



# **NIO200 HAG - WirelessHART All-in-One Gateway – User Guide**

**Version: 1.2**

*Date: March 17, 2017*

# Table of Contents

---

<b>1</b>	<b>General Information.....</b>	<b>6</b>
1.1	Document Purpose .....	6
1.2	Definitions, Acronyms and Abbreviations .....	6
<b>2</b>	<b>Product Overview .....</b>	<b>7</b>
2.1	About the NIO200 HAG Gateway .....	7
2.2	Logical Interfaces.....	7
<b>3</b>	<b>Hardware Installation .....</b>	<b>8</b>
3.1	Power-up NIO200HAG.....	8
3.2	Connect Wi-Fi Antennas.....	8
<b>4</b>	<b>Getting Started.....</b>	<b>9</b>
4.1	NIO200HAG Gateway .....	9
4.2	Connecting to the NIO200HAG Gateway.....	9
4.3	Accessing NIO200 Admin website.....	9
4.4	Configuring the IP Address.....	10
4.5	Configuring the NTP settings.....	11
4.6	Monitoring Control System .....	11
<b>5</b>	<b>Home page .....</b>	<b>13</b>
<b>6</b>	<b>Administration for the Network Devices .....</b>	<b>14</b>
6.1	Dashboard .....	15
6.2	Topology .....	17
6.3	Devices.....	21
6.4	Device Details.....	24
6.5	Network Health .....	35
6.6	Readings .....	37
6.7	Commands Log .....	38
6.8	Alerts .....	41

<b>7</b>	<b>Configuration</b> .....	<b>43</b>
<b>7.1</b>	<b>Access Point</b> .....	<b>43</b>
<b>7.2</b>	<b>Gateway</b> .....	<b>45</b>
<b>7.3</b>	<b>Network Manager</b> .....	<b>46</b>
<b>7.4</b>	<b>Device Management</b> .....	<b>48</b>
7.4.1.	Configuring Access Point .....	49
7.4.2.	Configuring Gateways .....	50
7.4.3.	Configuring Devices .....	50
<b>7.5</b>	<b>Monitoring Host</b> .....	<b>52</b>
7.6.1.	<i>Burst Messages</i> .....	52
7.6.2.	<i>Variables</i> .....	53
7.6.3.	<i>Triggers</i> .....	55
<b>7.6</b>	<b>MODBUS</b> .....	<b>56</b>
7.6.1.	<i>Mapping Registers</i> .....	57
<b>7.7</b>	<b>Advanced Settings</b> .....	<b>60</b>
7.6.2.	Edit Configuration Variables.....	60
7.6.3.	Restart .....	62
7.6.4.	Access NEXCOM NIO200 admin website .....	62
<b>8</b>	<b>System Status</b> .....	<b>63</b>
<b>9</b>	<b>Administration</b> .....	<b>65</b>
<b>9.1</b>	<b>System Upgrade</b> .....	<b>65</b>
<b>9.2</b>	<b>Custom Icons</b> .....	<b>66</b>
<b>9.3</b>	<b>Custom Settings</b> .....	<b>67</b>
<b>9.4</b>	<b>Device Codes</b> .....	<b>68</b>
9.4.1	<i>Adding a Device Code</i> .....	69
9.4.2	<i>Editing a Device Code</i> .....	69
9.4.3	<i>Deleting a Device Code</i> .....	70
<b>10</b>	<b>Session</b> .....	<b>71</b>
<b>10.1</b>	<b>Change Password</b> .....	<b>71</b>

## [Appendix Index](#)

1.	Login .....	<b>73</b>
2.	Status .....	<b>75</b>
2.1	Overview .....	75
	System .....	75
	Memory .....	76
	Network .....	76
	DHCP Leases .....	77
	DHCPv6 Leases .....	77
	Wireless .....	77
	Associated Stations .....	78
2.2	Firewall .....	79
2.3	Routes .....	79
	ARP .....	79
	Active IPv4-Routes .....	79
	Active IPv6-Routes .....	80
	IPv6 Neighbors .....	80
2.4	System Log .....	81
2.5	Kernel Log .....	81
2.6	Processes .....	82
2.7	Real-time Graphic .....	82
	Load .....	83
	Traffic .....	83
	Wireless .....	84
	Connections .....	86
3.	System .....	<b>87</b>
3.1	System .....	87
	General Settings .....	87
	Logging .....	88
	Language and Style .....	88
3.2	Administration .....	90
	Router Password .....	90
	SSH Access .....	90

