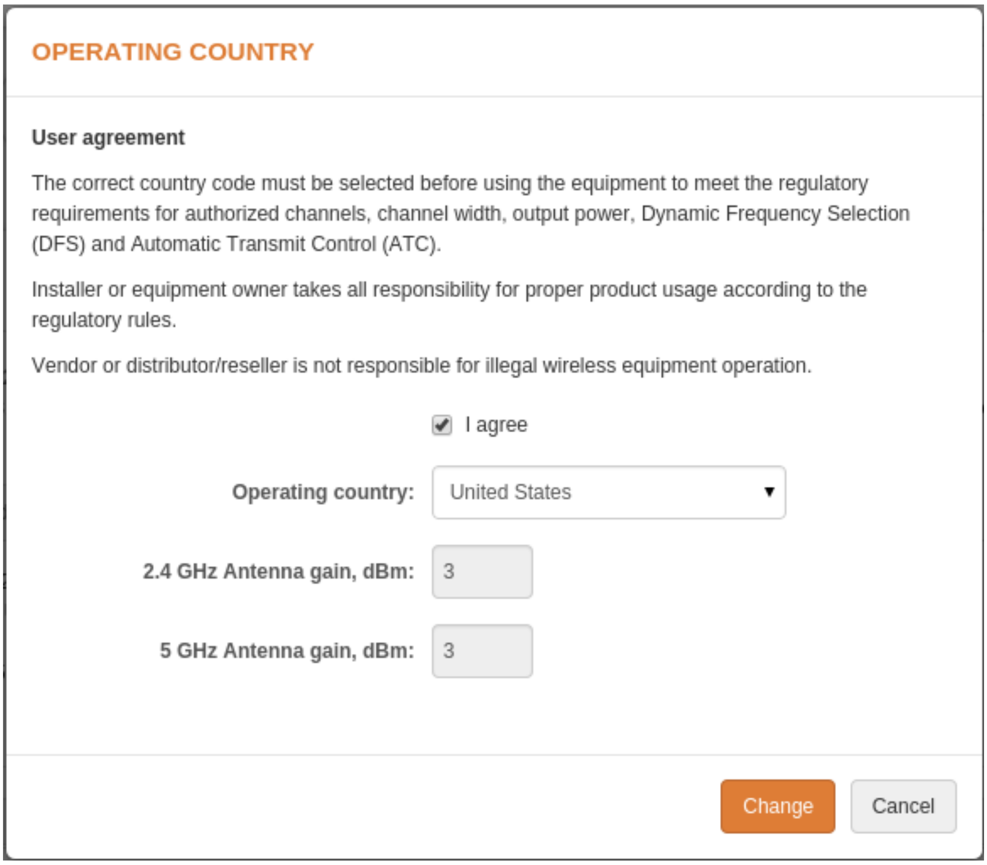
Step 1. Start your Web browser.

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:



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, dBm: 3

5 GHz Antenna gain, dBm: 3

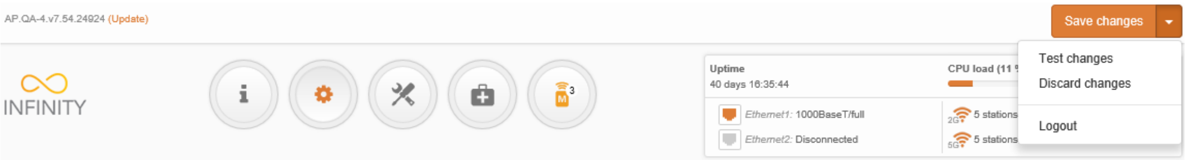
Step 4. After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

LigoWave NFT Configuration

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

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:



AP.QA-4.v7.54.24924 (Update)

Uptime
40 days 16:35:44

CPU load (11 %

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 5 stations
5G 5 stations

Save changes – if pressed new configuration settings are applied instantly and written to the permanent device memory.

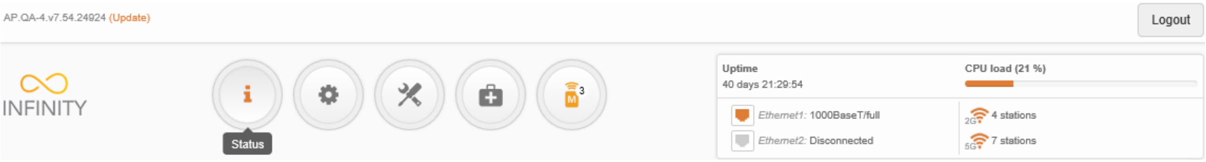
Test changes – if pressed the device will start operating with newly set configuration settings for 3 minutes. During this test time the administrator is able to gauge if device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings administrator 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.



AP.QA-4.v7.54.24924 (Update)

Uptime
40 days 21:29:54

CPU load (21 %)

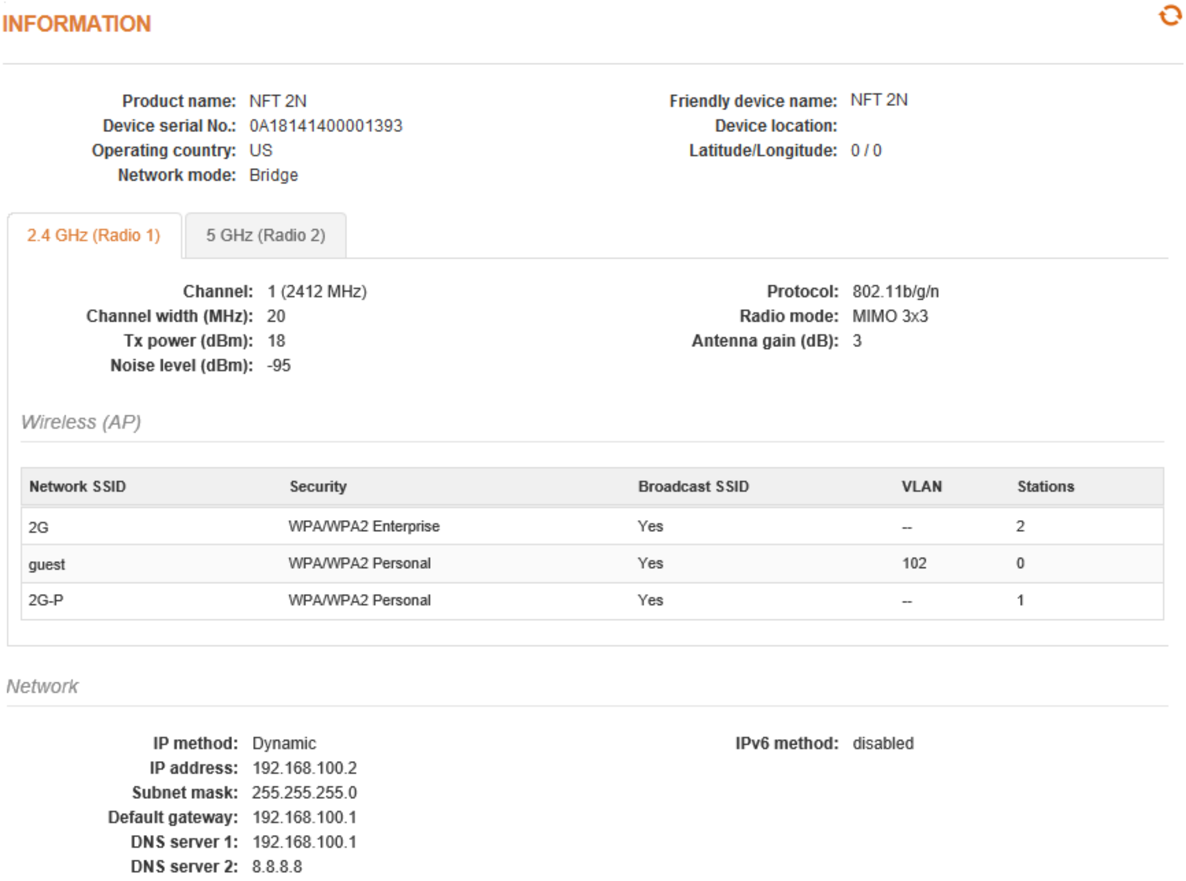
Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 4 stations
5G 7 stations

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.



INFORMATION

Product name:	NFT 2N	Friendly device name:	NFT 2N
Device serial No.:	0A18141400001393	Device location:	
Operating country:	US	Latitude/Longitude:	0 / 0
Network mode:	Bridge		

2.4 GHz (Radio 1) 5 GHz (Radio 2)

Channel:	1 (2412 MHz)	Protocol:	802.11b/g/n
Channel width (MHz):	20	Radio mode:	MIMO 3x3
Tx power (dBm):	18	Antenna gain (dB):	3
Noise level (dBm):	-95		

Wireless (AP)

Network SSID	Security	Broadcast SSID	VLAN	Stations
2G	WPA/WPA2 Enterprise	Yes	--	2
guest	WPA/WPA2 Personal	Yes	102	0
2G-P	WPA/WPA2 Personal	Yes	--	1

Network

IP method:	Dynamic	IPv6 method:	disabled
IP address:	192.168.100.2		
Subnet mask:	255.255.255.0		
Default gateway:	192.168.100.1		
DNS server 1:	192.168.100.1		
DNS server 2:	8.8.8.8		

Figure 2 – Device Information Page

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

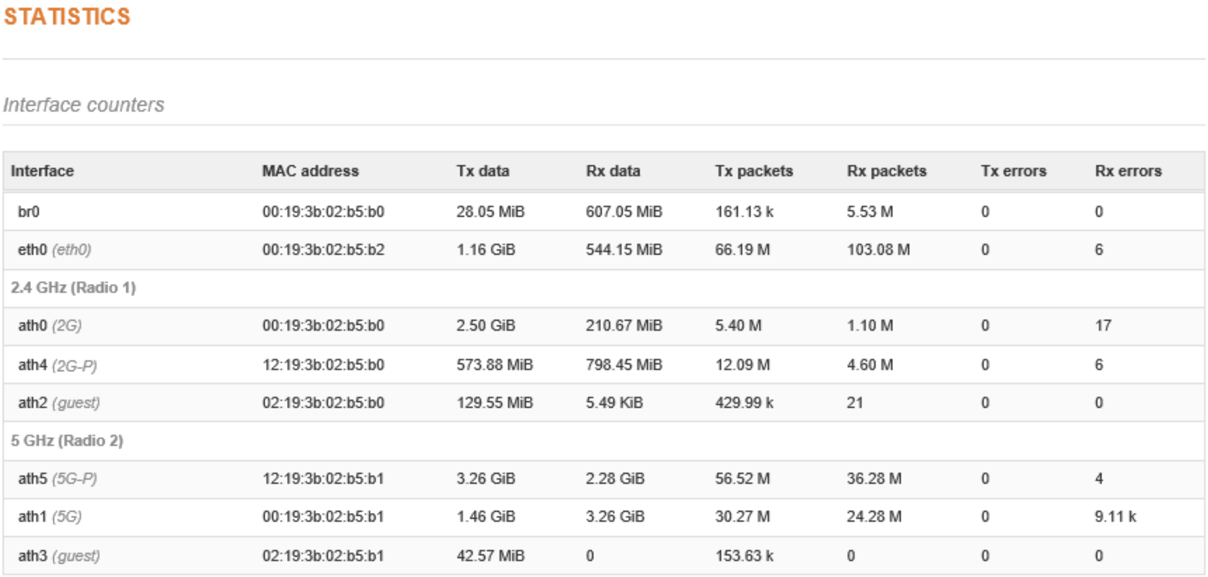
Wireless (AP) – table displays general VAP (Virtual AP) information: SSID, Security type, SSID Broadcast status, VLAN and number and connected clients.

Network– displays a short summary about current network configuration.

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

Statistics

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



STATISTICS

Interface counters

Interface	MAC address	Tx data	Rx data	Tx packets	Rx packets	Tx errors	Rx errors
br0	00:19:3b:02:b5:b0	28.05 MiB	607.05 MiB	161.13 k	5.53 M	0	0
eth0 *(eth0)*	00:19:3b:02:b5:b2	1.16 GiB	544.15 MiB	66.19 M	103.08 M	0	6
2.4 GHz (Radio 1)							
ath0 *(2G)*	00:19:3b:02:b5:b0	2.50 GiB	210.67 MiB	5.40 M	1.10 M	0	17
ath4 *(2G-P)*	12:19:3b:02:b5:b0	573.88 MiB	798.45 MiB	12.09 M	4.60 M	0	6
ath2 *(guest)*	02:19:3b:02:b5:b0	129.55 MiB	5.49 KiB	429.99 k	21	0	0
5 GHz (Radio 2)							
ath5 *(5G-P)*	12:19:3b:02:b5:b1	3.26 GiB	2.28 GiB	56.52 M	36.28 M	0	4
ath1 *(5G)*	00:19:3b:02:b5:b1	1.46 GiB	3.26 GiB	30.27 M	24.28 M	0	9.11 k
ath3 *(guest)*	02:19:3b:02:b5:b1	42.57 MiB	0	153.63 k	0	0	0

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.

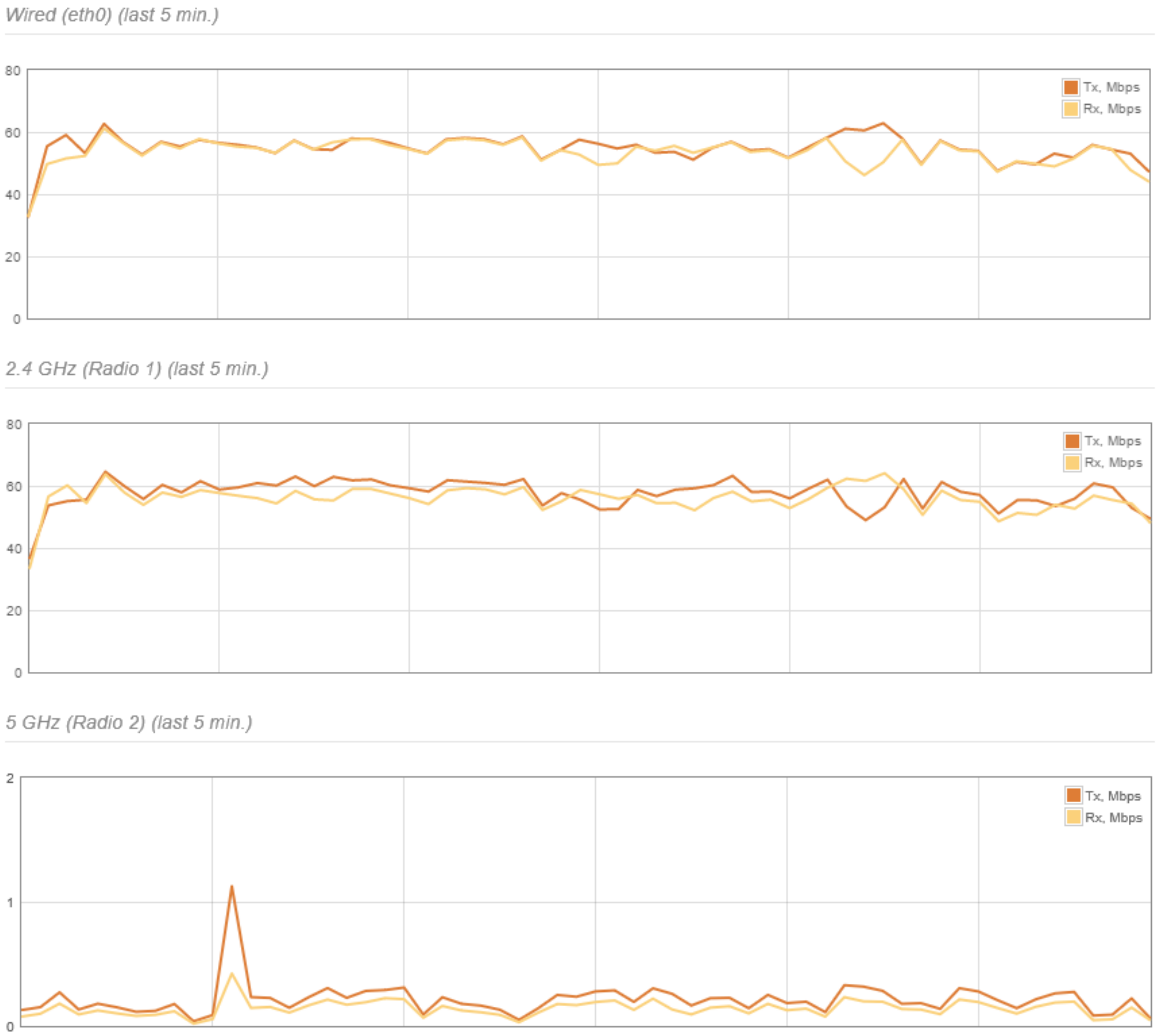
Tx packets – displays the number of transmitted packets.

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.



Wired (eth0) (last 5 min.)

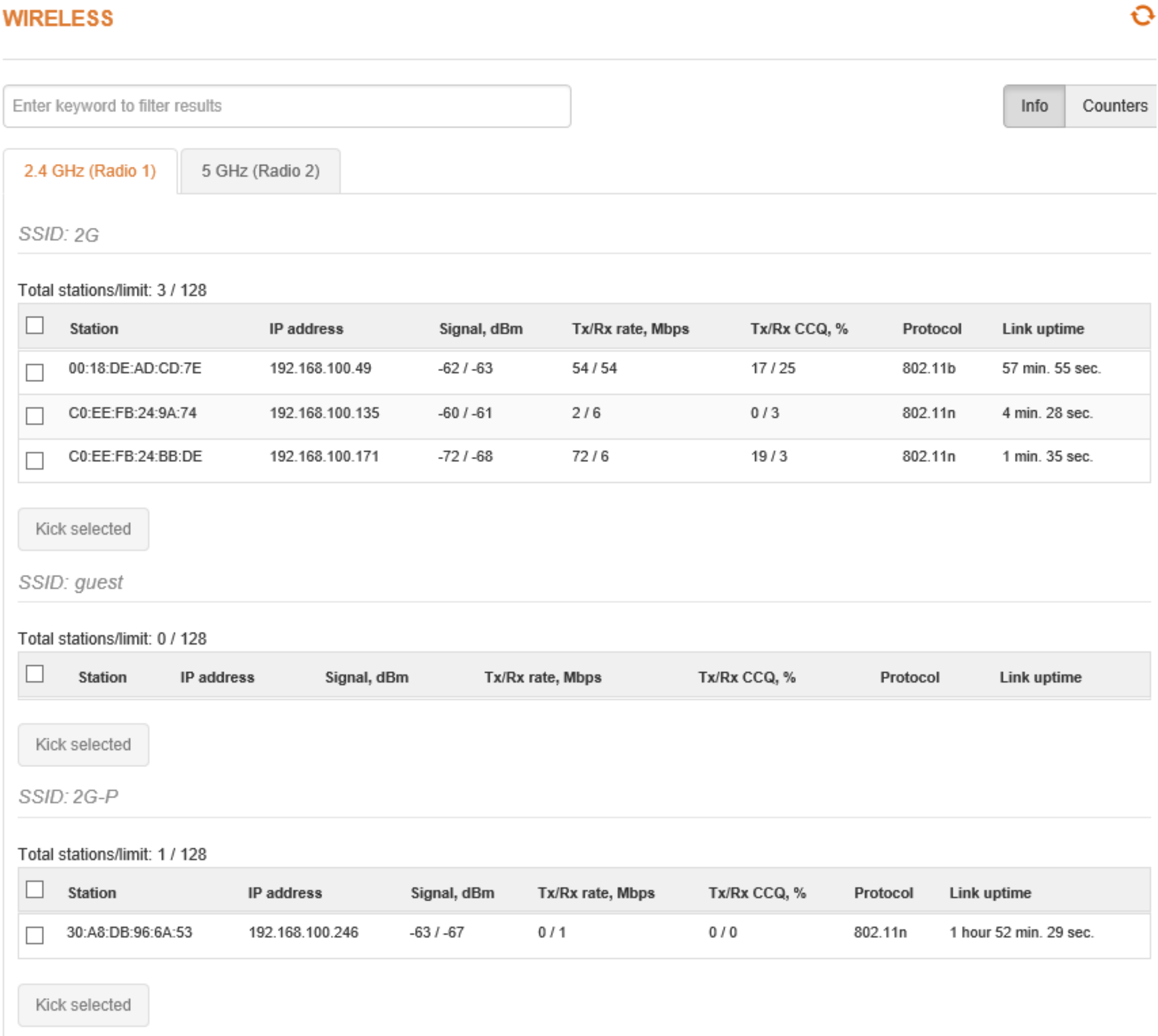
2.4 GHz (Radio 1) (last 5 min.)

5 GHz (Radio 2) (last 5 min.)

Figure 4 – Network Statistics: Graphs

Wireless

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):



WIRELESS

Enter keyword to filter results

SSID: 2G

Total stations/limit: 3 / 128

☐	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
☐	00:18:DE:AD:CD:7E	192.168.100.49	-62 / -63	54 / 54	17 / 25	802.11b	57 min. 55 sec.
☐	C0:EE:FB:24:9A:74	192.168.100.135	-60 / -61	2 / 6	0 / 3	802.11n	4 min. 28 sec.
☐	C0:EE:FB:24:BB:DE	192.168.100.171	-72 / -68	72 / 6	19 / 3	802.11n	1 min. 35 sec.

SSID: guest

Total stations/limit: 0 / 128

☐	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime

SSID: 2G-P

Total stations/limit: 1 / 128

☐	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
☐	30:A8:DB:96:6A:53	192.168.100.246	-63 / -67	0 / 1	0 / 0	802.11n	1 hour 52 min. 29 sec.

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.