3.3	Backup/Flash Firmware.....	91
	Upgrade Firmware .....	91
	Backup Configuration .....	93
	Reset to default.....	93
3.4	Reboot.....	94
4	Network.....	<b>95</b>
4.1	Interfaces .....	95
4.2	Wi-Fi.....	101
	Associated Stations.....	102
	Wireless configuration .....	102
	Mesh Advanced .....	107
4.3	DHCP and DNS .....	109
	General Settings.....	111
	Resolve and Hosts Files.....	111
	TFTP Settings .....	112
4.4	Advanced Settings.....	113
4.5	Hostnames .....	114
4.6	Static Routes .....	115
4.7	Diagnostics.....	117
4.8	Firewall.....	118
	General Settings.....	118
	Port Forwards.....	119
	Traffic Rules.....	119
	Custom Rules .....	120

# 1 General Information

## 1.1 Document Purpose

The purpose of this document is to provide instructions for using WirelessHART Monitoring Control System (MCS) and to provide information about the NEXCOM NIO200HAG WirelessHART All-In-One Gateway as well as instructions on how to configure certain settings.

## 1.2 Definitions, Acronyms and Abbreviations

The following table lists definitions, acronyms, and abbreviations that are only suitable to this document.

Term	Description
AP	Access Point
CSV	Comma Separated Values: A method to store data that is separated by “comma” so that it can be easily read and processed by Win32 and Unix programs
GW	Gateway
Hop	A hop describes the data being passed from one device to another as a means to lengthen the transmit distance
MCS	Monitoring Control System
NM	Network Manager
NIO200HAG	NIO 200HAG – NEXCOM WirelessHART All-in-One Gateway

## 2 Product Overview

### 2.1 About the NIO200 HAG Gateway

The NIO200HAG Gateway is industrial wireless-enabled computer designed to enable customers to deliver market leading wireless solutions. The WirelessHART Monitoring Control System is a web application that runs on NIO200 HAG Gateway enables users to remotely view and configure their WirelessHART network. The MCS runs on the NIO200HAG and gives users with proper rights control over the network, including the means to monitor the topology, set up data transmissions, and control the processes that take place in the network.

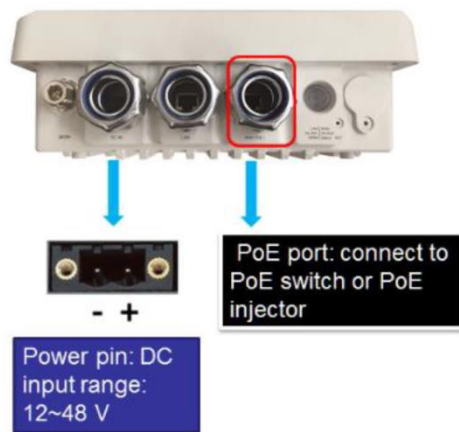
### 2.2 Logical Interfaces

Interface	Description
<b>Serial Port</b>	The serial port is used as a kernel console and emergency backup.
<b>TCP</b>	The NIO200HAG Gateway accepts the following TCP connections. <ul style="list-style-type: none"><li>➤ The NIO200HAG Gateway has an http server listening on port 80.</li><li>➤ The NIO200HAG Gateway has an http server listening on port 8080.</li><li>➤ The NIO200HAG Gateway has an https server listening on port 443.</li><li>➤ The MODBUS TCP server is listening on TCP port 502.</li></ul>
<b>UDP</b>	The NIO200HAG Gateway utilizes the NTP protocol to synchronize time with Internet time servers. The UDP port 123 must be open in both directions to allow time synchronization.

**NOTE:** Not all interfaces are guaranteed to be up in all cases. Some might be disabled for specific applications.

# 3 Hardware Installation

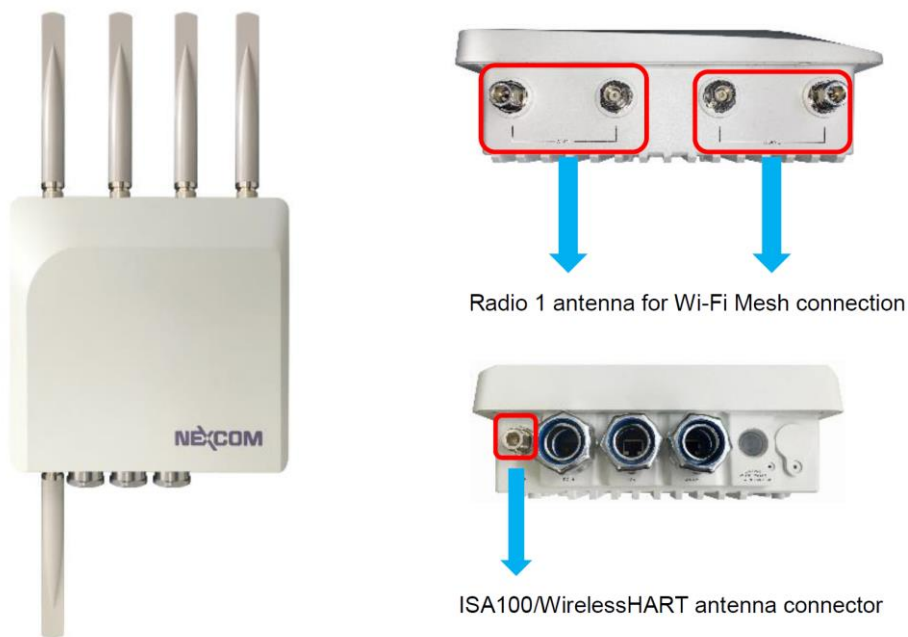
## 3.1 Power-up NIO200HAG



- Prepare DC power source ( 12~48 VDC ) or standard PoE facility such PoE switch or PoE injector.
- If use external DC power source, please carefully check if the polarity of power cord fits the polarity drawing in this diagram.
- When use PoE power source, just plug in the Ethernet cable

If the power connects correctly, then the “Power LED” will lit accordingly.

## 3.2 Connect Wi-Fi Antennas





## 4 Getting Started

### 4.1 NIO200HAG Gateway

The web-based administration is the **preferred** method to administer/configure the NIO200HAG Gateway. It requires a web browser and the IP of the NIO200HAG Gateway. The NIO200HAG Gateway must be connected to the local LAN then powered on, and the IP/mask or the router must be accessible from the PC where the browser is running.

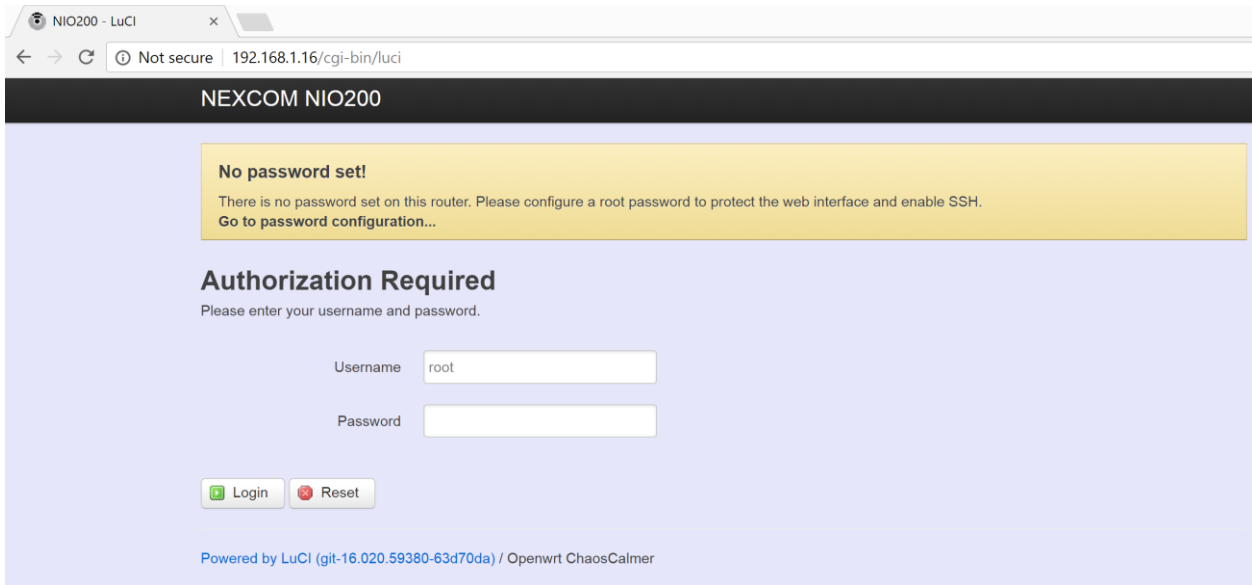
### 4.2 Connecting to the NIO200HAG Gateway

The NIO200HAG is pre-configured a static IP address **192.168.1.1** for connection directly to a computer. In order to communicate with the NIO200HAG, the user must temporarily set the computer IP address to a static address (**192.168.1.100** for example) and may use an Ethernet cross-over cable to connect the NIO200HAG to the computer.