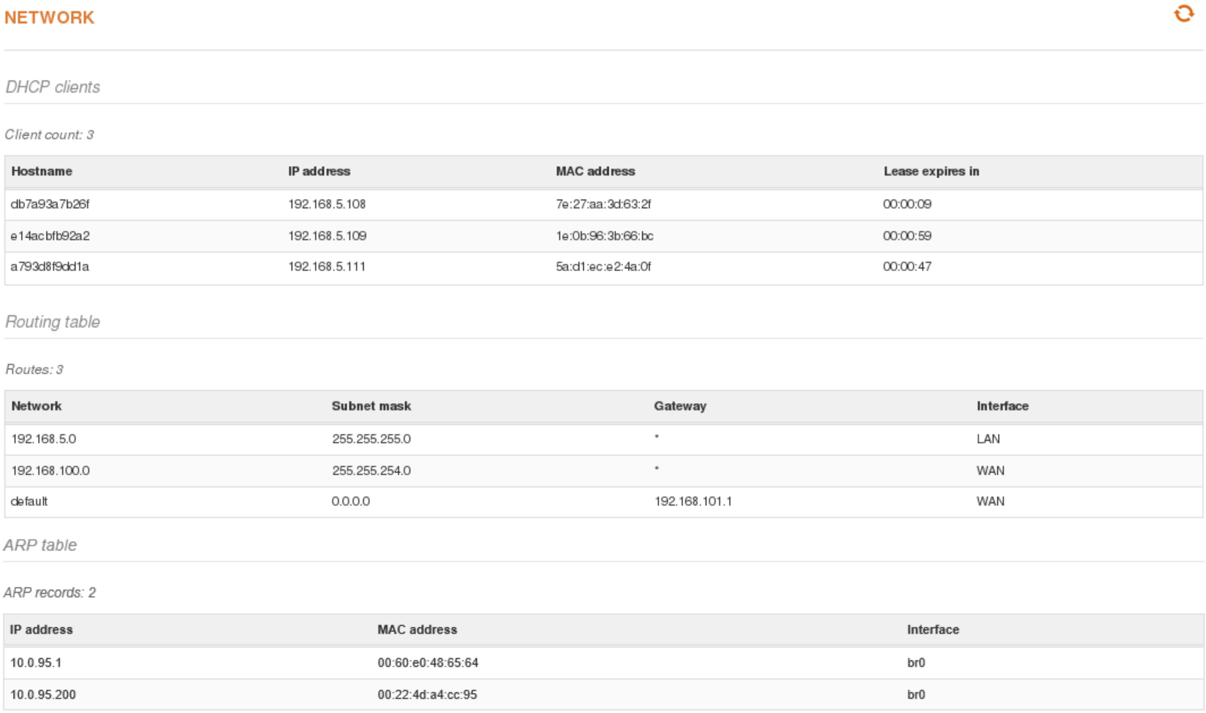
Link uptime – displays the duration of the particular session.

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

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

Network

The **Network** page displays networking information: routing table, ARP table (Address Resolution Protocol) table currently recorded on the device and DHCP lease table:



NETWORK

DHCP clients

Client count: 3

Hostname	IP address	MAC address	Lease expires in
db7a93a7b26f	192.168.5.108	7e:27:aa:3d:63:2f	00:00:09
e14acbfb92a2	192.168.5.109	1e:0b:96:3b:66:bc	00:00:59
a793d8f9dd1a	192.168.5.111	5a:d1:ec:e2:4a:0f	00:00:47

Routing table

Routes: 3

Network	Subnet mask	Gateway	Interface
192.168.5.0	255.255.255.0	*	LAN
192.168.100.0	255.255.254.0	*	WAN
default	0.0.0.0	192.168.101.1	WAN

ARP table

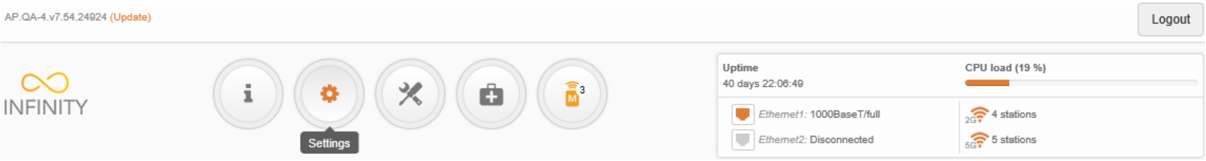
ARP records: 2

IP address	MAC address	Interface
10.0.95.1	00:60:e0:48:65:64	br0
10.0.95.200	00:22:4d:a4:cc:95	br0

Figure 6 – Networking Tables

DHCP client table is displayed only if unit operates in Router mode with DHCP server enabled.

Settings



AP.QA-4.v7.54.24924 (Update)

Uptime
40 days 22:06:49

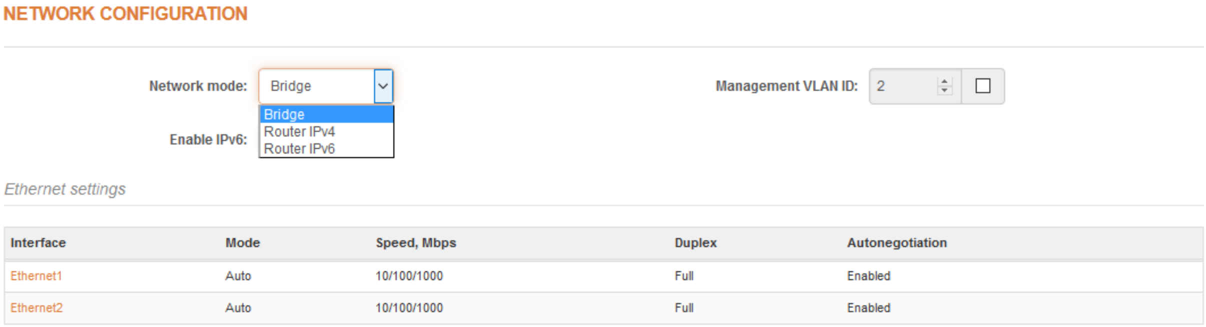
CPU load (19 %)

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 4 stations
5G 5 stations

Network configuration

The **Settings | Network Configuration** page allows you to control the network configuration of the device. First, the device operation mode must be defined to work as a bridge or router (IPv4 or IPv6). The content of the window varies depending on your selection:



NETWORK CONFIGURATION

Network mode: Bridge

Management VLAN ID: 2 □

Enable IPv6:

Ethernet settings

Interface	Mode	Speed, Mbps	Duplex	Autonegotiation
Ethernet1	Auto	10/100/1000	Full	Enabled
Ethernet2	Auto	10/100/1000	Full	Enabled

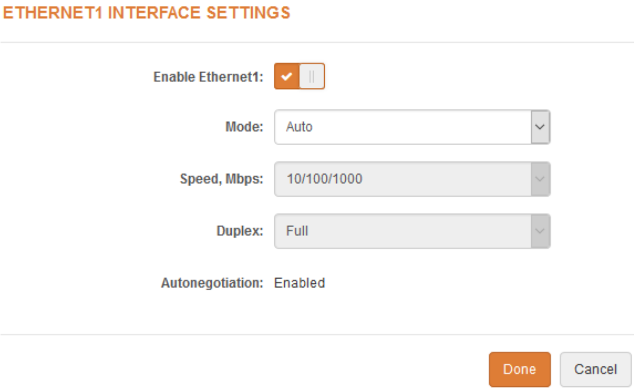
Figure 7 - Network Mode Options

Network mode – choose the device operating mode. Network settings will vary according to the selected Network mode. The Bridge mode allows configuring device IPv4 and IPv6 LAN IP settings, while the Router mode requires more parameters such as LAN network settings, WAN network settings, LAN DHCP settings.

If the **Infinity Controller** functionality is enabled, the Router network mode is not available on the LigoNFT device.

Ethernet settings

This table allows configuring the ETH interface settings (or interfaces in case NFT device have more ETH interfaces). Click on the appropriate Ethernet interface name and setup required parameters:



ETHERNET1 INTERFACE SETTINGS

Enable Ethernet1: ☑

Mode: Auto

Speed, Mbps: 10/100/1000

Duplex: Full

Autonegotiation: Enabled

Figure 8 - Ethernet Interface Configuration

Mode – select the Ethernet port configuration mode:

- **Auto**

- **Fixed**
- **Advanced**

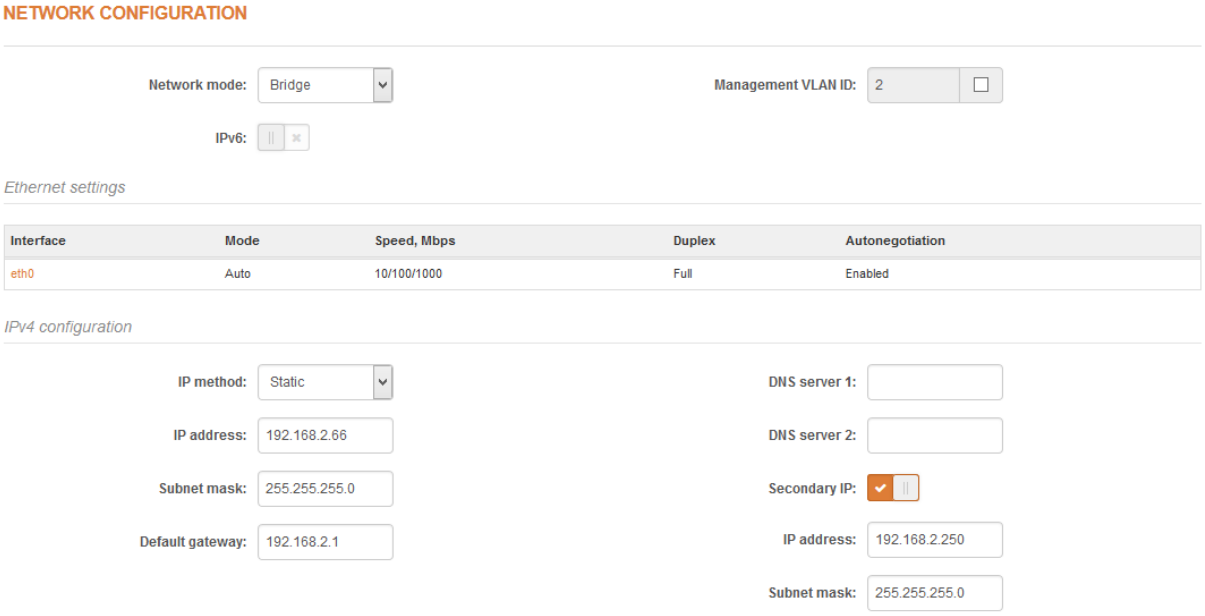
Speed, Mbps – select the Ethernet link speed of the particular Ethernet port.

Duplex – select the duplex mode of the particular Ethernet port.

Autonegotiation – select the auto negotiation which advertise and negotiate Ethernet link duplex configuration (half/full) for the highest possible data rates.

Bridge Configuration

When device is configured to operate in Bridge mode, only device LAN settings should be configured on the **Network configuration** page:



NETWORK CONFIGURATION

Network mode: Bridge

Management VLAN ID: 2 □

IPv6: ✕

Ethernet settings

Interface	Mode	Speed, Mbps	Duplex	Autonegotiation
eth0	Auto	10/100/1000	Full	Enabled

IPv4 configuration

IP method: Static

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

DNS server 1:

DNS server 2:

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

Figure 9 - Bridge Mode Settings

Enable management VLAN – 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.

IPv4 configuration

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.

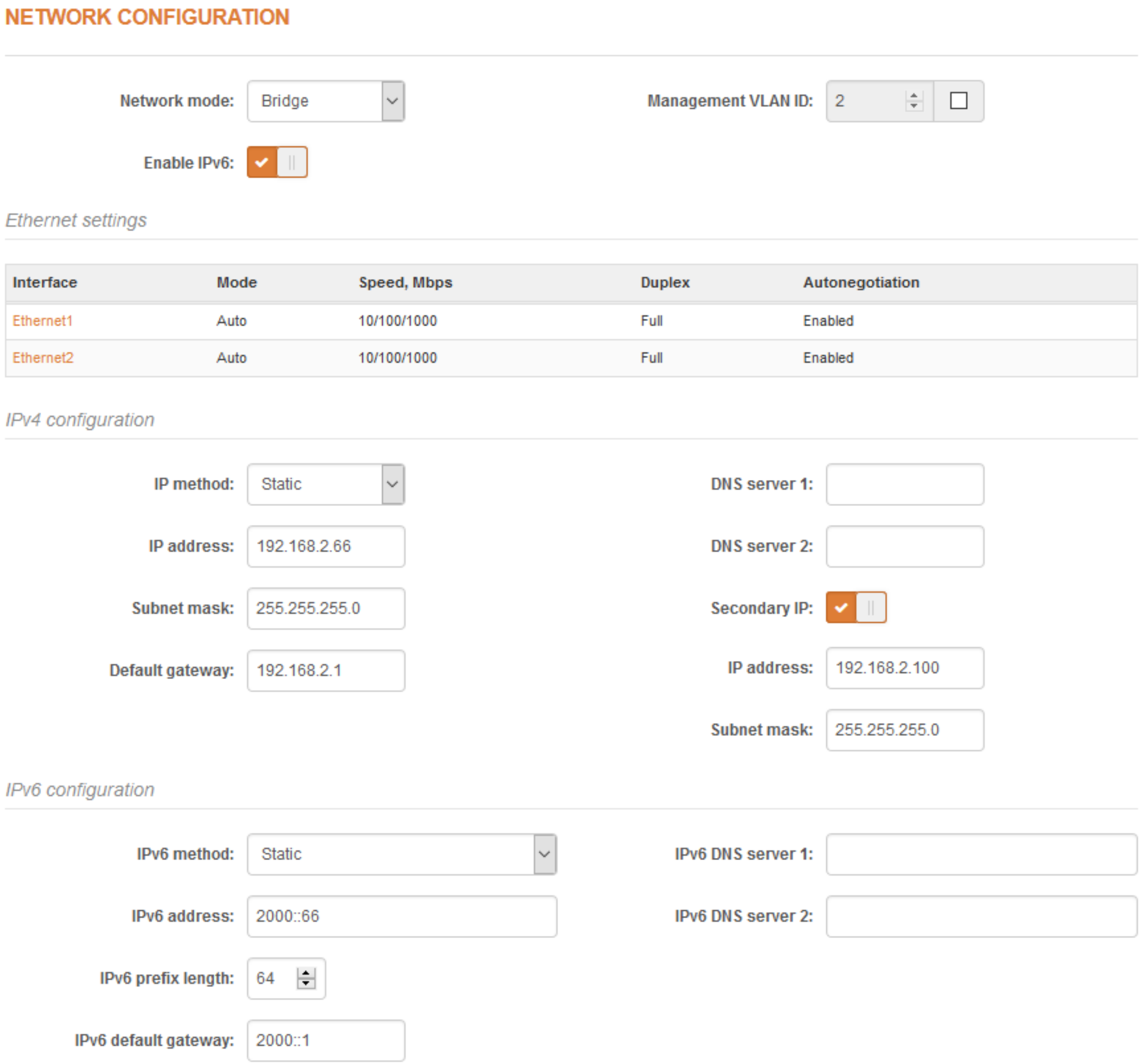
Default gateway – specify a gateway IP address for device.

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

Network mode: Bridge

Management VLAN ID: 2 □

Enable IPv6: ✓

Ethernet settings

Interface	Mode	Speed, Mbps	Duplex	Autonegotiation
Ethernet1	Auto	10/100/1000	Full	Enabled
Ethernet2	Auto	10/100/1000	Full	Enabled

IPv4 configuration

IP method: Static

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

DNS server 1:

DNS server 2:

Secondary IP: ✓

IP address: 192.168.2.100

Subnet mask: 255.255.255.0

IPv6 configuration

IPv6 method: Static

IPv6 address: 2000::66

IPv6 prefix length: 64

IPv6 default gateway: 2000::1

IPv6 DNS server 1:

IPv6 DNS server 2:

Figure 10 –IPv6 Network Settings

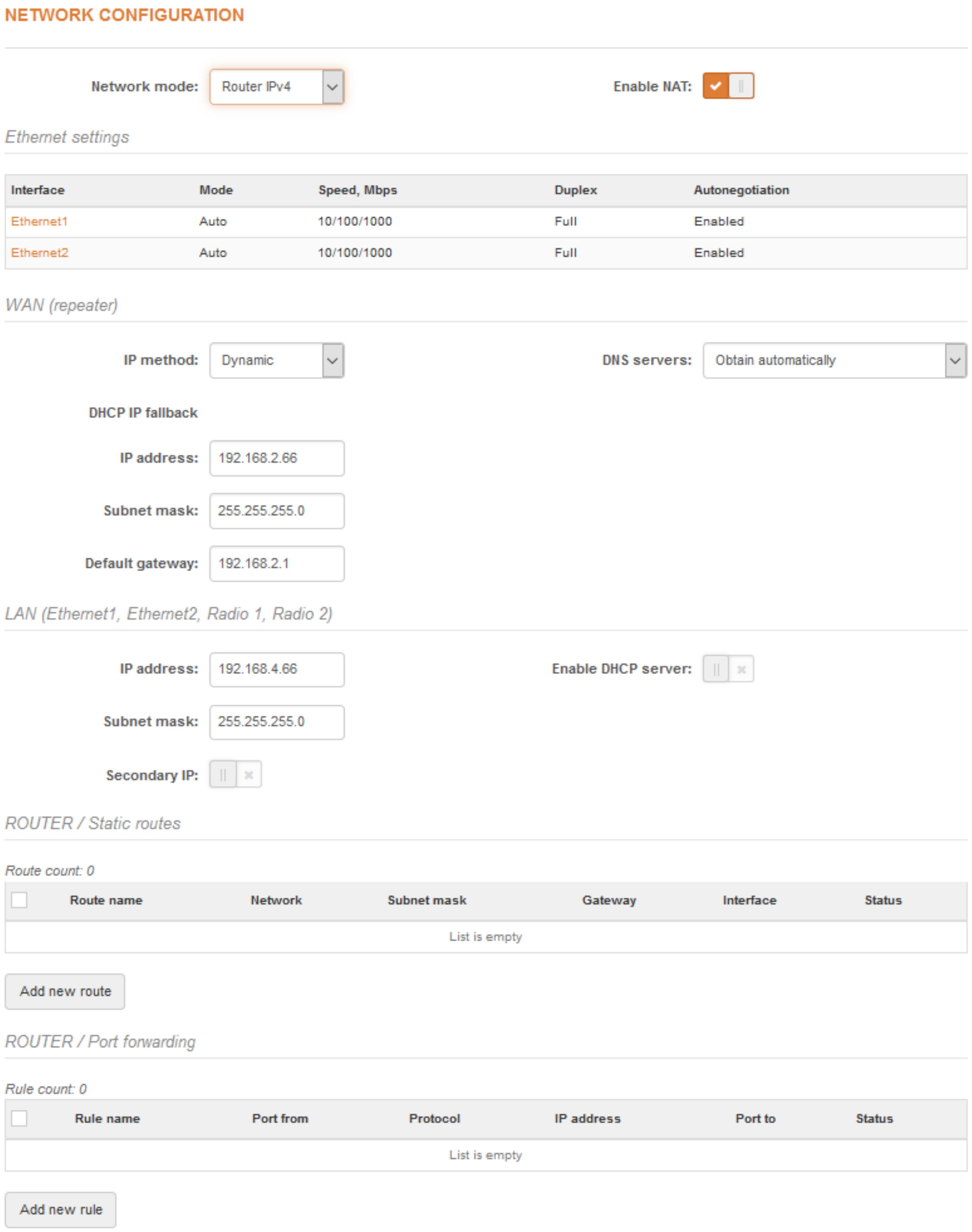
IPv6 method – specify IPv6 reception method: IPv6 addresses can either be retrieved from a DHCPv6 server or configured manually:

- **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.

Router IPv4

This section allows customizing parameters of the Router to suit the needs of network, including ability to use the built-in DHCP server, create Port Forwarding rules and Static routes. When device is configured to operate as Router, the following sections should be specified: WAN network settings, LAN network settings and LAN DHCP settings.



NETWORK CONFIGURATION

Network mode: Router IPv4

Enable NAT: ✓

Ethernet settings

Interface	Mode	Speed, Mbps	Duplex	Autonegotiation
Ethernet1	Auto	10/100/1000	Full	Enabled
Ethernet2	Auto	10/100/1000	Full	Enabled

WAN (repeater)

IP method: Dynamic

DNS servers: Obtain automatically

DHCP IP fallback

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

LAN (Ethernet1, Ethernet2, Radio 1, Radio 2)

IP address: 192.168.4.66

Enable DHCP server: ✗

Subnet mask: 255.255.255.0

Secondary IP: ✗

ROUTER / Static routes

Route count: 0

□	Route name	Network	Subnet mask	Gateway	Interface	Status
			List is empty			

ROUTER / Port forwarding

Rule count: 0

□	Rule name	Port from	Protocol	IP address	Port to	Status
			List is empty			

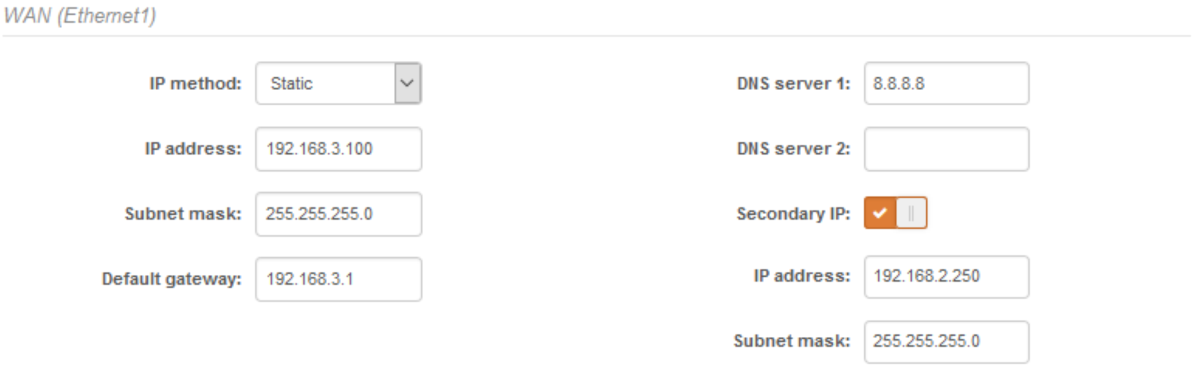
Figure 11 - Router IPv4 Settings

Enable NAT – select to enable NAT (Network Address Translation), that functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network, the multiple PCs on your network would then appear as a single client to the WAN interface.

WAN Settings

WAN network settings include settings related to the WAN interface. The access type of the WAN interface can be configured as: Static IP, Dynamic IP, PPPoE client.

IP method – choose **Static** to specify IP settings for device WAN interface manually:



WAN (Ethernet1)

IP method: Static

IP address: 192.168.3.100

Subnet mask: 255.255.255.0

Default gateway: 192.168.3.1

DNS server 1: 8.8.8.8

DNS server 2:

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

Figure 12 – Router IPv4 WAN Settings: Static IP

IP address – specify static IP address.

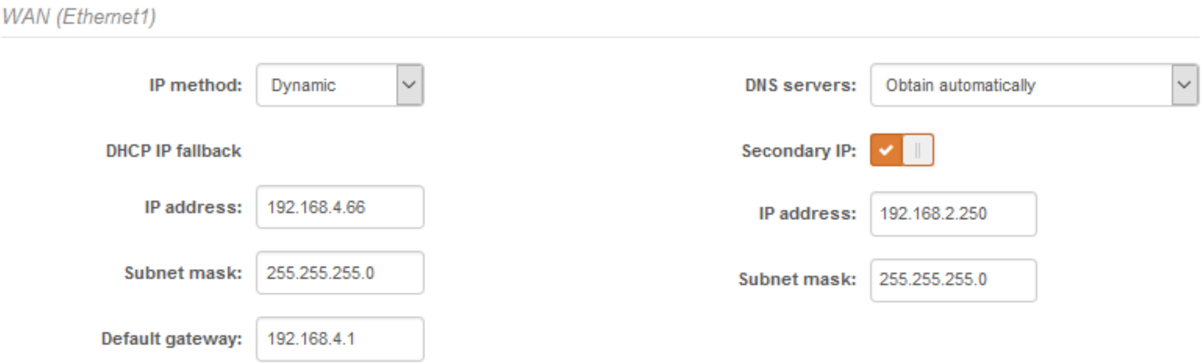
Subnet mask – specify a subnet mask.

Default gateway – specify a gateway.

DNS server – specify primary and/or secondary DNS server

Secondary IP – enable to specify the alternative IP address and the netmask for APC unit management.

WAN mode – choose **Dynamic** to enable DHCP client on the WAN side and get IP address from the running DHCP server:



WAN (Ethernet1)

IP method: Dynamic

DHCP IP fallback

IP address: 192.168.4.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.4.1

DNS servers: Obtain automatically

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

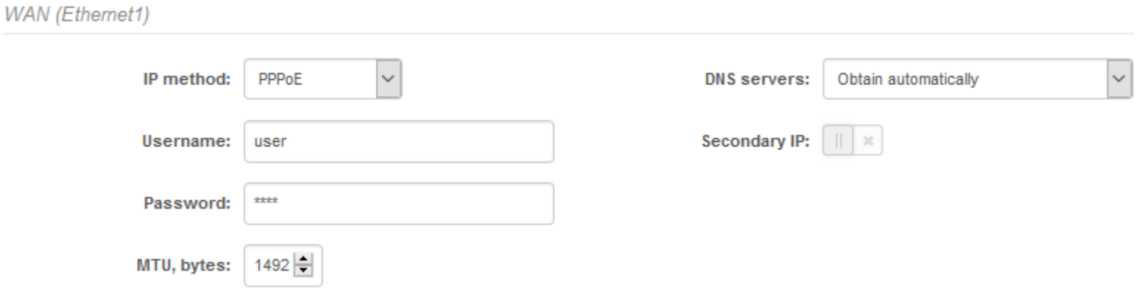
Figure 13 – Routers IPv4 WAN Settings: Dynamic IP

DHCP fallback setting – specify IP address, Subnet mask, Default gateway and optionally DNS server for DHCP fallback. In case the APC unit will not get the IP address from the DHCP, the specified fallback IP settings will be used.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

DNS servers – allows selecting if automatically assigned or alternative DNS servers should be used

WAN mode – choose **PPPoE** to configure WAN interface to connect to an ISP via a PPPoE:



WAN (Ethernet1)

IP method: PPPoE

DNS servers: Obtain automatically

Username: user

Secondary IP: ✗

Password: ****

MTU, bytes: 1492

Figure 14 – Routers IPv4 WAN Settings: PPPoE client

User name – specify the user name for PPPoE.

Password – specify the password for PPPoE.

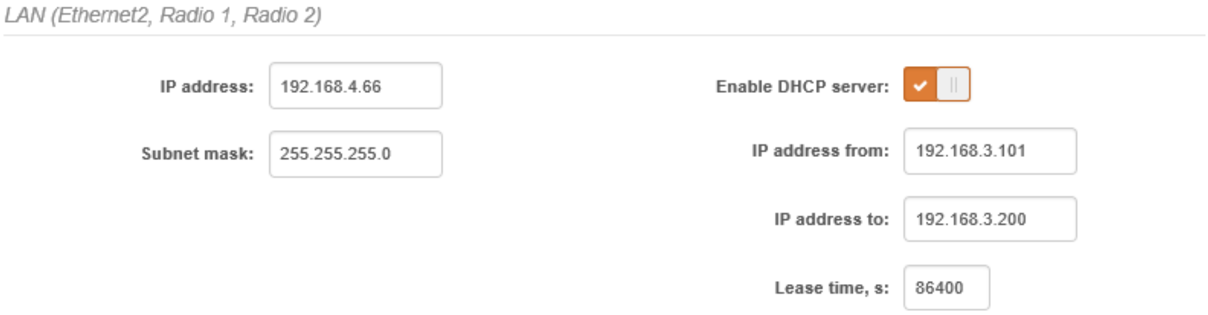
MTU – specify the MTU (Maximum Transmission Unit) in bytes.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

DNS settings – allows selecting if automatically assigned or alternative DNS servers should be used.

LAN Settings

LAN configuration include settings related to the LAN interface.



LAN (Ethernet2, Radio 1, Radio 2)

IP address: 192.168.4.66

Enable DHCP server: ✓

Subnet mask: 255.255.255.0

IP address from: 192.168.3.101

IP address to: 192.168.3.200

Lease time, s: 86400

Figure 15 – Router LAN Settings

IP address – specify the IP address of the device LAN interface.

Subnet mask – specify the subnet mask of the device LAN interface.

Enable DHCP server – select to enable DHCP server on LAN interface.

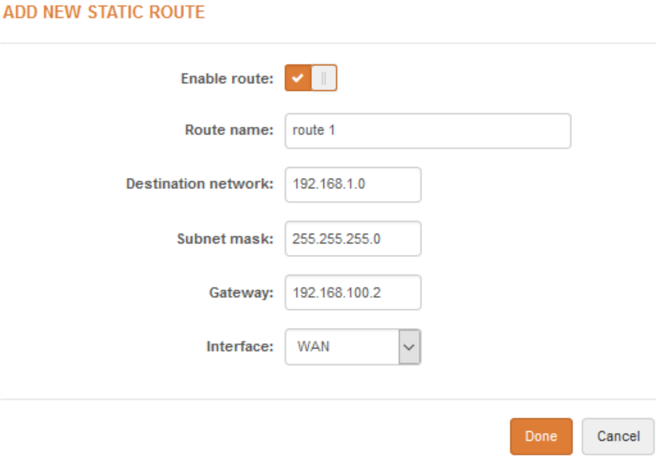
- **IP address from** – specify the starting IP address of the DHCP address pool.
- **IP address to** – specify the ending IP address of DHCP address pool.
- **Lease time** – specify the expiration time in seconds for the IP address assigned by the DHCP server.

Static Routes

Static routes is active only in Router IPv4 network mode.

Use **Settings | Network Configuration** page for configuring Static routes. Routing rule is defined by the destination subnet (Destination IP address and netmask) and gateway where to route the target traffic.

To add a new static route, click on **Add new route** button under the Routing table and specify the following parameters:



ADD NEW STATIC ROUTE

Enable route:	☑
Route name:	route 1
Destination network:	192.168.1.0
Subnet mask:	255.255.255.0
Gateway:	192.168.100.2
Interface:	WAN

Figure 16 - Static Route Configuration

Enable route – slide to enable or disable route. This option allows disable particular route without deleting it.

Route name – specify a name for the particular route.

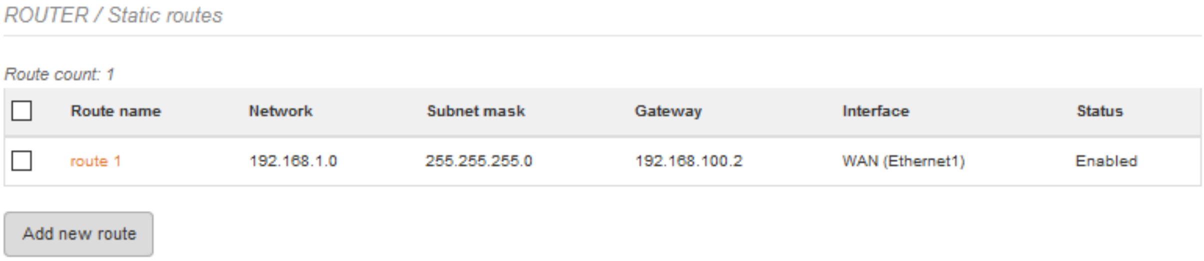
Destination network – specify the destination network IP address.

Subnet mask – specify destination netmask.

Gateway – specify the gateway address for the route.

Interface – select the routing interface from the drop-down.

After saving the route settings, the new route will be added in the routing table on **Settings| Network configuration** page:



ROUTER / Static routes

Route count: 1

□	Route name	Network	Subnet mask	Gateway	Interface	Status
□	route 1	192.168.1.0	255.255.255.0	192.168.100.2	WAN (Ethernet1)	Enabled

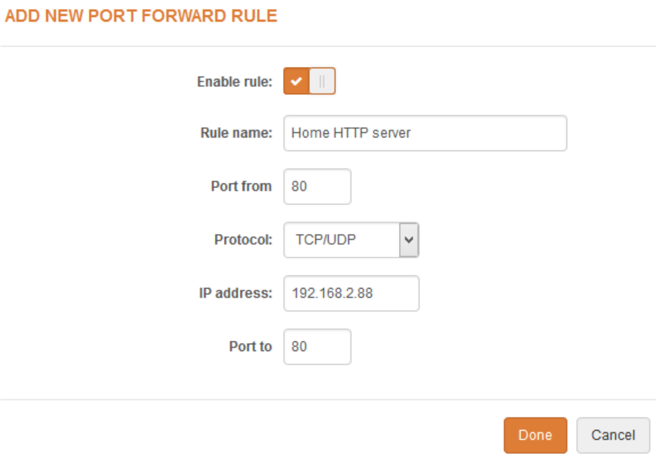
Figure 17 - Static Route Table

Port Forwarding

Port forwarding is available only in Router IPv4 network mode.

Use **Settings | Network Configuration** page for configuring Port forwarding. The **Port forwarding** section gives the ability to pass traffic behind an interface that has NAT enabled. For instance if the unit is in router mode with NAT enabled on the WAN interface, no devices on the outside of the WAN interface can see any private IPs on the LAN side of the unit. By using port forwarding it is possible to pass traffic through to these private IP addresses.

To add a new Port forwarding rule, click on **Add new rule** button under the Port forwarding table and specify the following parameters:



ADD NEW PORT FORWARD RULE

Enable rule:	✓
Rule name:	Home HTTP server
Port from	80
Protocol:	TCP/UDP
IP address:	192.168.2.88
Port to	80

Figure 18 - Port Forward Configuration

Enable rule – slide to enable or disable Port forwarding rule. This option allows disable particular rule without deleting it.

Rule name – specify a name for the particular Port forwarding rule.

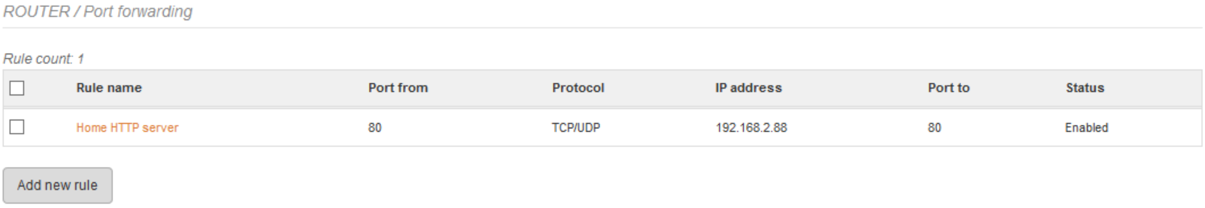
Port from– specify the TCP/UDP port from which the selected traffic should be forwarded.

Protocol – select type of forwarding traffic: TCP, UDP or both.

IP address – specify the IP address that specified traffic will get forwarded to.

Port to – specify TCP/UDP port to which the selected traffic shall be forwarded.

After saving the new Port forwarding rule, it appears in the routing table on **Settings| Network configuration** page:



ROUTER / Port forwarding

Rule count: 1

□	Rule name	Port from	Protocol	IP address	Port to	Status
□	Home HTTP server	80	TCP/UDP	192.168.2.88	80	Enabled

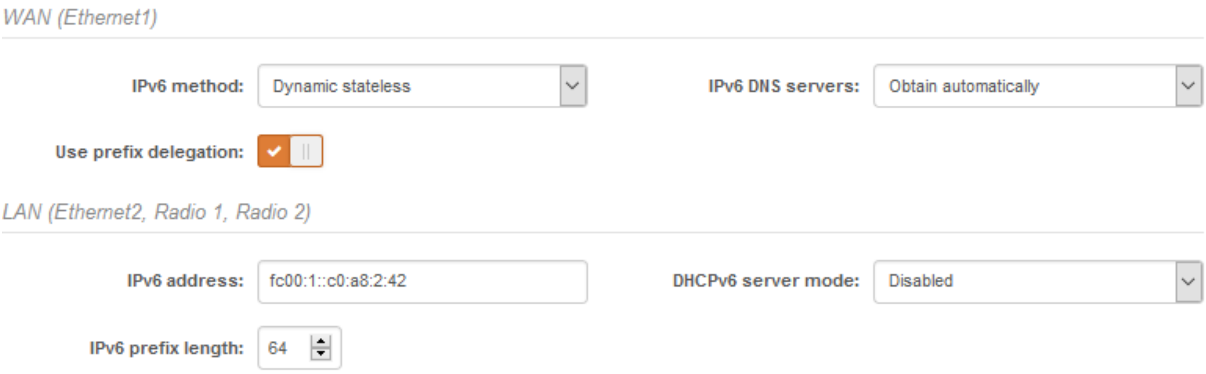
Figure 19 - Port Forward Table

Router IPv6

To setup IPv6 router, select the **Network mode** as Router IPv6 and specify the required WAN and LAN settings.

IPv6 WAN (wired) settings: Dynamic Stateless

With Dynamic stateless IPv6, device generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from a DHCPv6 server. The IP address is a dynamic address.



WAN (Ethernet1)

IPv6 method: Dynamic stateless

IPv6 DNS servers: Obtain automatically

Use prefix delegation: ✓

LAN (Ethernet2, Radio 1, Radio 2)

IPv6 address: fc00:1::c0:a8:2:42

DHCPv6 server mode: Disabled

IPv6 prefix length: 64

Figure 20 – IPv6 Router WAN Settings: Dynamic Stateless IP

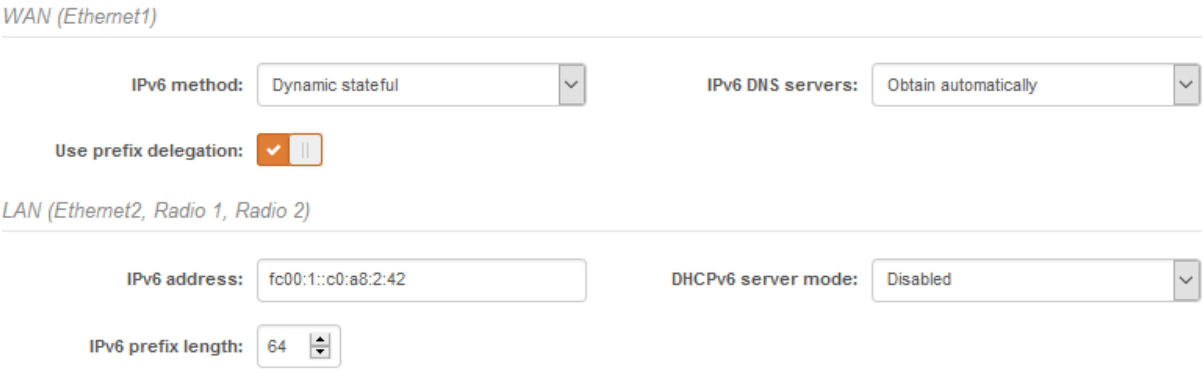
Use prefix delegation – if enabled, a prefix (IP address block) is delegated from Internet service provider to customer's network (LAN).

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically from ISP.
- **Use following** – specify IPv6 DNS servers manually.

IPv6 WAN (wired) settings: Dynamic Stateful

With Dynamic stateful IP, device obtains an interface address, configuration information such as DNS server information, and other parameters from a DHCPv6 server. The IP address is a dynamic address.



WAN (Ethernet1)

IPv6 method: Dynamic stateful

IPv6 DNS servers: Obtain automatically

Use prefix delegation: ✓

LAN (Ethernet2, Radio 1, Radio 2)

IPv6 address: fc00:1::c0:a8:2:42

DHCPv6 server mode: Disabled

IPv6 prefix length: 64

Figure 21 – IPv6 Router WAN Settings: Dynamic Stateful

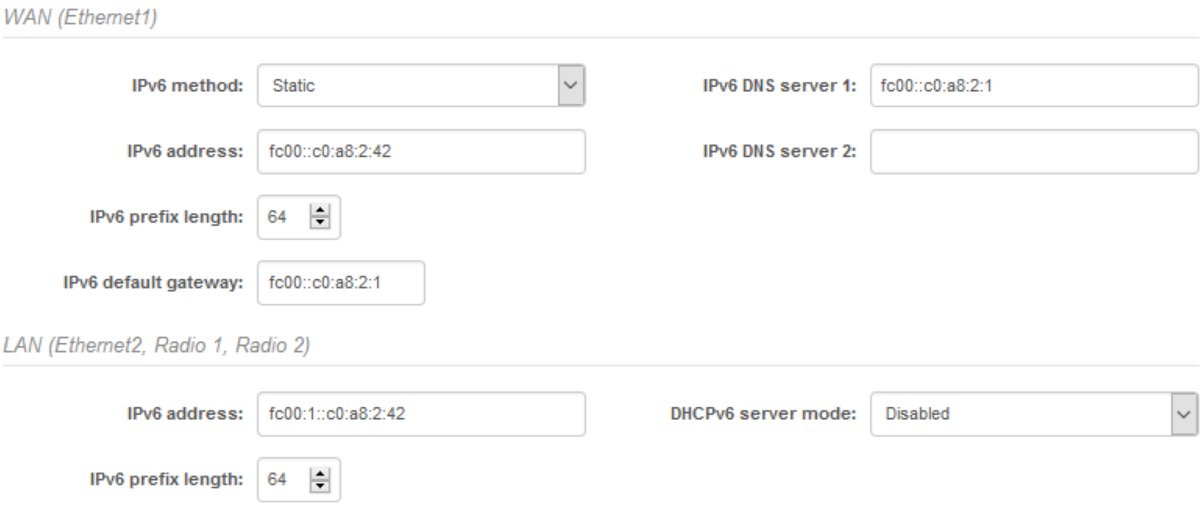
Use prefix delegation – if enabled, a prefix (IP address block) is delegated from Internet service provider to customer's network (LAN).

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically from ISP.
- **Use following** – specify IPv6 DNS servers manually.

IPv6 WAN (wired) settings: Static

With this IPv6 method selected, settings must be specified manually:



WAN (Ethernet1)

IPv6 method: Static

IPv6 DNS server 1: fc00::c0:a8:2:1

IPv6 address: fc00::c0:a8:2:42

IPv6 DNS server 2:

IPv6 prefix length: 64

IPv6 default gateway: fc00::c0:a8:2:1

LAN (Ethernet2, Radio 1, Radio 2)

IPv6 address: fc00:1::c0:a8:2:42

DHCPv6 server mode: Disabled

IPv6 prefix length: 64

Figure 22 – IPv6 Router WAN Settings: Static IPv6

IPv6 address – specify the **IPv6 address** for the interface.

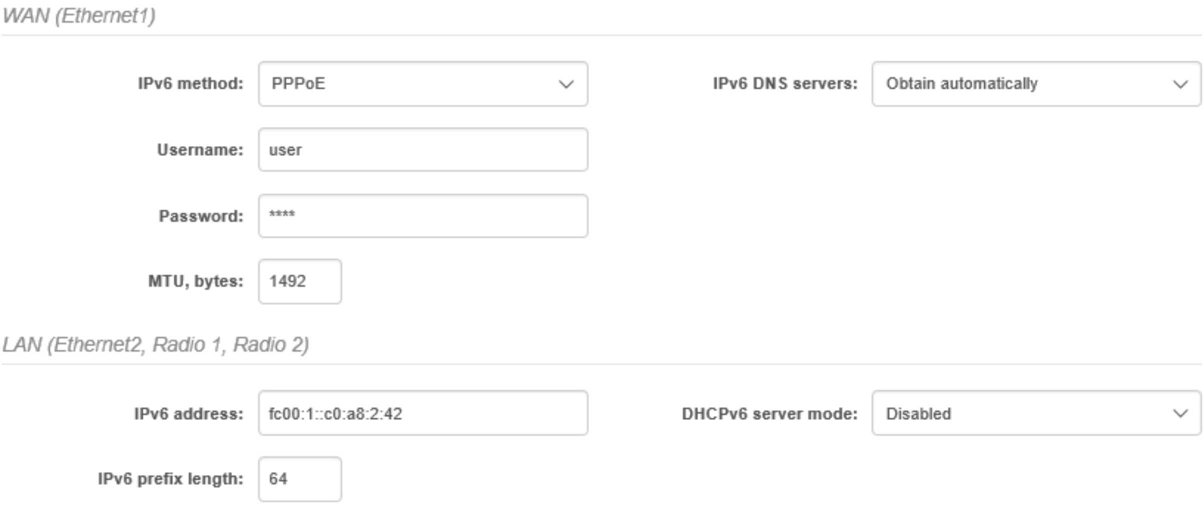
IPv6 prefix length– enter the **prefix length** for the address (default is 64).

IPv6 default gateway – specify IPv6 address for default gateway.

IPv6 DNS server – specify the Domain Naming Server IPv6 addresses.

IPv6 WAN (wired) settings: PPPoE

With this method device will get WAN interface IPv6 address via PPPoE.



WAN (Ethernet1)

IPv6 method: PPPoE

IPv6 DNS servers: Obtain automatically

Username: user

Password: ****

MTU, bytes: 1492

LAN (Ethernet2, Radio 1, Radio 2)

IPv6 address: fc00:1::c0:a8:2:42

DHCPv6 server mode: Disabled

IPv6 prefix length: 64

Figure 23 – IPv6 Router WAN Settings: PPPoE

Username – enter the login information for PPPoE.

Password – enter the password for PPPoE.

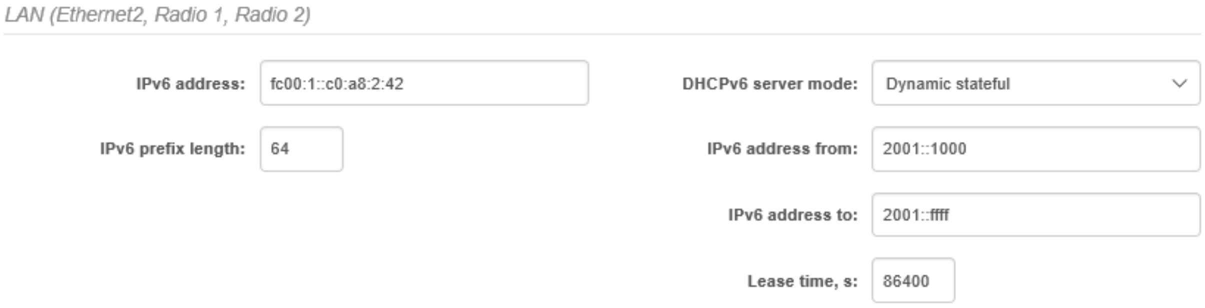
MTU – specify the MTU (Maximum Transmission Unit) in bytes.

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically.
- **Use following** – specify IPv6 DNS servers manually.

LAN (wireless) Settings

LAN configuration includes settings related to the LAN interface.



LAN (Ethernet2, Radio 1, Radio 2)

IPv6 address: fc00:1::c0:a8:2:42

IPv6 prefix length: 64

DHCPv6 server mode: Dynamic stateful

IPv6 address from: 2001::1000

IPv6 address to: 2001::ffff

Lease time, s: 86400

Figure 24 – IPv6 Router LAN Settings

IPv6 address – enter the IPv6 LAN address.

IPv6 prefix length – specify the IPv6 prefix length, or keep the default prefix length (64).

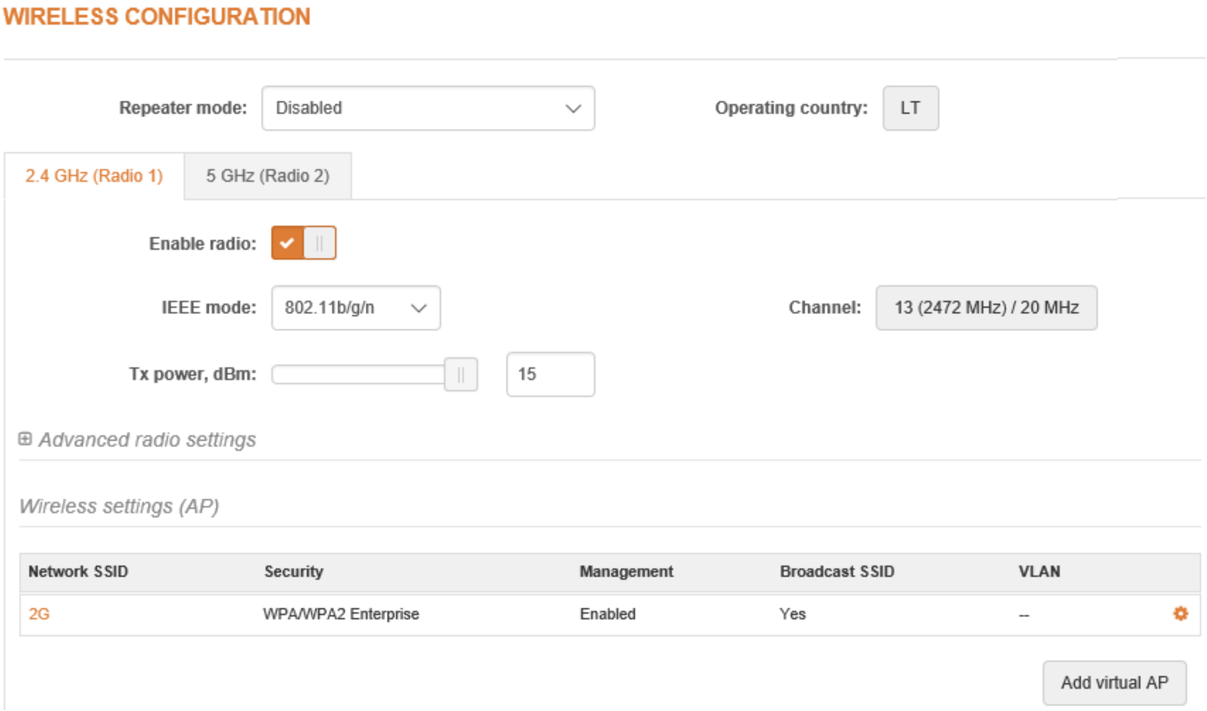
DHCPv6 server mode – select from the drop-down required DHCPv6 mode:

- **Disabled** – select to disable DHCPv6 server. No IPv6 addresses will be assigned for clients.
- **Dynamic stateless IP** – select for automatic IPv6 address configuration.
- **Dynamic stateful IP** – select to configure stateful DHCPv6 server for the LAN by specifying local DHCP IPv6 address pools so the DHCPv6 server can control the allocation of IPv6 addresses in the LAN:
  - **IPv6 address from** - enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool.
    IPv6 address to – enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool.
  - **Lease time** – specify the expiration time in seconds for the IP address assigned by the DHCPv6 server.

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 contains all parameters that required to configure LigoWave NFT device in order have working wireless link. The Wireless page of the dual-band LigoWave NFT device is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate wireless settings:


WIRELESS CONFIGURATION

Repeater mode: Disabled

Operating country: LT

2.4 GHz (Radio 1) | 5 GHz (Radio 2)

Enable radio: ✓

IEEE mode: 802.11b/g/n

Channel: 13 (2472 MHz) / 20 MHz

Tx power, dBm: 15

⊞ Advanced radio settings

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
2G	WPA/WPA2 Enterprise	Enabled	Yes	--

Figure 25 – Wireless Configuration

Repeater mode – allows to extend the range of the existing network infrastructure. With dual-band radio LigoNFT devices it is possible to choose the radio on the repeater mode will be enabled.

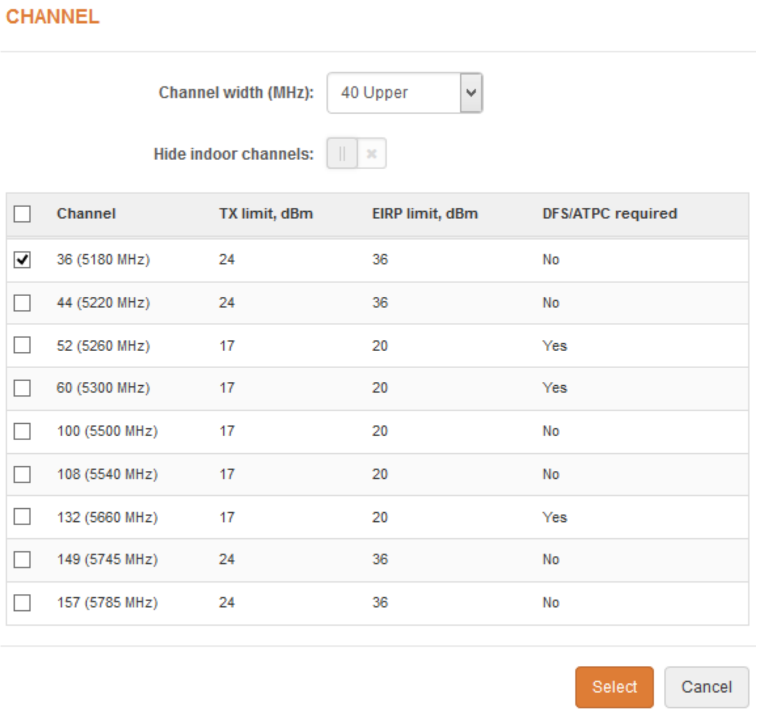
Operating country – displays LigoWave NFT unit operating country. The country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the LigoWave NFT unit's installation, though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

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

IEEE mode – choose the wireless network mode, depending on radio hardware [802.11a, 802.11n, 802.11a/n/ac, 802.11ac].

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

Channel width (MHz): 40 Upper

Hide indoor channels: ☐

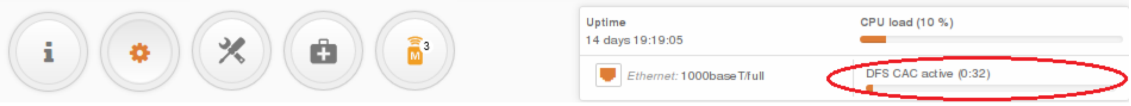
☐	Channel	TX limit, dBm	EIRP limit, dBm	DFS/ATPC required
☑	36 (5180 MHz)	24	36	No
☐	44 (5220 MHz)	24	36	No
☐	52 (5260 MHz)	17	20	Yes
☐	60 (5300 MHz)	17	20	Yes
☐	100 (5500 MHz)	17	20	No
☐	108 (5540 MHz)	17	20	No
☐	132 (5660 MHz)	17	20	Yes
☐	149 (5745 MHz)	24	36	No
☐	157 (5785 MHz)	24	36	No

Figure 26 – Channel List Table

Channel width – select the width of the operating radio channel. The LigoWave NFT supports 20, 40 Lower and 40 Upper and 80 (for 802.11ac products only) channel widths.

Channel table – select the channel(s) at which the NFT device will operate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows device 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.

The DFS CAC (Channel Availability Check) indicator will be visible on the web management page header, in case LigoDLB unit is operating on CAC waiting period:



Uptime
14 days 19:19:05

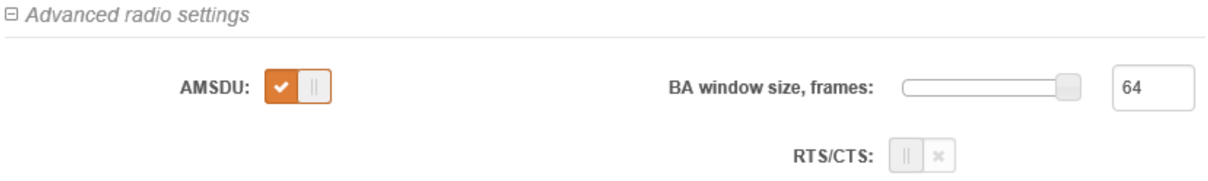
CPU load (10 %)

Ethernet: 1000baseT/full

DFS CAC active (0:32)

Advanced radio settings

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



⊟ *Advanced radio settings*

AMSDU: ✓

BA window size, frames: 64

RTS/CTS: ☐

Figure 27 - Wireless Advanced 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.

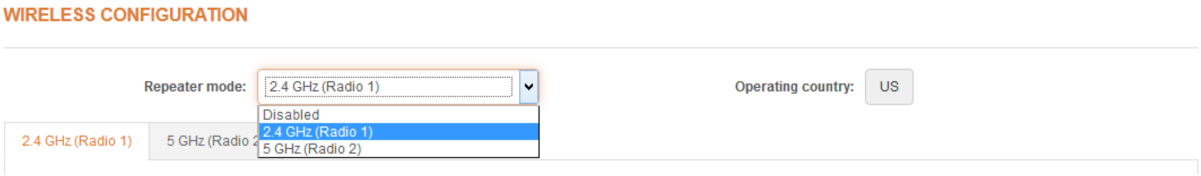
BA window size – specify BA (Block ACK) window size in frames [1-64].

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.

Repeater settings (Station)

Use **Repeater** mode in order to extend the range of the existing network infrastructure. The LigoWave NFT acting as repeater have possibility to scan SSID of the surrounding APs and choose the required one.

Select which LigoWave NFT wireless interface will operate as **Repeater**:



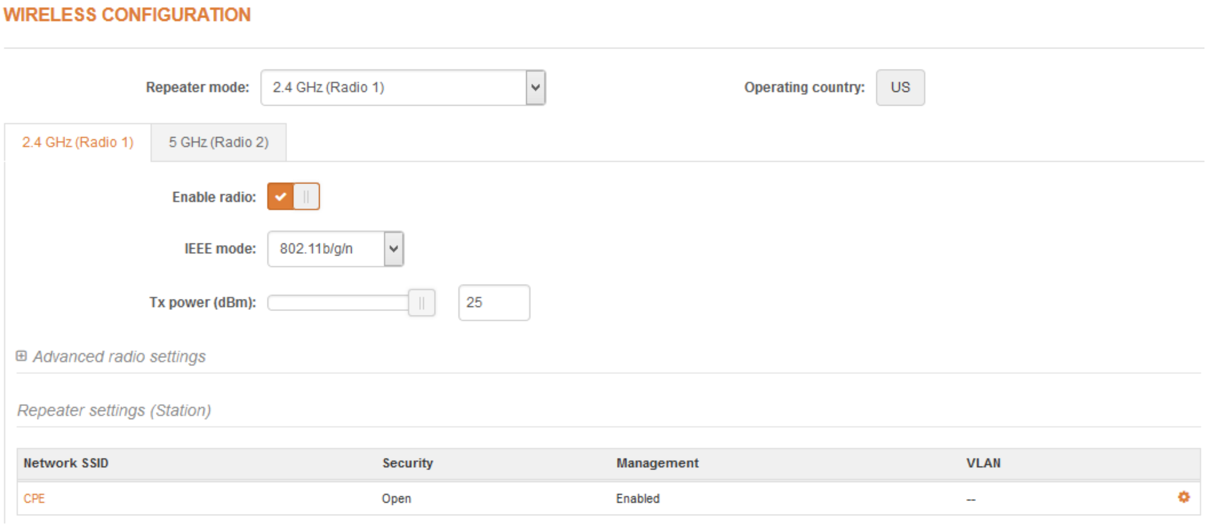
WIRELESS CONFIGURATION

Repeater mode: 2.4 GHz (Radio 1)

Operating country: US

Figure 28 – Repeater Mode

After the wireless interface for Repeater was selected, the appropriate table appears with default repeater settings on the Wireless Configuration page:



WIRELESS CONFIGURATION

Repeater mode: 2.4 GHz (Radio 1)

Operating country: US

Enable radio: ✓

IEEE mode: 802.11b/g/n

Tx power (dBm): 25

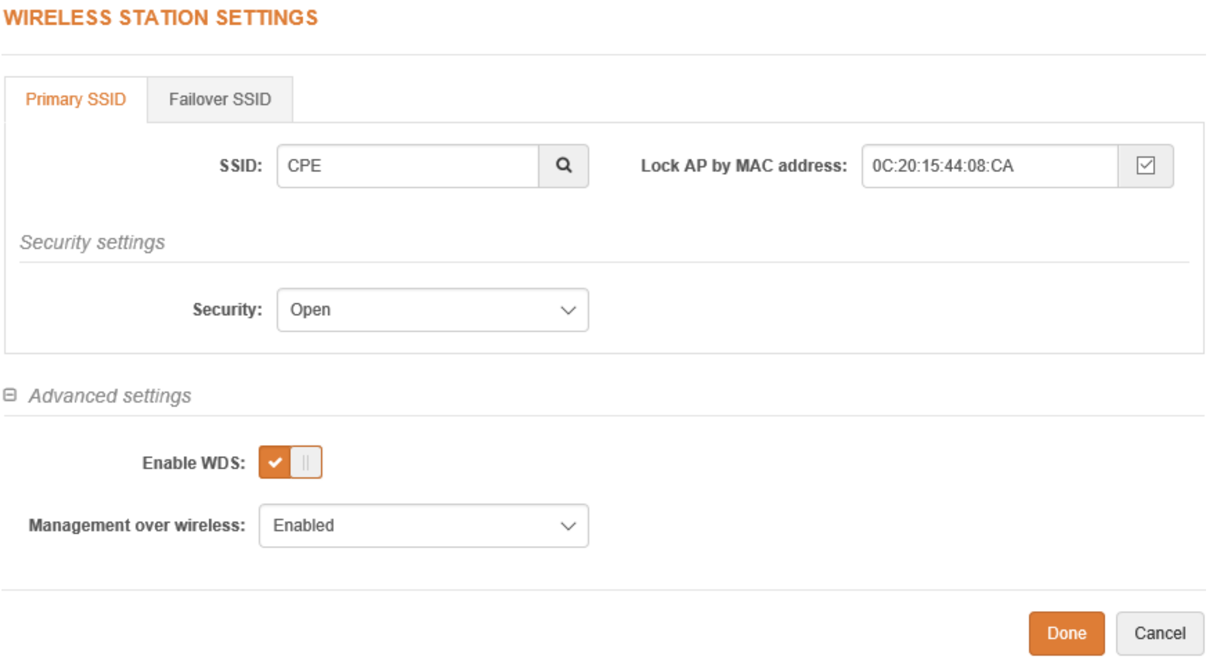
⊞ Advanced radio settings

Repeater settings (Station)

Network SSID	Security	Management	VLAN	
CPE	Open	Enabled	--	⚙

Figure 29 - Repeater Table

Click on the icon ⚙ for Repeater configuration:



WIRELESS STATION SETTINGS

SSID: CPE

Lock AP by MAC address: 0C:20:15:44:08:CA ☑

Security settings

Security: Open

Advanced settings

Enable WDS: ✓

Management over wireless: Enabled

Figure 30 - Repeater: Primary SSID Settings

Primary SSID – specify the SSID of the repeater's peer access point.

Scan – click 🔍 button to scan for surrounding wireless networks. Found network SSID's will be available in drop down menu.

Lock AP by MAC address – enter the MAC address of the particular Peer AP, thus preventing the roaming between access points with the same SSID.

Security – choose and specify the security settings of the peer access point

- **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).

For detailed information about **Security** settings refer at the respective sections *Wireless security*

Enable WDS – use slide to enable WDS (Wireless Distribution System). With WDS enabled the wireless clients can easy pass through the access points with the same SSID.

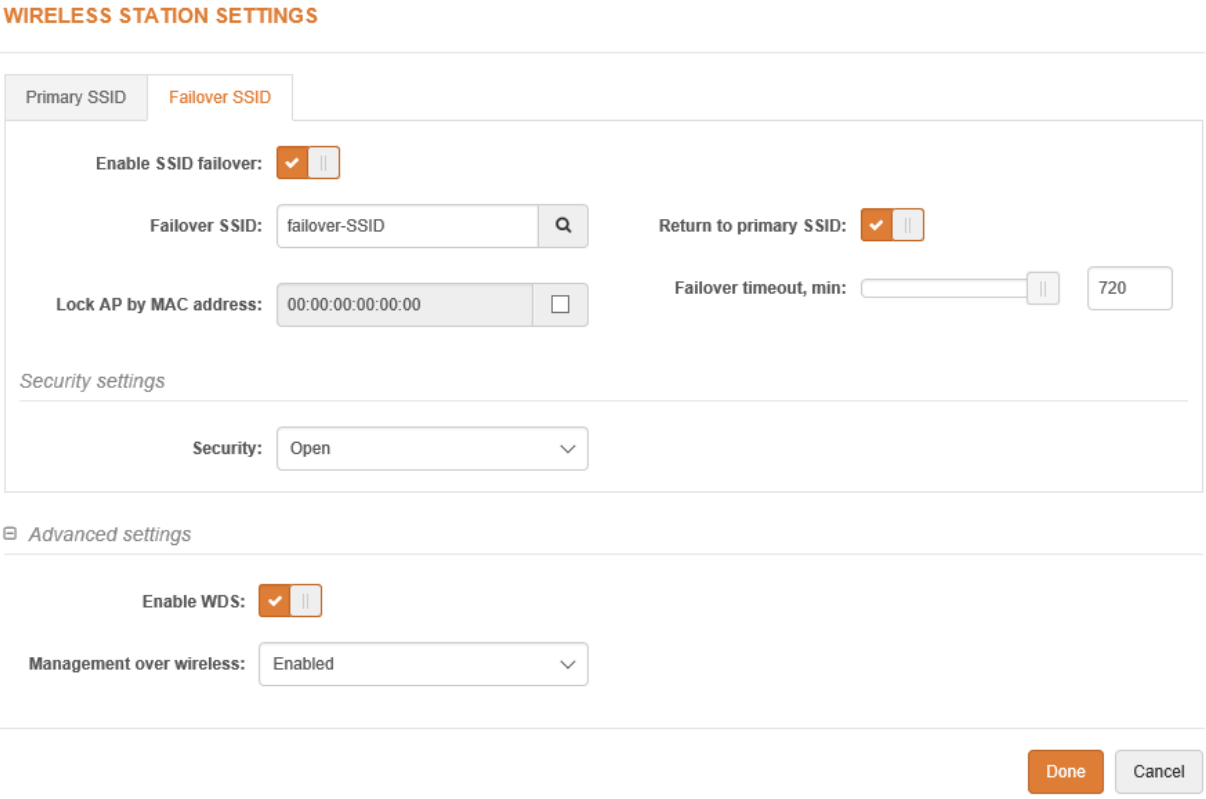
Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead require a physical network connection using an Ethernet cable for administrative access to LigoWave device.

Failover SSID

LigoNFT units have possibility to connect to preconfigured failover SSID, in case the connection to the primary SSID is lost.

In case the LigoNFT device is operating on failover SSID and then loses this connection, the device will try to connect to primary SSID first, and only then will try to attempt to connect to the failover SSID. Reboot will result in the same sequence.

Use the **Failover SSID** tab to enable SSID failover function:



WIRELESS STATION SETTINGS

Primary SSID | Failover SSID

Enable SSID failover: ☑

Failover SSID: failover-SSID

Return to primary SSID: ☑

Failover timeout, min: 720

Lock AP by MAC address: 00:00:00:00:00:00 □

Security settings

Security: Open

⊟ *Advanced settings*

Enable WDS: ☑

Management over wireless: Enabled

Figure 31 - Repeater: Failover SSID Settings

Failover SSID – specify the secondary SSID where the LigoNFT will try to connect.

Return to primary SSID – when enabled the LigoNFT unit tries to connect continuously to the primary SSID in the intervals preset.

Failover timeout – specify the amount of time in minutes, the station will attempt to connect to primary SSID.

For detailed information about **Security** settings refer at the respective sections *Wireless security*

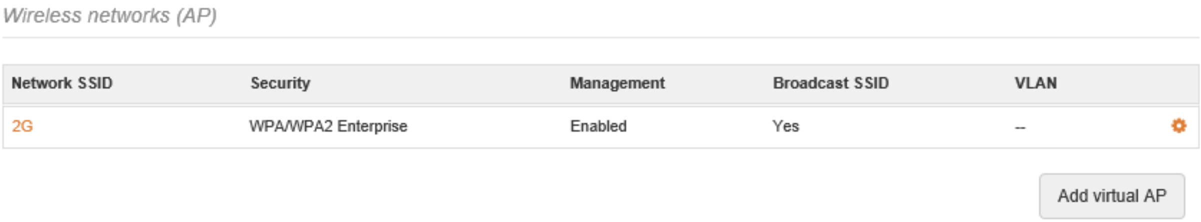
Enable WDS – use slide to enable WDS (Wireless Distribution System). With WDS enabled the wireless clients can easy pass through the access points with the same SSID.

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

Wireless networks (VAP) settings

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

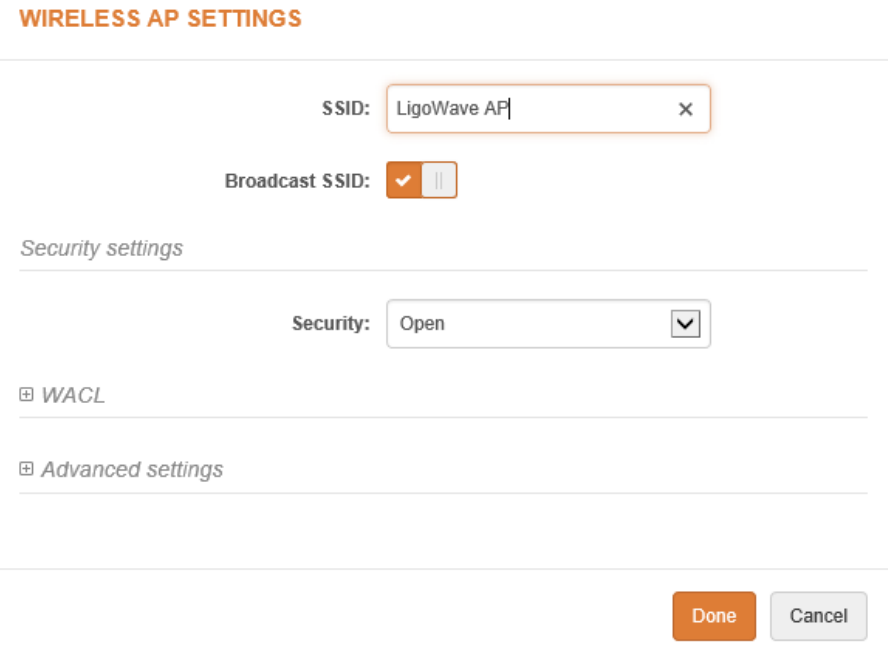


Wireless networks (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	
2G	WPA/WPA2 Enterprise	Enabled	Yes	--	⚙

Figure 32 - 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

Figure 33 – 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 VAP that station is associated with.

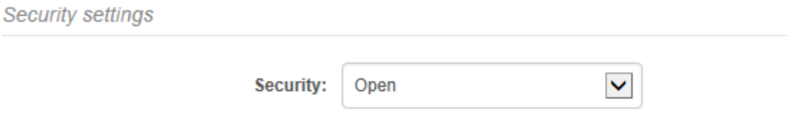
Each VAP of the LigoWave NFT supports following authentication/encryption methods:

- **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).
- **Hotspot (UAM)** – Web browser based user authentication method. UAM authentication is available only if Access Point is working in **router mode**.

Note that wireless clients must be able to respond with a specific security configuration.

Open

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



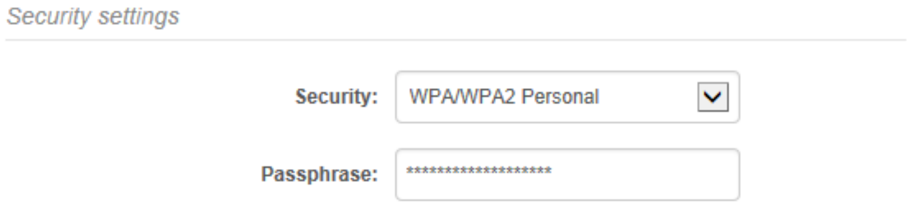
Security settings

Security: Open

Figure 34 – Wireless Security: Open

WPA/WPA2 Personal

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



Security settings

Security: WPA/WPA2 Personal

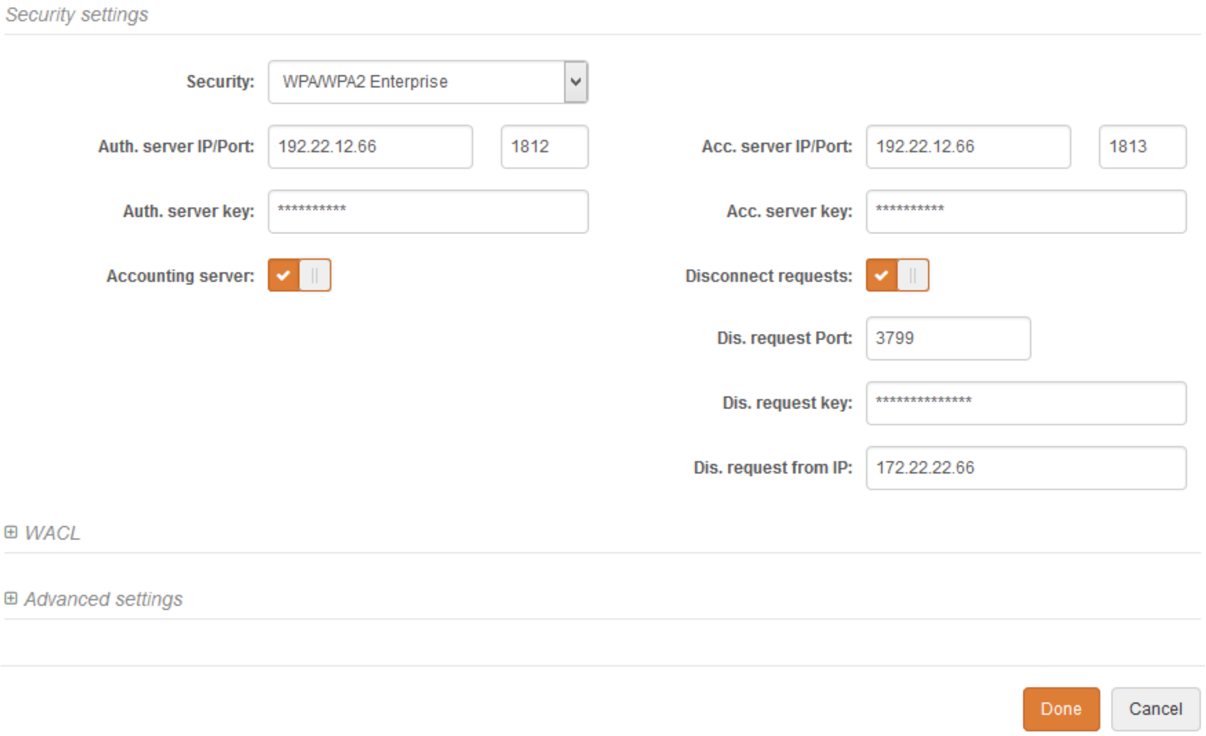
Passphrase: *******************

Figure 35 –Wireless Security: Personal WPA/WPA2 Security

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

WPA/WPA2 Enterprise

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

Security: WPA/WPA2 Enterprise

Auth. server IP/Port: 192.22.12.66 1812

Auth. server key: **********

Accounting server: ✓

Acc. server IP/Port: 192.22.12.66 1813

Acc. server key: **********

Disconnect requests: ✓

Dis. request Port: 3799

Dis. request key: **************

Dis. request from IP: 172.22.22.66

Figure 36 –Wireless Security: Enterprise WPA/WPA2 Security

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 send 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 send to.

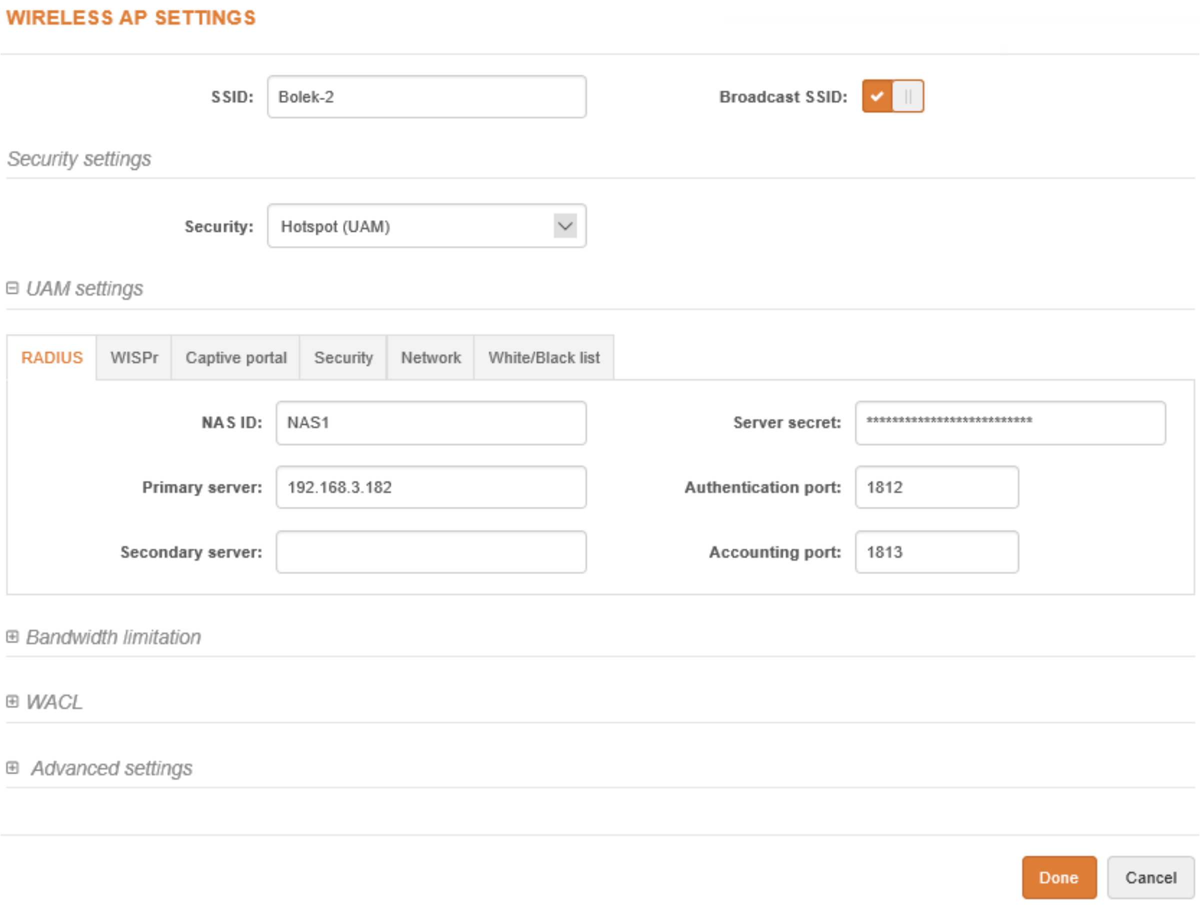
Acc. server key – enter the key for the authentication on specified accounting RADIUS server.

Hotspot (UAM)

Hotspot (UAM) security is available only if LigoWave NFT operates in Router mode.

With Hotspot (UAM) enabled, the wireless user provides login credentials and then Web portal attempts to authenticate and authorize the client using the provided information. Client will not send any authentication requests directly to the device, the Web portal will do this. On success, LigoWave NFT device will allow access to the Internet; otherwise Web portal will display failure notice.

Use Security section under Wireless AP settings page for UAM authentication configuration: choose the security option **Hotspot (UAM)** and fill all the required tabs (RADIUS, WISPr, Captive portal, Security, Network, Whitelist/Backlist) of the UAM settings:



WIRELESS AP SETTINGS

SSID: Bolek-2

Broadcast SSID: ✓

Security settings

Security: Hotspot (UAM)

⊟ UAM settings

NAS ID: NAS1

Server secret: **************************

Primary server: 192.168.3.182

Authentication port: 1812

Secondary server:

Accounting port: 1813

Figure 37 - UAM Configuration: RADIUS Setup

RADIUS Settings:

NAS ID – specify the NAS identifier.

Primary server – specify the name or IP address of the primary RADIUS server.

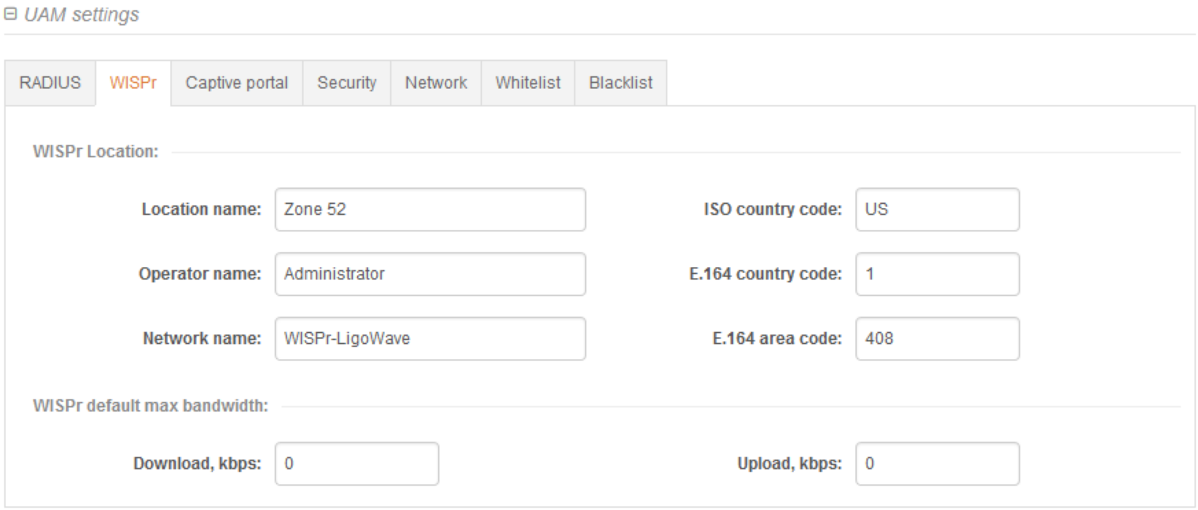
Secondary server – specify the name or IP address of the secondary RADIUS server (optional).

Server secret – specify the RADIUS shared secret.

Authentication port – specify the UDP port number to use for radius authentication requests, default 1812

Accounting port – specify the UDP port number to use for radius accounting requests, default 1813.

WISPr Settings



WISPr Location:

Location name: Zone 52

ISO country code: US

Operator name: Administrator

E.164 country code: 1

Network name: WISPr-LigoWave

E.164 area code: 408

WISPr default max bandwidth:

Download, kbps: 0

Upload, kbps: 0

Figure 38 - UAM Configuration: WISPr Settings

WISPr location name – specify the WISPr location name.

Operator name – specify the operator's name

Network name – specify the network name

ISO country code – specify the country code in ISO standard.

E.164 country code – specify the country code in E.164 standard.

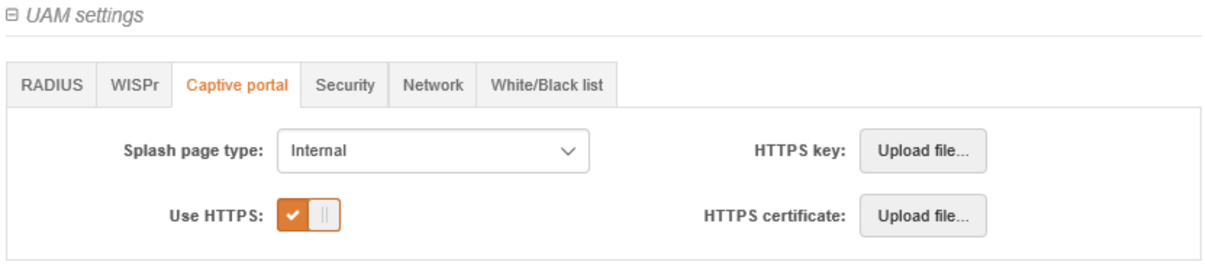
E.164 area code – specify the area code in E.164 standard.

WISPr default max bandwidth – specify the default bandwidth limitation for clients. Note that if the external RADIUS server has traffic limitations preconfigured, then RADIUS overrides these settings.

Download, kbps – specify max download bandwidth in kbps.

Upload, kbps – specify the max upload bandwidth in kbps.

Captive portal settings:



Splash page type: Internal

HTTPS key: Upload file...

Use HTTPS: ☑

HTTPS certificate: Upload file...

Figure 39 - UAM Configuration: Internal Captive Portal Settings

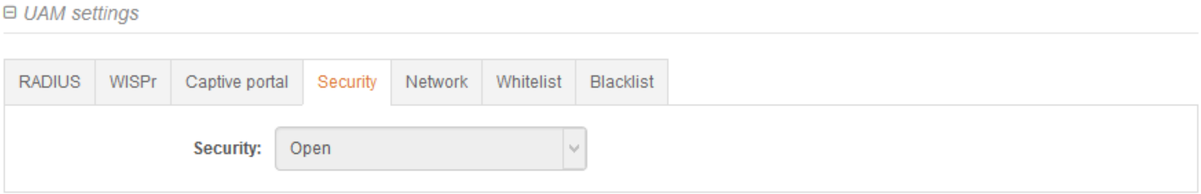
Splash page type – choose the authentication Web portal type: internal or external.

- **Internal** – use the built in authentication Web page. If selected, then when users first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data will be sent to the Radius Server for authentication.
- **External** – specify the existing external authentication Web page URLs and portal. If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL specified below.

Use HTTPS – enable to use the HTTPS protocol for connection and authentication.

- **HTTPS key** – upload a PEM formatted private key file.
- **HTTPS certificate** – upload a PEM formatted certificate file.

Security



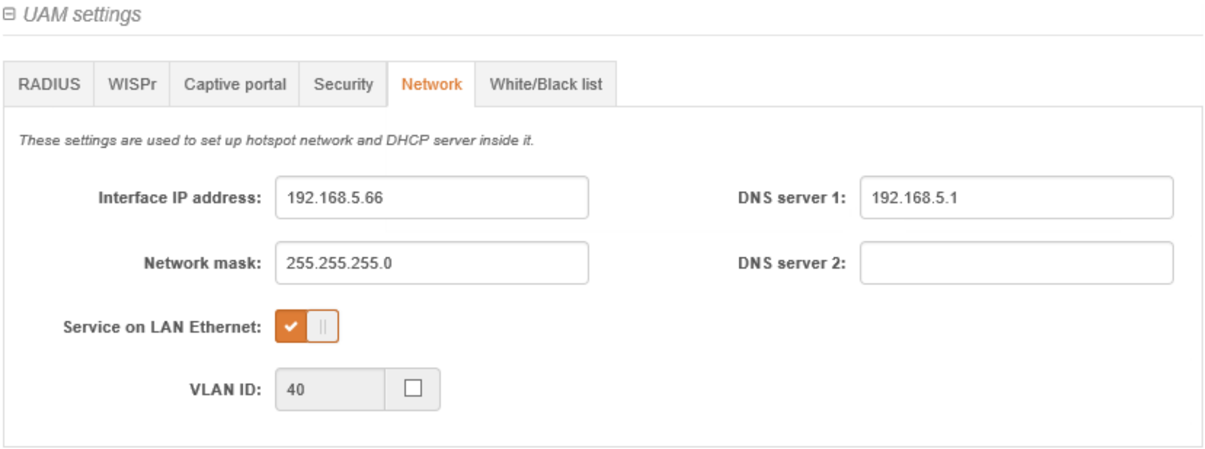
Security: Open

Figure 40 - UAM Configuration: Data Security Settings

Security settings – choose the data encryption method:

- **Open** – no encryption.
- **WPA/WPA2 personal** – preshared key encryption with WPA/WPA2 using AES method.

Network



These settings are used to set up hotspot network and DHCP server inside it.

Interface IP address: 192.168.5.66

DNS server 1: 192.168.5.1

Network mask: 255.255.255.0

DNS server 2:

Service on LAN Ethernet: ✓

VLAN ID: 40 □

Figure 41 - UAM Configuration: Network Settings

Interface IP address – specify the LAN interface IP address. Note that LAN settings on Network menu will be disabled if UAM is enabled.

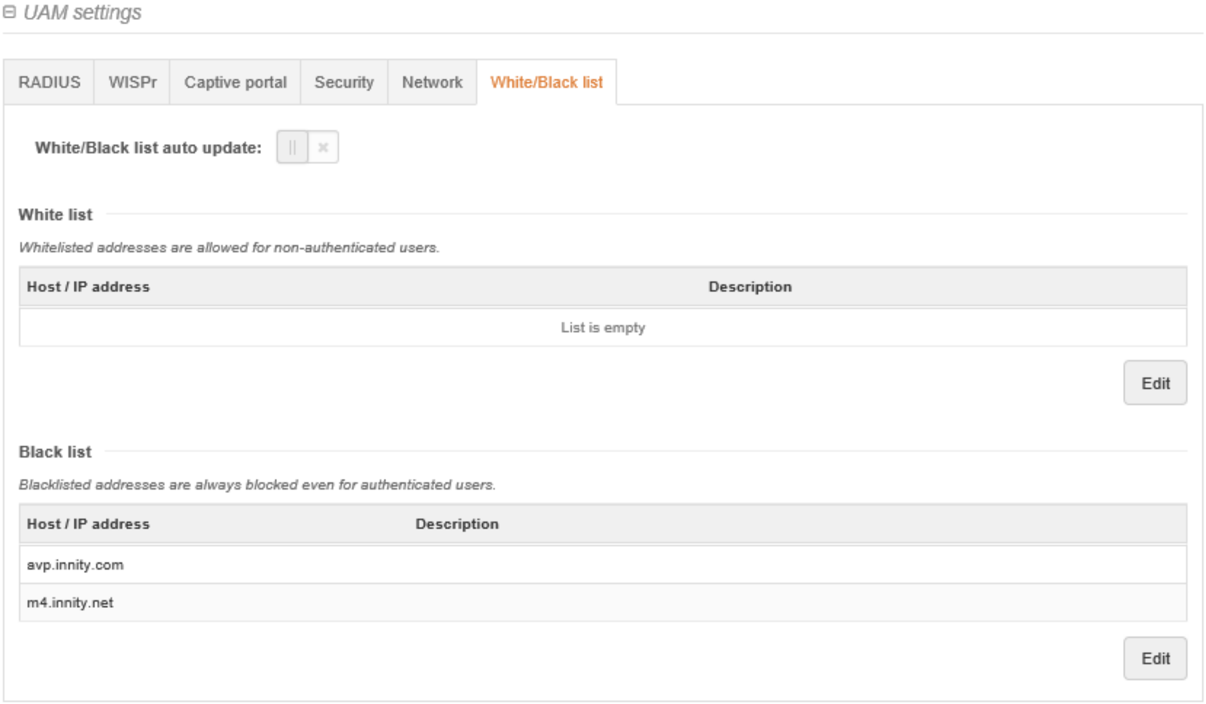
Network mask – specify the subnet mask.

VLAN ID – specify the VLAN ID for traffic tagging [2-4095]. The client devices that associate using the particular SSID will be grouped into this VLAN.

DNS servers – specify DNS servers.

Whitelist/Blacklist

The **white** and **black** access lists control user access to Web content through the LigoWave NFT device. The unauthenticated users will be allowed to access sites from white list while access to the sites from black list will be denied even for authenticated users.



⊟ UAM settings

RADIUS | WISPr | Captive portal | Security | Network | White/Black list

White/Black list auto update: ☒

White list

Whitelisted addresses are allowed for non-authenticated users.

Host / IP address	Description
List is empty	

Edit

Black list

Blacklisted addresses are always blocked even for authenticated users.

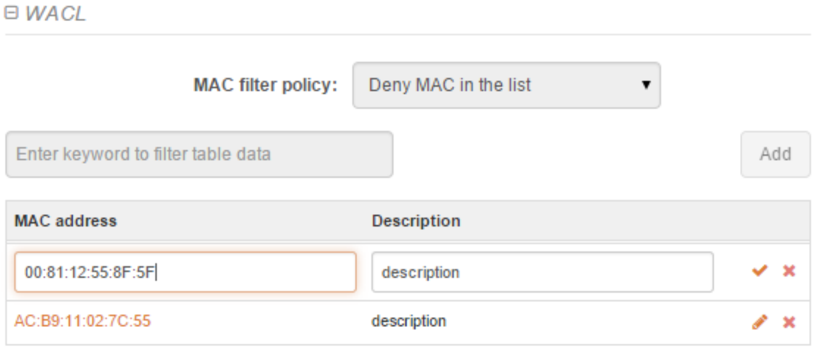
Host / IP address	Description
avp.innity.com	
m4.innity.net	

Edit

Figure 42 - UAM Configuration: White/Black List

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).



⊟ WACL

MAC filter policy: Deny MAC in the list ▾

Enter keyword to filter table data | Add

MAC address	Description	
00:81:12:55:8F:5F	description	✓ ✖
AC:B9:11:02:7C:55	description	✎ ✖

Figure 43 – Wireless ACL Configuration

MAC filter policy – define the main VAP policy:

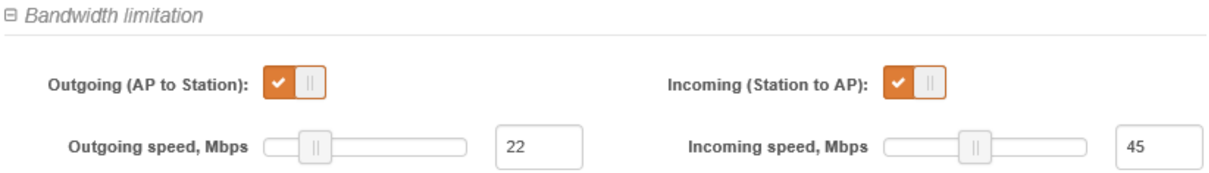
- **Open** – no rules applied.
- **Allow MAC in the list** – only listed MAC clients can connect to the VAP (white list).
- **Deny MAC in the list** – only listed MAC clients can NOT connect to the VAP (black list).

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.

Bandwidth limitation



⊟ Bandwidth limitation

Outgoing (AP to Station): ✓

Outgoing speed, Mbps: 22

Incoming (Station to AP): ✓

Incoming speed, Mbps: 45

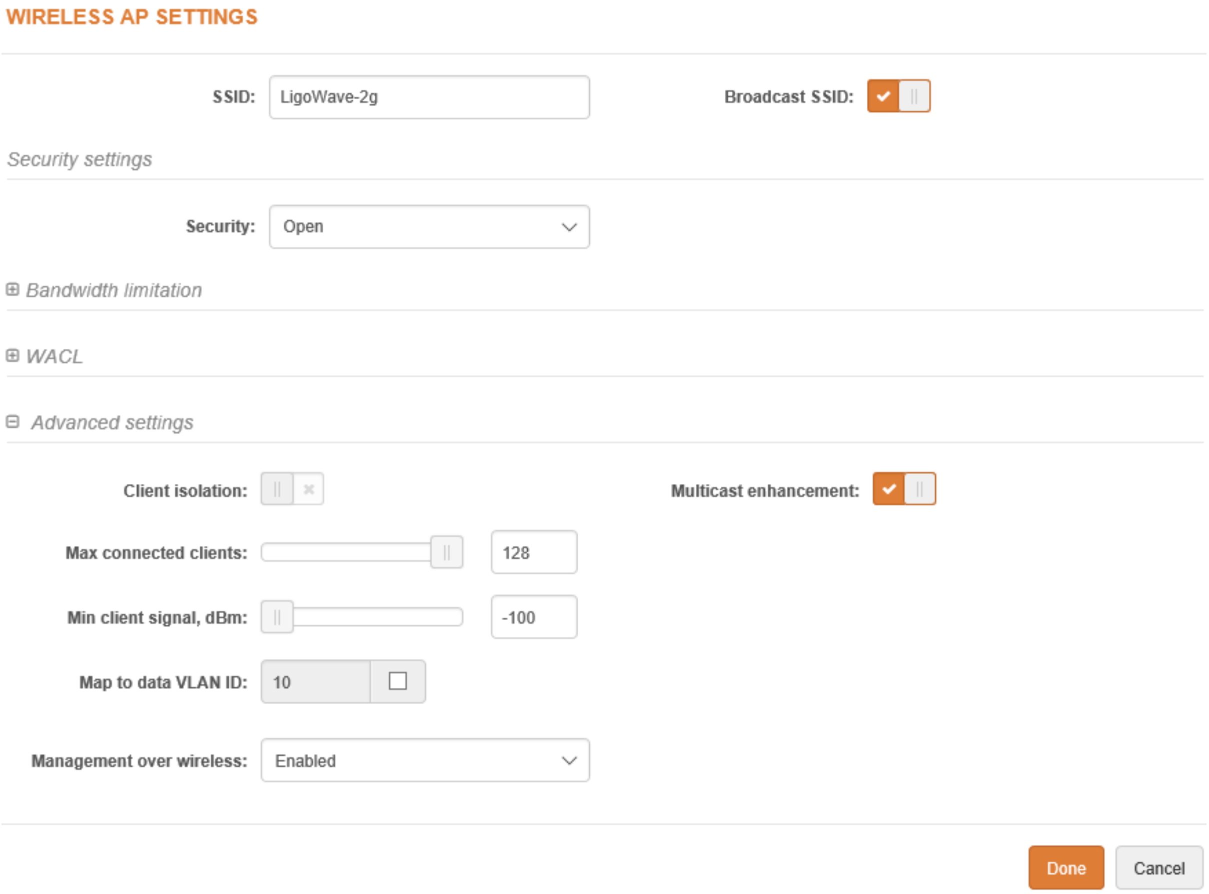
Figure 44 - Bandwidth Limitation

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced settings

Advanced wireless settings allow configuring VAP to get the best performance/capacity of the link:



WIRELESS AP SETTINGS

SSID: LigoWave-2g

Broadcast SSID: ✓

Security settings

Security: Open

⊞ Bandwidth limitation

⊞ WACL

⊟ Advanced settings

Client isolation: ✗

Multicast enhancement: ✓

Max connected clients: 128

Min client signal, dBm: -100

Map to data VLAN ID: 10 □

Management over wireless: Enabled

Figure 45 – 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 VAP interface.

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 devices that associate using the particular SSID will be grouped into this VLAN.

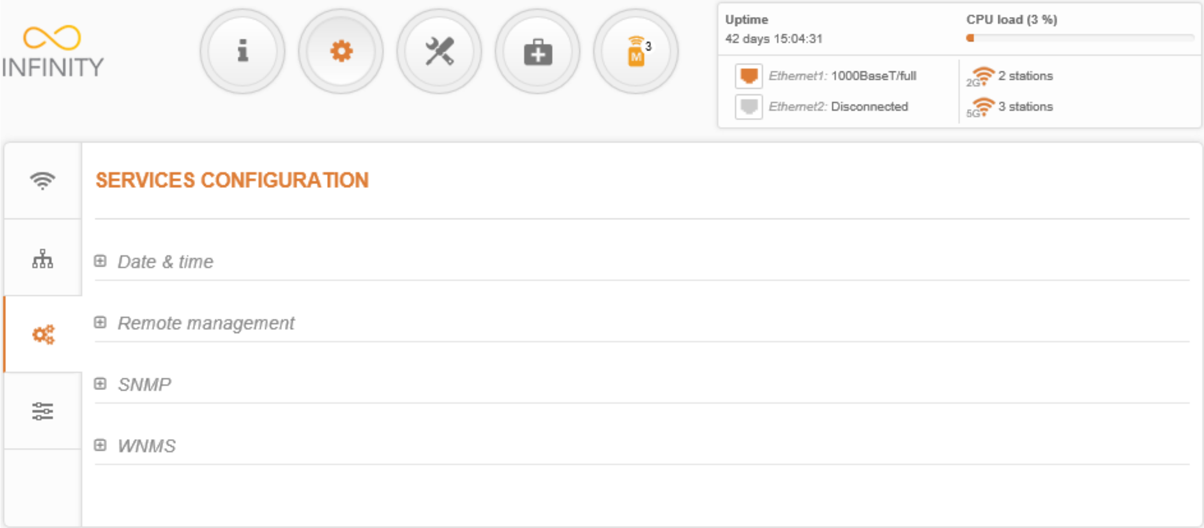
Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead require a physical network connection using an Ethernet cable for administrative access to LigoWave NFT.

Multicast enhancement – using IGMP snooping, the **Multicast Enhancement** option isolates multicast traffic from unregistered clients and allows the LigoWave NFT device to send multicast traffic to registered clients using higher data rates. This lessens the risk of traffic overload on PtMP links and increases the reliability of multicast traffic since packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, then you may need to disable the Multicast Enhancement option. By default this option is enabled.

Services configuration

Use **Services** menu is divided into further five sections:

- Date & time
- Remote management
- SNMP
- WNMS



Uptime 42 days 15:04:31

CPU load (3 %)

Ethernet1: 1000BaseT/full

Ethernet2: Disconnected

2G 2 stations

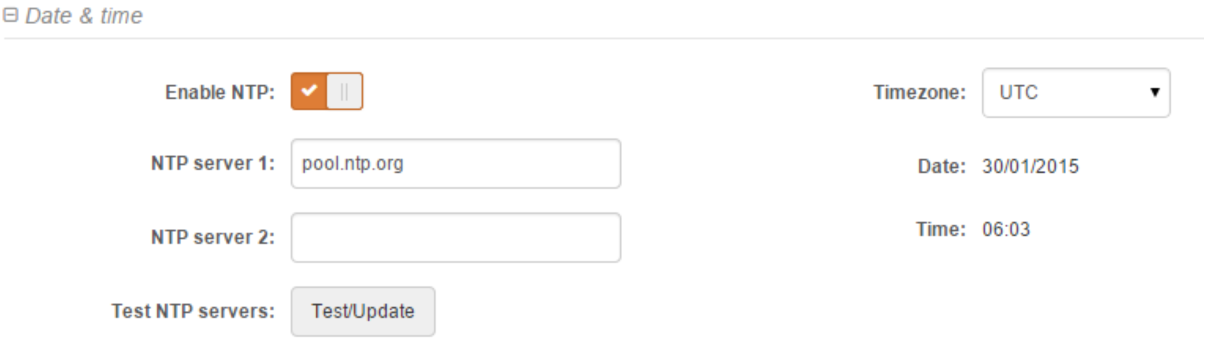
5G 3 stations

Figure 46 - 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.



Enable NTP: ☑

NTP server 1: pool.ntp.org

NTP server 2:

Test NTP servers: Test/Update

Timezone: UTC

Date: 30/01/2015

Time: 06:03

Figure 47 – Date&time: NTP Configuration

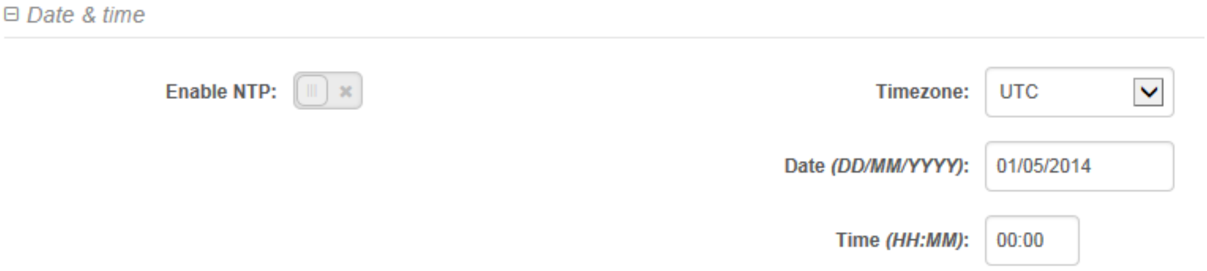
Enable NTP – select this option as enabled to configure NTP.

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 server's responses successfully.

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



⊟ *Date & time*

Enable NTP: ☒

Timezone: UTC

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

Time *(HH:MM)*: 00:00

Figure 48 – Date&time: Manual Configuration

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

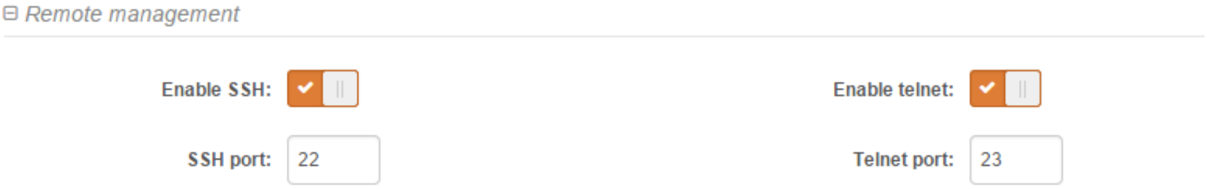
Timezone – select the timezone. Time zone should be specified as a difference between local time and UTC time.

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

Time – specify the time in format HH:MM.

Remote management

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



⊟ *Remote management*

Enable SSH: ✓

SSH port: 22

Enable telnet: ✓

Telnet port: 23

Figure 49 – Remote Management Configuration

Enable SSH – enable or disable SSH access to device.

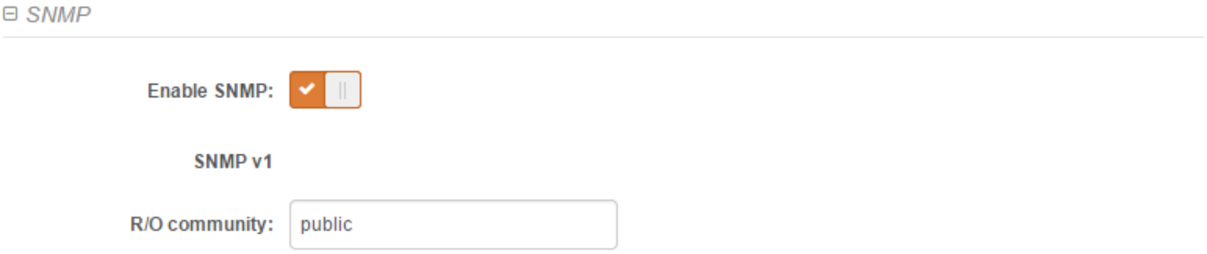
SSH port – specify the SSH service port. By default SSH port is 22.

Enable telnet – enable or disable telnet access to device.

Telnet port – specify the telnet port. By default, telnet 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.



⊟ *SNMP*

Enable SNMP: ✓

SNMP v1

R/O community: public

Figure 50 – SNMP Service Settings

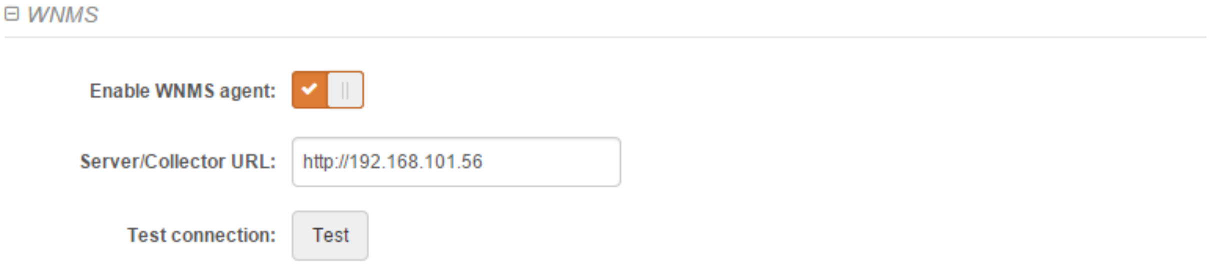
Enable SNMP – specify the SNMP service status.

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

If the **Infinity Controller** functionality is enabled, the is no need to use WNMS monitoring system, therefore WNMS option will be disabled.

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*

Enable WNMS agent: ☑

Server/Collector URL: http://192.168.101.56

Test connection: Test

Enable WNMS agent – select to enable WNMS agent.

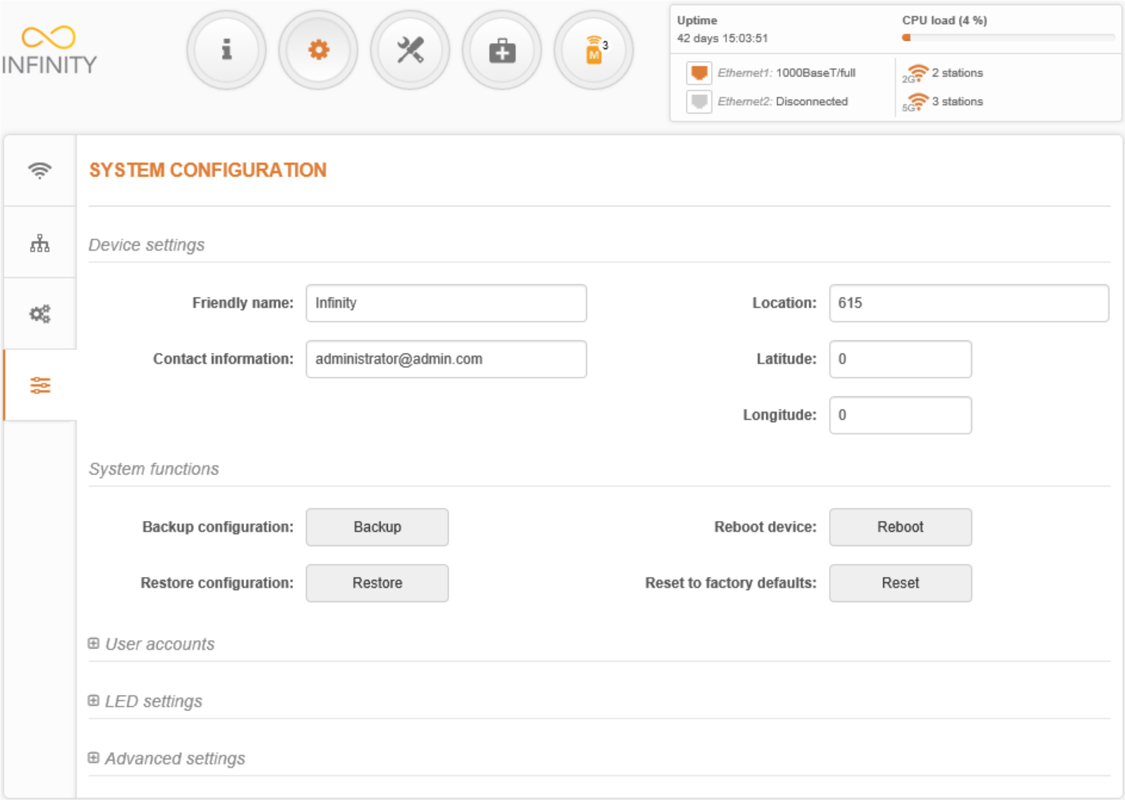
Server/Collector URL – specify the URL of the WMS server to which that heartbeat notifications will be sent to.

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
- LED usage
- Advanced settings



Uptime
42 days 15:03:51

CPU load (4 %)

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 2 stations
5G 3 stations

SYSTEM CONFIGURATION

Device settings

Friendly name:	Infinity	Location:	615
Contact information:	administrator@admin.com	Latitude:	0
		Longitude:	0

System functions

Backup configuration:	Backup	Reboot device:	Reboot
Restore configuration:	Restore	Reset to factory defaults:	Reset

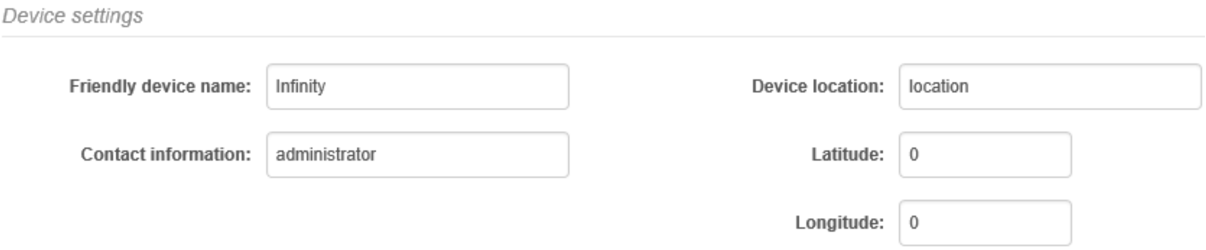
⊞ *User accounts*

⊞ *LED settings*

⊞ *Advanced settings*

Figure 51 - System Menu

Device settings



Device settings

Friendly device name:	Infinity	Device location:	location
Contact information:	administrator	Latitude:	0
		Longitude:	0

Figure 52- Device Settings

Friendly device name – specify name of the LigoWave NFT that will be used to identify the unit.

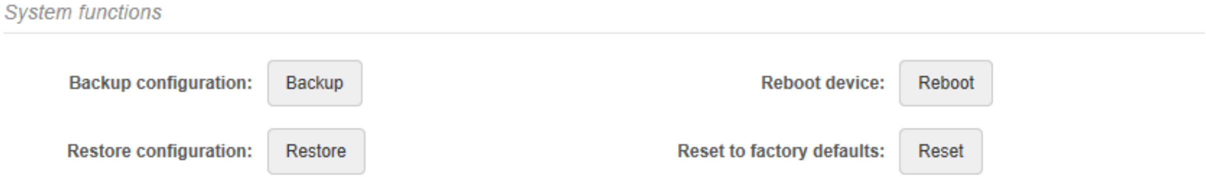
Contact information – specify the name of the contact person, such as a network administrator, for the LigoWave NFT.

Device location – describe the location of the device.

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

Latitude – specify the latitude coordinates of the device [specific decimal format, e.q. 23.891058]. Both coordinates help indicate accurate location of the device.

System functions



System functions

Backup configuration:	Backup	Reboot device:	Reboot
Restore configuration:	Restore	Reset to factory defaults:	Reset

Figure 53 - 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.

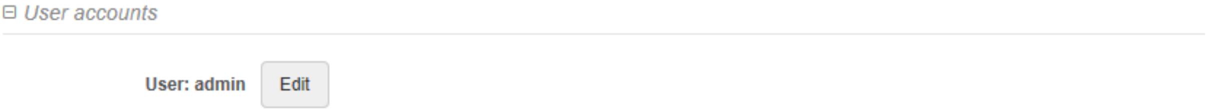
Reboot device – reboot device with the last saved configuration.

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.

User accounts

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



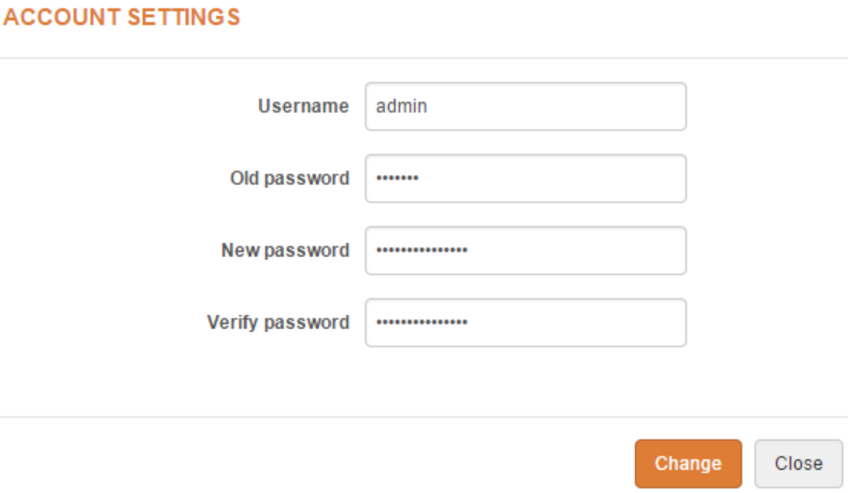
⊟ User accounts

User: admin

Figure 54 – User Accounts

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

Click **Edit** button next to user for changing credentials:



ACCOUNT SETTINGS

Username: admin
Old password: •••••••
New password: •••••••••••••••
Verify password: •••••••••••••••

Figure 55 – User Account Settings

Username – change the administrator’s username.

Old password – enter the old administrator password.

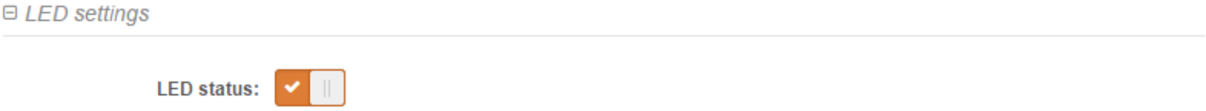
New password – enter the new administrator password for user authentication.

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.

LED settings

The LigoNFT device has possibility to control LEDs.



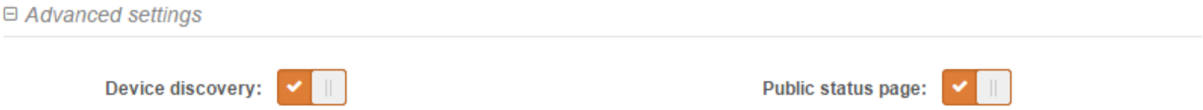
⊟ *LED settings*

LED status: ✓

Figure 56 – Device LED Control

LED status – use the slide to disable or enable LED signals on the unit. If disabled, no LEDs will light up on the device.

Advanced settings



⊟ *Advanced settings*

Device discovery: ✓

Public status page: ✓

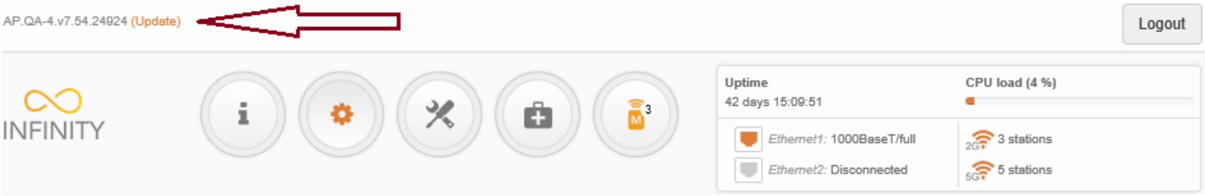
Figure 57 – Device discovery

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.



AP.QA-4.v7.54.24924 (Update)

Uptime
42 days 15:09:51

CPU load (4 %)

Ethernet1: 1000BaseT/full

Ethernet2: Disconnected

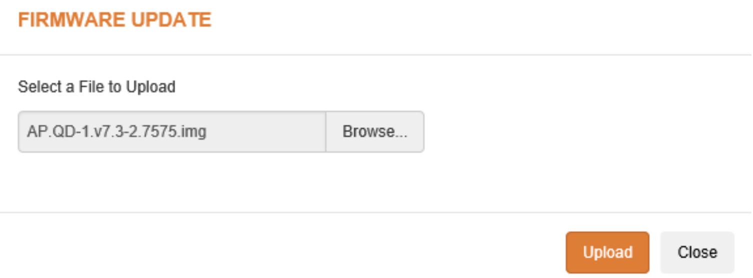
2G 3 stations

5G 5 stations

Figure 58 – 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:



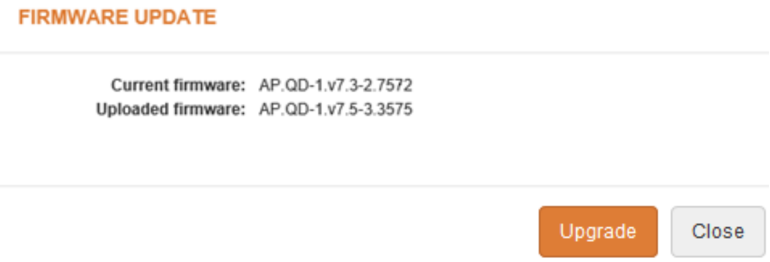
FIRMWARE UPDATE

Select a File to Upload

AP.QD-1.v7.3-2.7575.img

Figure 59 – 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 UPDATE

Current firmware: AP.QD-1.v7.3-2.7572
Uploaded firmware: AP.QD-1.v7.5-3.3575

Figure 60 –Firmware Upgrade

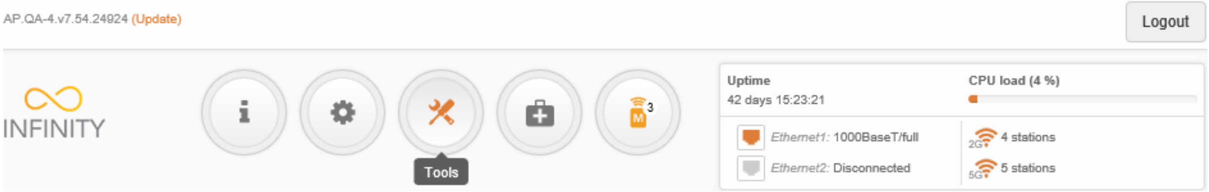
Current version – displays version of the current firmware.

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



AP.QA-4.v7.54.24924 (Update)

Logout

Uptime
42 days 15:23:21

CPU load (4 %)

Ethernet1: 1000BaseT/full

Ethernet2: Disconnected

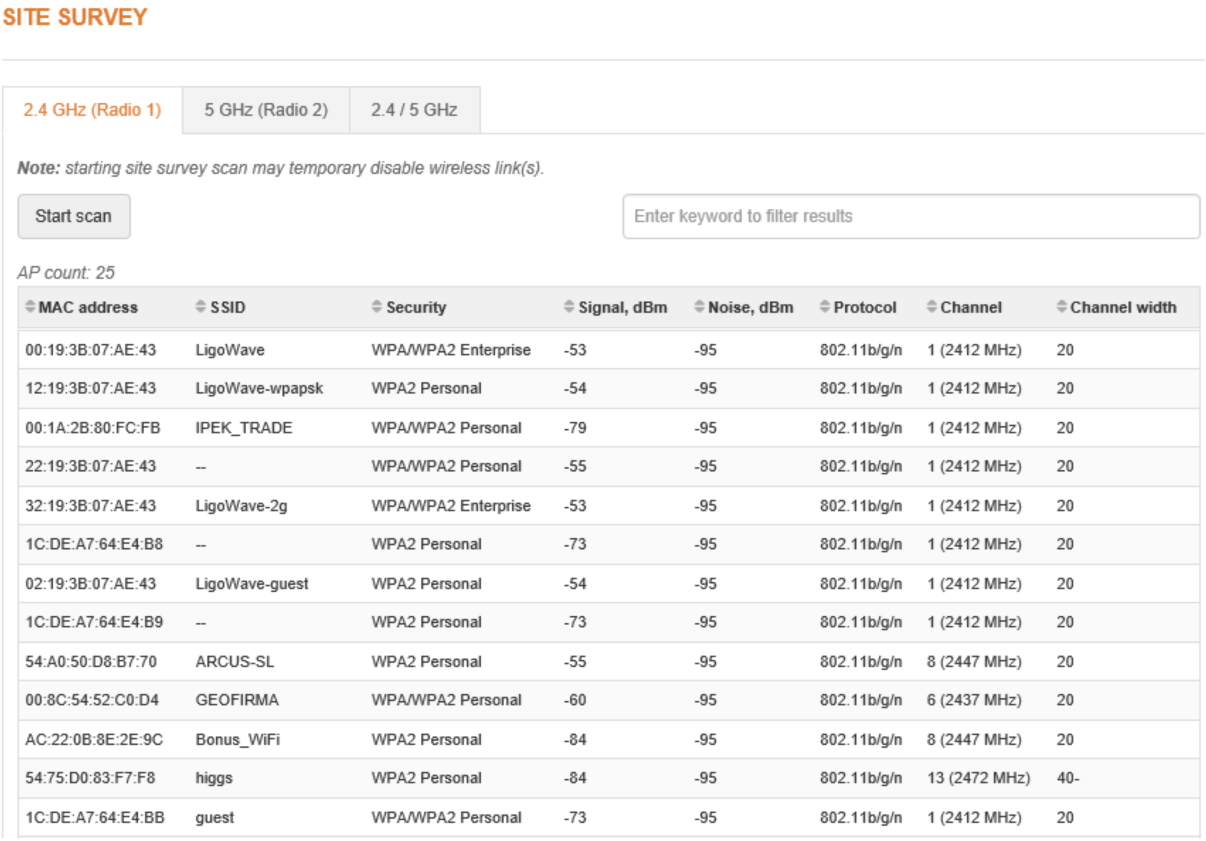
2G 4 stations

5G 5 stations

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, channel width, encryption and see signal/noise levels.

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



SITE SURVEY

2.4 GHz (Radio 1) | 5 GHz (Radio 2) | 2.4 / 5 GHz

Note: *starting site survey scan may temporary disable wireless link(s).*

Start scan

Enter keyword to filter results

AP count: 25

MAC address	SSID	Security	Signal, dBm	Noise, dBm	Protocol	Channel	Channel width
00:19:3B:07:AE:43	LigoWave	WPA/WPA2 Enterprise	-53	-95	802.11b/g/n	1 (2412 MHz)	20
12:19:3B:07:AE:43	LigoWave-wpapsk	WPA2 Personal	-54	-95	802.11b/g/n	1 (2412 MHz)	20
00:1A:2B:80:FC:FB	IPEK_TRADE	WPA/WPA2 Personal	-79	-95	802.11b/g/n	1 (2412 MHz)	20
22:19:3B:07:AE:43	--	WPA/WPA2 Personal	-55	-95	802.11b/g/n	1 (2412 MHz)	20
32:19:3B:07:AE:43	LigoWave-2g	WPA/WPA2 Enterprise	-53	-95	802.11b/g/n	1 (2412 MHz)	20
1C:DE:A7:64:E4:B8	--	WPA2 Personal	-73	-95	802.11b/g/n	1 (2412 MHz)	20
02:19:3B:07:AE:43	LigoWave-guest	WPA2 Personal	-54	-95	802.11b/g/n	1 (2412 MHz)	20
1C:DE:A7:64:E4:B9	--	WPA2 Personal	-73	-95	802.11b/g/n	1 (2412 MHz)	20
54:A0:50:D8:B7:70	ARCUS-SL	WPA2 Personal	-55	-95	802.11b/g/n	8 (2447 MHz)	20
00:8C:54:52:C0:D4	GEOFIRMA	WPA/WPA2 Personal	-60	-95	802.11b/g/n	6 (2437 MHz)	20
AC:22:0B:8E:2E:9C	Bonus_WiFi	WPA2 Personal	-84	-95	802.11b/g/n	8 (2447 MHz)	20
54:75:D0:83:F7:F8	higgs	WPA2 Personal	-84	-95	802.11b/g/n	13 (2472 MHz)	40-
1C:DE:A7:64:E4:BB	guest	WPA/WPA2 Personal	-73	-95	802.11b/g/n	1 (2412 MHz)	20

Figure 61 – Site Survey Results

Start/Stop scan – click to start or to stop the scan.

Additionally, two charts display connected **Device count** and **Signal leve**l on particular frequencies. The grey colored column represents LigoNFT unit's current operating frequency:

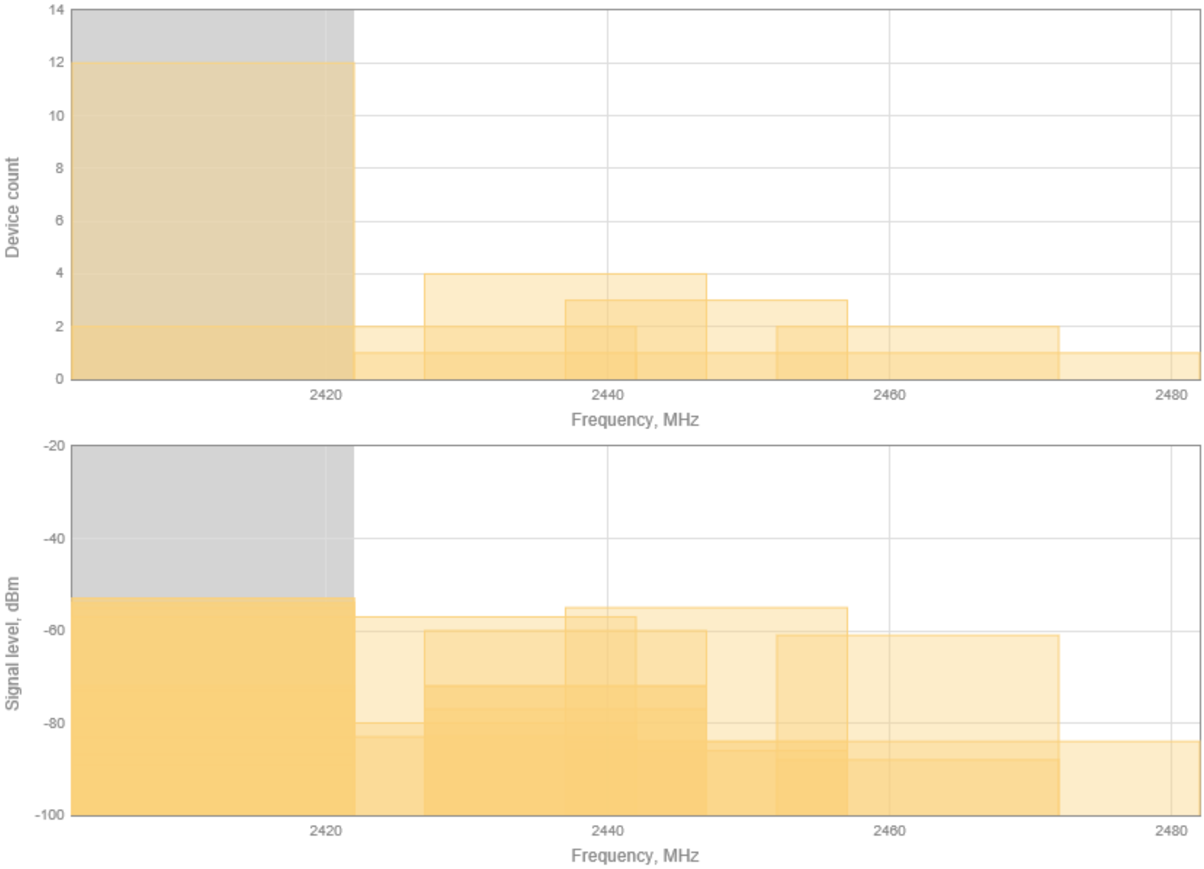
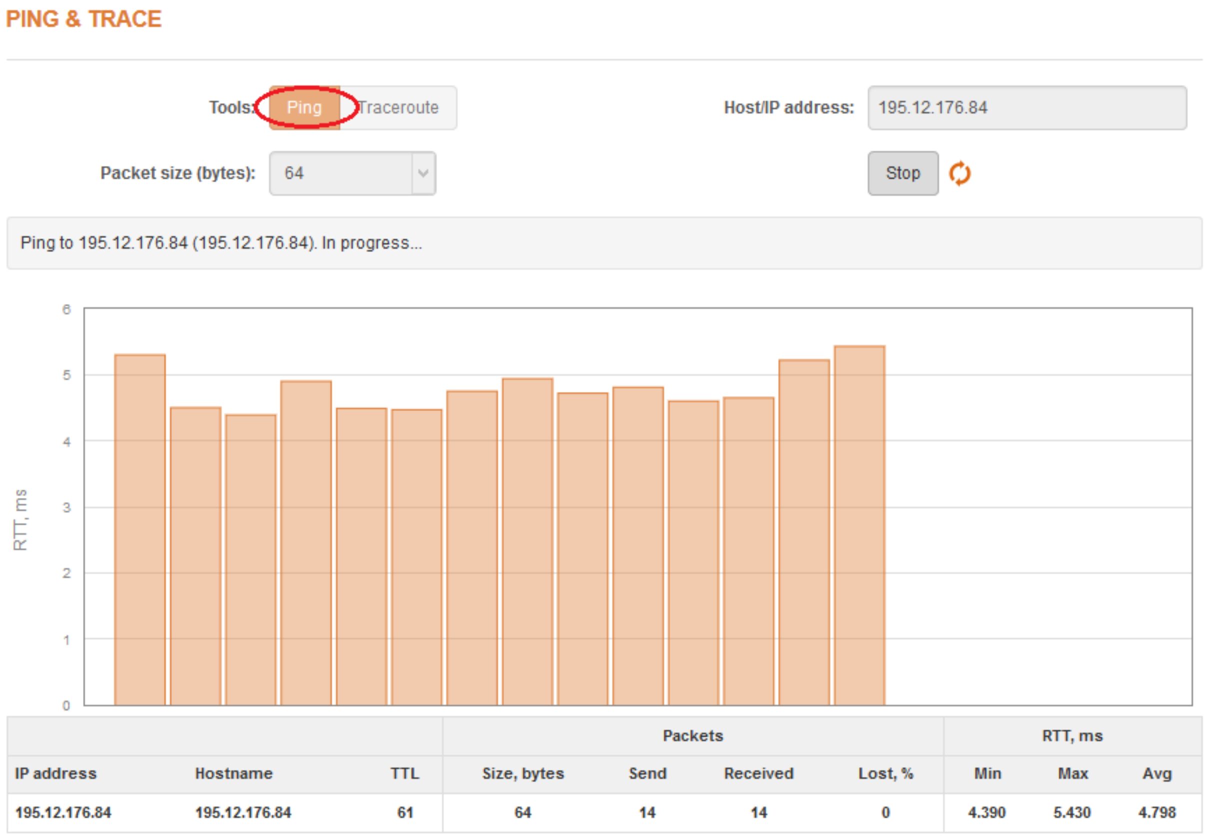


Figure 62 - Site Survey Charts: Device count and Signal level.

Ping & Trace

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



PING & TRACE

Tools: [✓ Ping] Traceroute

Host/IP address: 195.12.176.84

Packet size (bytes): 64

Stop

Ping to 195.12.176.84 (195.12.176.84). In progress...

			Packets				RTT, ms		
IP address	Hostname	TTL	Size, bytes	Send	Received	Lost, %	Min	Max	Avg
195.12.176.84	195.12.176.84	61	64	14	14	0	4.390	5.430	4.798

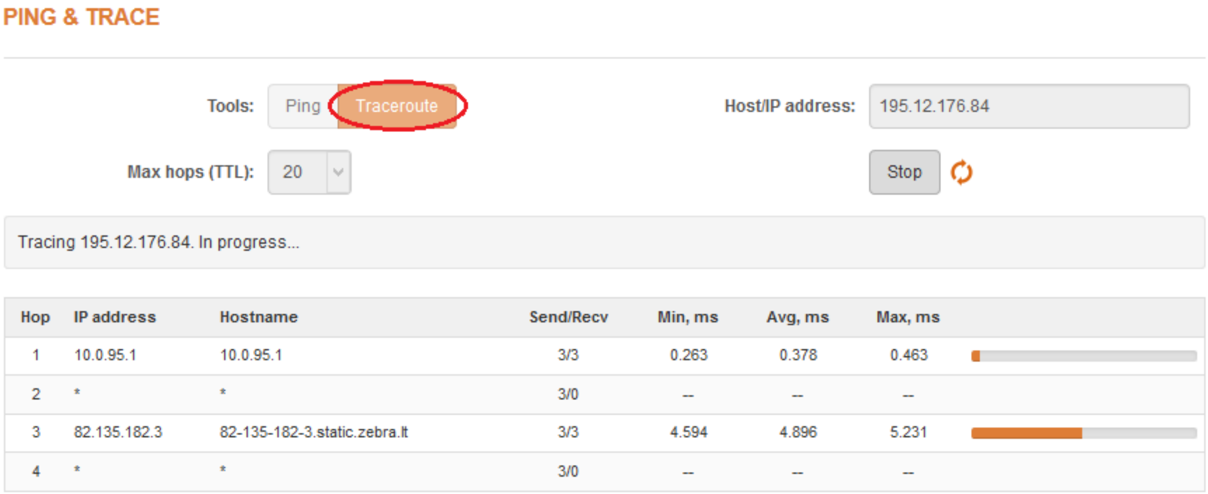
Figure 63 - Ping tool

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 LigoWave NFT unit. This is useful when trying to find out why destination is unreachable, as you will be able to see where the connection fails.



PING & TRACE

Tools: Ping [✓ Traceroute]

Host/IP address: 195.12.176.84

Max hops (TTL): 20

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	--	--	--

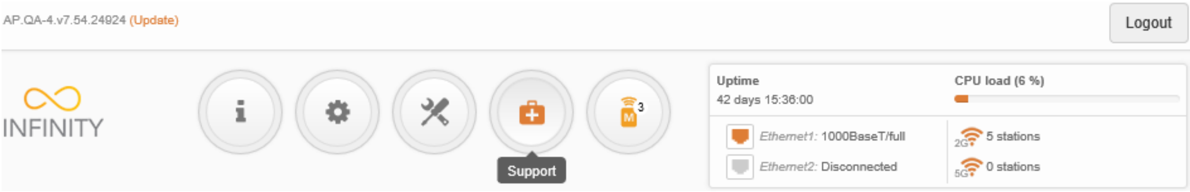
Figure 64 - Trace tool

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.

Support



Uptime
42 days 15:36:00

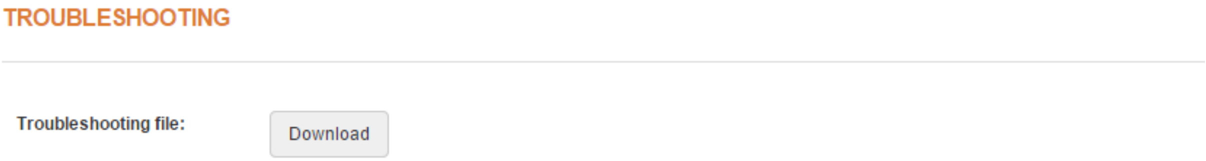
CPU load (6 %)

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 5 stations
5G 0 stations

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

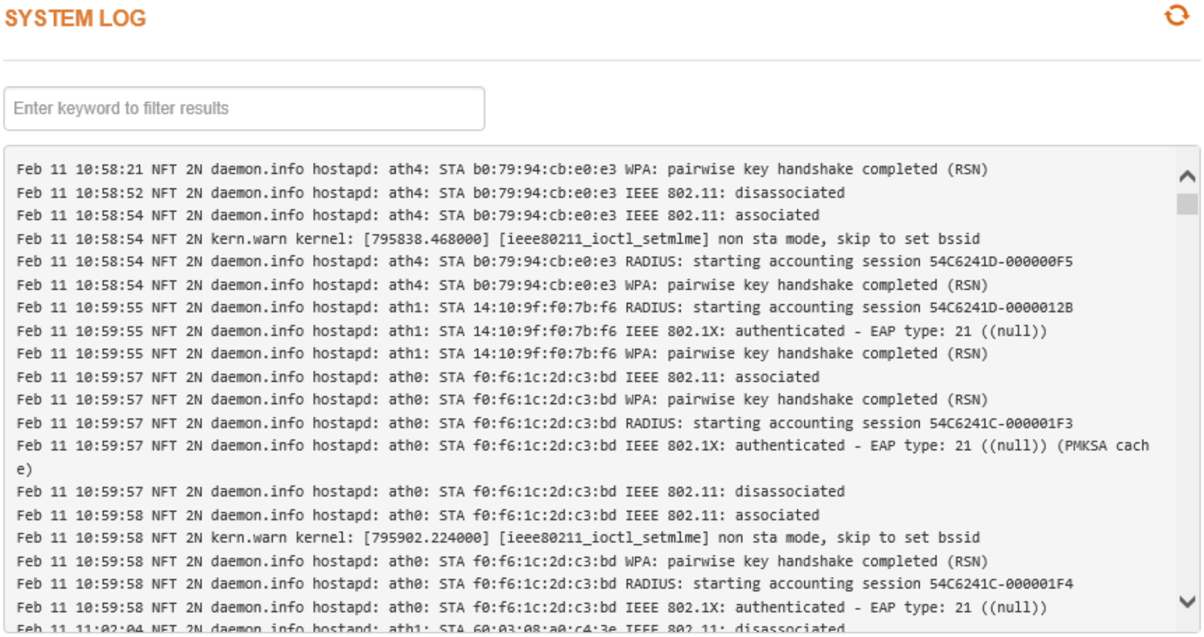
Troubleshooting file: Download

Figure 65 – Troubleshooting File Download

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

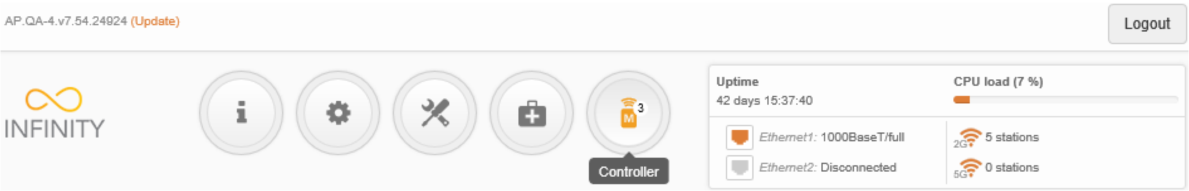
Enter keyword to filter results

```
Feb 11 10:58:21 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 WPA: pairwise key handshake completed (RSN)
Feb 11 10:58:52 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 IEEE 802.11: disassociated
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 IEEE 802.11: associated
Feb 11 10:58:54 NFT 2N kern.warn kernel: [795838.468000] [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 RADIUS: starting accounting session 54C6241D-000000F5
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 RADIUS: starting accounting session 54C6241D-0000012B
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 IEEE 802.1X: authenticated - EAP type: 21 ((null))
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: associated
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd RADIUS: starting accounting session 54C6241C-000001F3
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.1X: authenticated - EAP type: 21 ((null)) (PMKSA cach
e)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: disassociated
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: associated
Feb 11 10:59:58 NFT 2N kern.warn kernel: [795902.224000] [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd RADIUS: starting accounting session 54C6241C-000001F4
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.1X: authenticated - EAP type: 21 ((null))
Feb 11 11:02:04 NFT 2N daemon.info hostapd: ath1: STA 60:03:08:a0:c4:3e IEEE 802.11: disassociated
```

Figure 66 – Device System Log

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

Infinity Controller



AP.QA-4.v7.54.24924 (Update)

Uptime
42 days 15:37:40

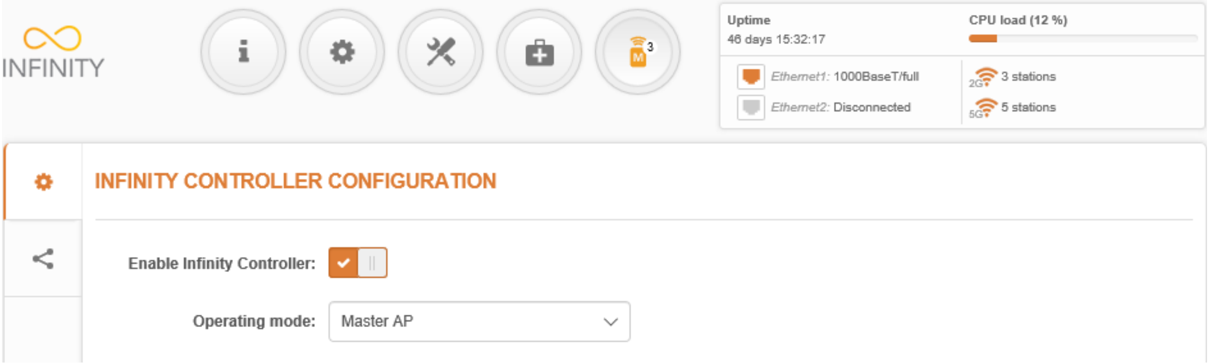
CPU load (7 %)

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 5 stations
5G 0 stations

The ecosystem is self-configuring system that allows to easy maintain or expand network. The system can be integrated, or external (network management system):

- **Integrated** – the local network that is made of **Managed AP**s and the **Master AP**. All Managed APs are managed by the Master AP.
- **External** – the network that is made of **Cloud AP**s and is managed by the Infinity Controller software located on a server.



Uptime
46 days 15:32:17

CPU load (12 %)

Ethernet1: 1000BaseT/full
Ethernet2: Disconnected

2G 3 stations
5G 5 stations

INFINITY CONTROLLER CONFIGURATION

Enable Infinity Controller: ☑

Operating mode: Master AP

Figure 67 – Infinity Controller's Configuration

Enable Infinity Controller – use this option to enable or disable Infinity Controller functionality on LigoNFT device.

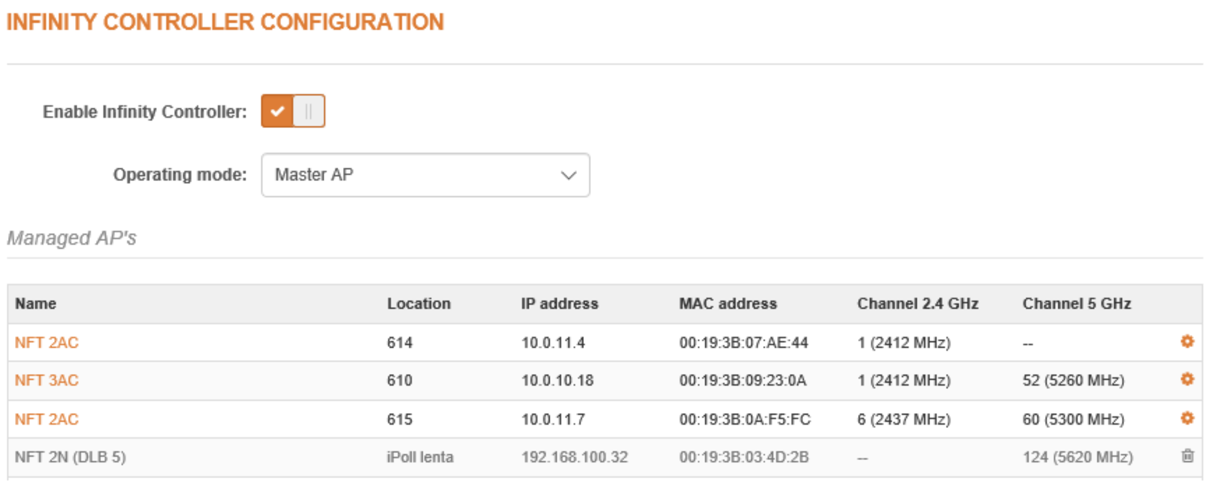
Operating mode – select the LigoNFT device’s role in Infinity Controller system:

- **Master AP** – the Master AP controls all Managed APs running on the same network (Integrated Infinity Controller system).
- **Managed AP** – if enabled, unit will wait for automatic configuration upload from the Master AP running on this network (Integrated Infinity Controller system).
- **Cloud AP** – if enabled, unit will wait for automatic configuration upload from the registered External Infinity Controller.

Integrated Infinity Controller: Master AP

Choose the **Master AP** to create the Integrated Infinity Controller system. Master AP is responsible for configuration of new out-of-box devices, connected into the local network. Once configured, the Master AP will automatically apply its configuration on each Managed AP, connected to the same network.

Once the Managed AP connects to the network, it automatically will appear on the Master’s AP UI, on Controller page, under the Managed AP table, where is possible to change individual settings for each Managed AP.



INFINITY CONTROLLER CONFIGURATION

Enable Infinity Controller: ☑

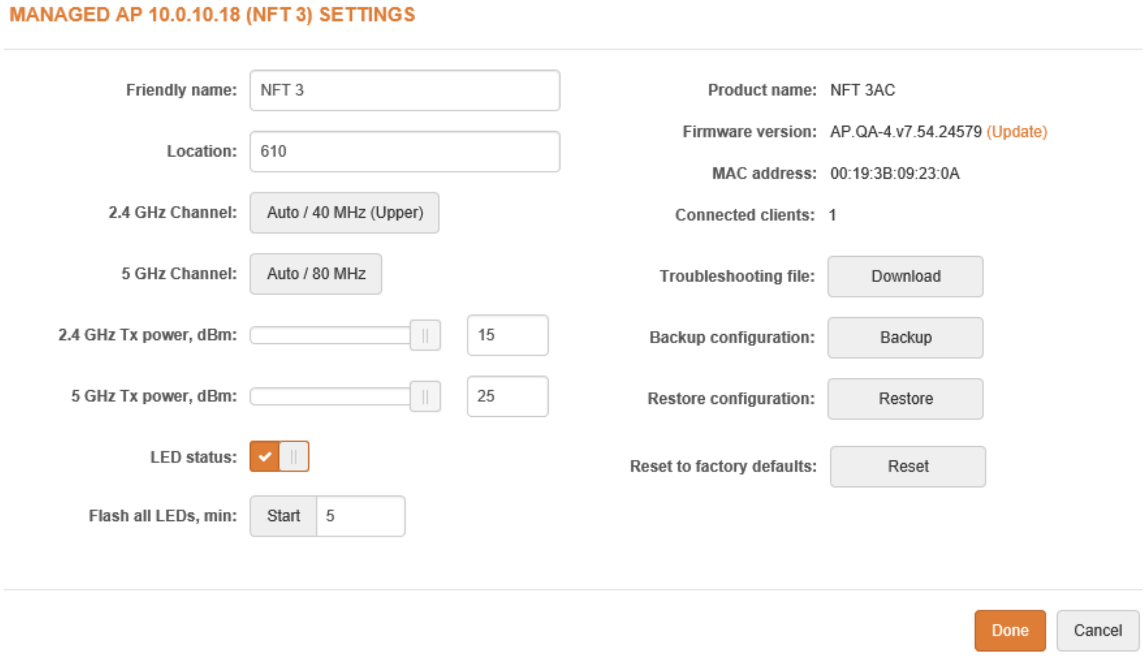
Operating mode: Master AP

Managed AP's

Name	Location	IP address	MAC address	Channel 2.4 GHz	Channel 5 GHz	
NFT 2AC	614	10.0.11.4	00:19:3B:07:AE:44	1 (2412 MHz)	--	⚙
NFT 3AC	610	10.0.10.18	00:19:3B:09:23:0A	1 (2412 MHz)	52 (5260 MHz)	⚙
NFT 2AC	615	10.0.11.7	00:19:3B:0A:F5:FC	6 (2437 MHz)	60 (5300 MHz)	⚙
NFT 2N (DLB 5)	iPoll lenta	192.168.100.32	00:19:3B:03:4D:2B	--	124 (5620 MHz)	🗑

Figure 68 – Master AP: table of Managed APs

There is possibility to change some parameters for each Managed AP individually. Just click on the configuration icon ⚙ to load individual settings:



MANAGED AP 10.0.10.18 (NFT 3) SETTINGS

Friendly name: NFT 3

Location: 610

2.4 GHz Channel: Auto / 40 MHz (Upper)

5 GHz Channel: Auto / 80 MHz

2.4 GHz Tx power, dBm: 15

5 GHz Tx power, dBm: 25

LED status: ☑

Flash all LEDs, min: Start 5

Product name: NFT 3AC

Firmware version: AP.QA-4.v7.54.24579 (Update)

MAC address: 00:19:3B:09:23:0A

Connected clients: 1

Troubleshooting file: Download
Backup configuration: Backup
Restore configuration: Restore
Reset to factory defaults: Reset
Done
Cancel

Figure 69 - Managed AP Settings

Friendly name – a friendly name for identification.

Location – describe physical location of the unit.

Channel – indicates which channel the AP is operating on or that an autochannel function is used. Click on the button for channel configuration.

Tx power, dBm – control unit’s radio transmitting power.

LED status – enable or disable all LEDs. If disabled, no LEDs will light up on the unit.

Flash LEDs – use this function for particular unit identification. Once enabled, all LEDs of the unit will flash for 5 minutes (changeable parameter) thus helping identify the location of the unit in the area.

Connected clients – displays the number of connected client to this particular Managed AP.

Troubleshooting file – generate and download a troubleshoot file with device's status information which may help in resolving support issues.

Backup configuration – click to download current configuration file. The 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.

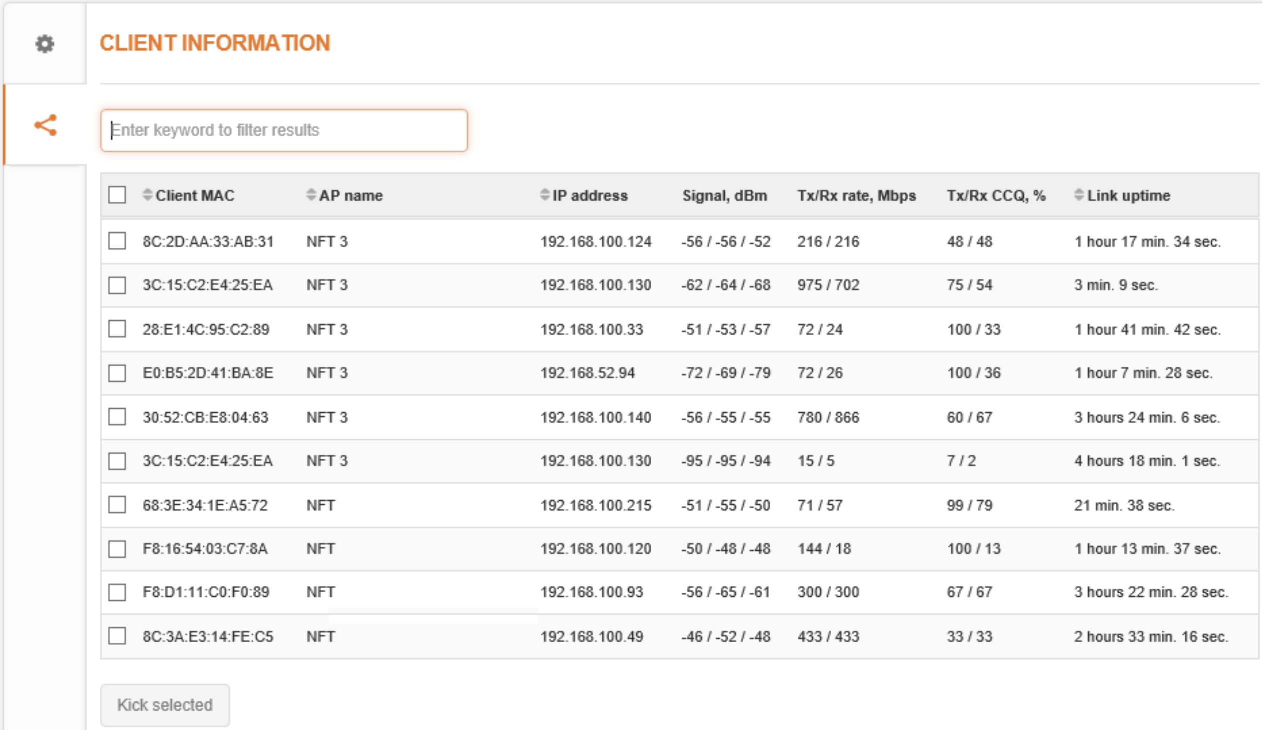
Restore configuration – click to upload an existing configuration file to the device.

Reset 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 settings subsequently changed on Master AP will be automatically uploaded on all Managed APs on this Infinity Controller's network.

Use **Controller | Client Information** menu to view wireless clients connected to each Master AP and Managed APs:



CLIENT INFORMATION

Enter keyword to filter results

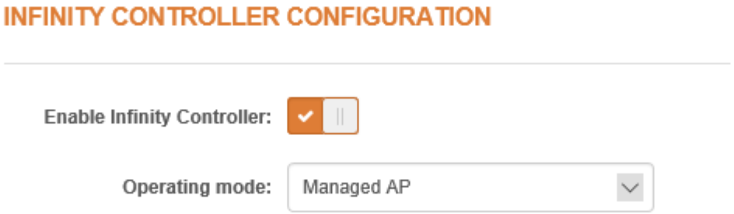
□	Client MAC	AP name	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Link uptime
□	8C:2D:AA:33:AB:31	NFT 3	192.168.100.124	-56 / -56 / -52	216 / 216	48 / 48	1 hour 17 min. 34 sec.
□	3C:15:C2:E4:25:EA	NFT 3	192.168.100.130	-62 / -64 / -68	975 / 702	75 / 54	3 min. 9 sec.
□	28:E1:4C:95:C2:89	NFT 3	192.168.100.33	-51 / -53 / -57	72 / 24	100 / 33	1 hour 41 min. 42 sec.
□	E0:B5:2D:41:BA:8E	NFT 3	192.168.52.94	-72 / -69 / -79	72 / 26	100 / 36	1 hour 7 min. 28 sec.
□	30:52:CB:E8:04:63	NFT 3	192.168.100.140	-56 / -55 / -55	780 / 866	60 / 67	3 hours 24 min. 6 sec.
□	3C:15:C2:E4:25:EA	NFT 3	192.168.100.130	-95 / -95 / -94	15 / 5	7 / 2	4 hours 18 min. 1 sec.
□	68:3E:34:1E:A5:72	NFT	192.168.100.215	-51 / -55 / -50	71 / 57	99 / 79	21 min. 38 sec.
□	F8:16:54:03:C7:8A	NFT	192.168.100.120	-50 / -48 / -48	144 / 18	100 / 13	1 hour 13 min. 37 sec.
□	F8:D1:11:C0:F0:89	NFT	192.168.100.93	-56 / -65 / -61	300 / 300	67 / 67	3 hours 22 min. 28 sec.
□	8C:3A:E3:14:FE:C5	NFT	192.168.100.49	-46 / -52 / -48	433 / 433	33 / 33	2 hours 33 min. 16 sec.

Figure 70 - Wireless Clients' Table

Integrated Infinity Controller: Managed AP

While device is operating in the **Managed AP** mode, all settings will be overwritten by the Master AP device.

Choose the **Managed AP** in order to change LigoNFT device operating mode:



INFINITY CONTROLLER CONFIGURATION

Enable Infinity Controller: ✓

Operating mode: Managed AP

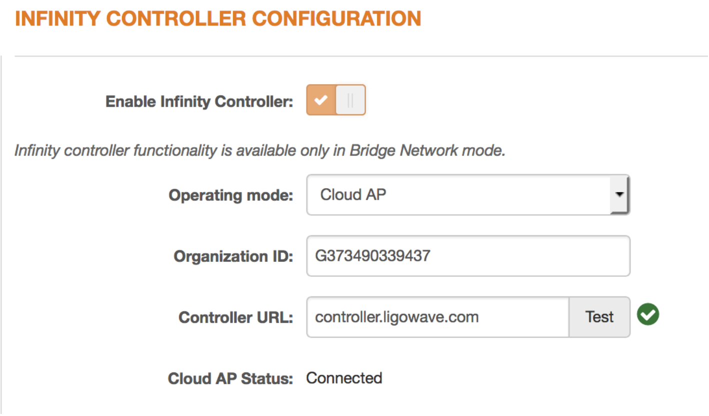
Figure 71 - Integrated Infinity Controller: Managed AP mode

In this operating mode LigoNFT unit will wait for automatic configuration upload from the Master AP running on this network. No further configuration is needed from the Managed AP side.

External Infinity Controller: Cloud AP

While device is operating in Cloud AP mode, all settings will be overwritten by the External Infinity Controller's management system.

Choose the **Cloud AP** in order to change LigoNFT device operating mode. Once this Cloud AP device is connected to the network, it will download the network specific configuration from an External Infinity Controller.



INFINITY CONTROLLER CONFIGURATION

Enable Infinity Controller: ✓

Infinity controller functionality is available only in Bridge Network mode.

Operating mode: Cloud AP

Organization ID: G373490339437

Controller URL: controller.ligowave.com Test ✓

Cloud AP Status: Connected

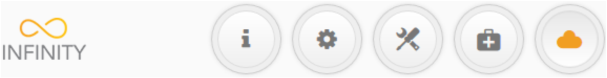
Figure 72 - External Infinity Controller: Cloud AP mode

Organization ID – enter the Organization ID, provided by the External Infinity Controller.

Controller URL – Specify the correct External Infinity Controller's URL where the Cloud AP will be registered and managed. Use **Test** button in order to check the controller's URL availability.

Ensure that External Infinity Controller is accessible to this LigoNFT device.

After the Cloud AP access the External Infinity Controller, the Controller menu icon will change, thus identifying the Cloud AP mode:



Index