### 4.3 Accessing NIO200 Admin website

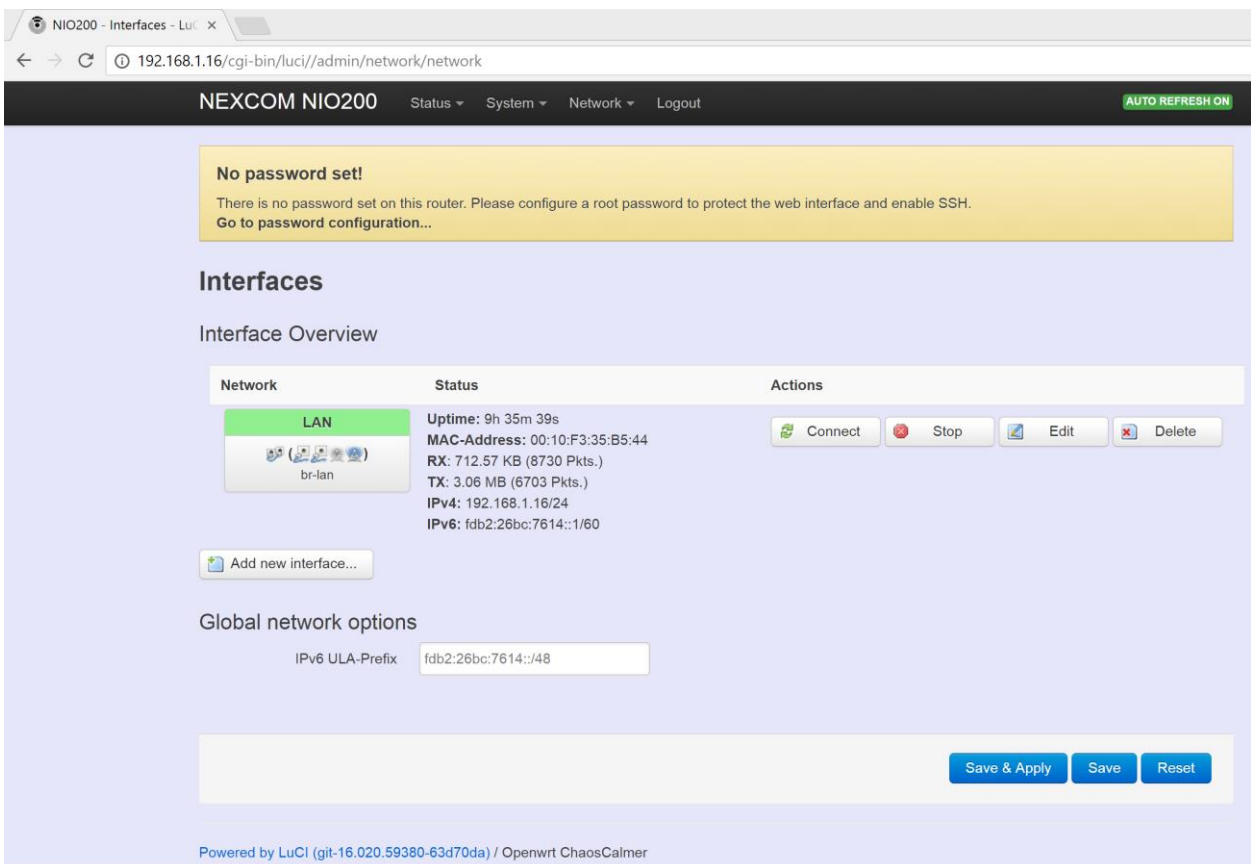
Once the communication has been established with the NIO200HAG, the user can log in the NIO200 Admin website to change the network configuration, including its IP address. To the access this website:

- In browser, open a connection to <http://192.168.1.1/> (or the user defined IP Address)
- Admin website requires authentication, the default *username* and *password* are *root* and *admin*.



## 4.4 Configuring the IP Address

The IP Address can be changed in Network>Interfaces page. The user must click “Save” or “Click Save and Apply” when done.



## 4.5 Configuring the NTP settings

The NTP Settings can be changed in System page. The user must click “Save” or “Click Save and Apply” when done. *It is strongly recommended to have access to the Internet in order to allow the NTP client configured on the HAG to synchronize with external time servers present online.* WIRELESSHART mandates the existence of a master source clock exists in each network. In this implementation this role is fulfilled by the Network Manager through the NTP application running on the device.

## 4.6 Monitoring Control System

WIRELESSHART specific network management and configuration takes place into the Monitoring Control System (MCS). Steps to access the MCS:

Step	Action
1.	Open the following URL: <a href="http://&lt;NIO200HAG_IP&gt;:8080/">http://&lt;NIO200HAG_IP&gt;:8080/</a> replacing <NIO200HAG_IP> with NIO 200HAG Gateway IP. Once the address is accessed, the login screen appears, as shown in the Figure 4.
2.	Type the following user name and password in the <b>Login</b> fields: <ul style="list-style-type: none"><li>➤ Username: the username provided.</li><li>➤ Password: use the password provided.</li></ul> Note: the default <i>username</i> and <i>password</i> are <i>admin</i> and <i>adminadmin</i> .
3.	Click the <b>Login</b> button.

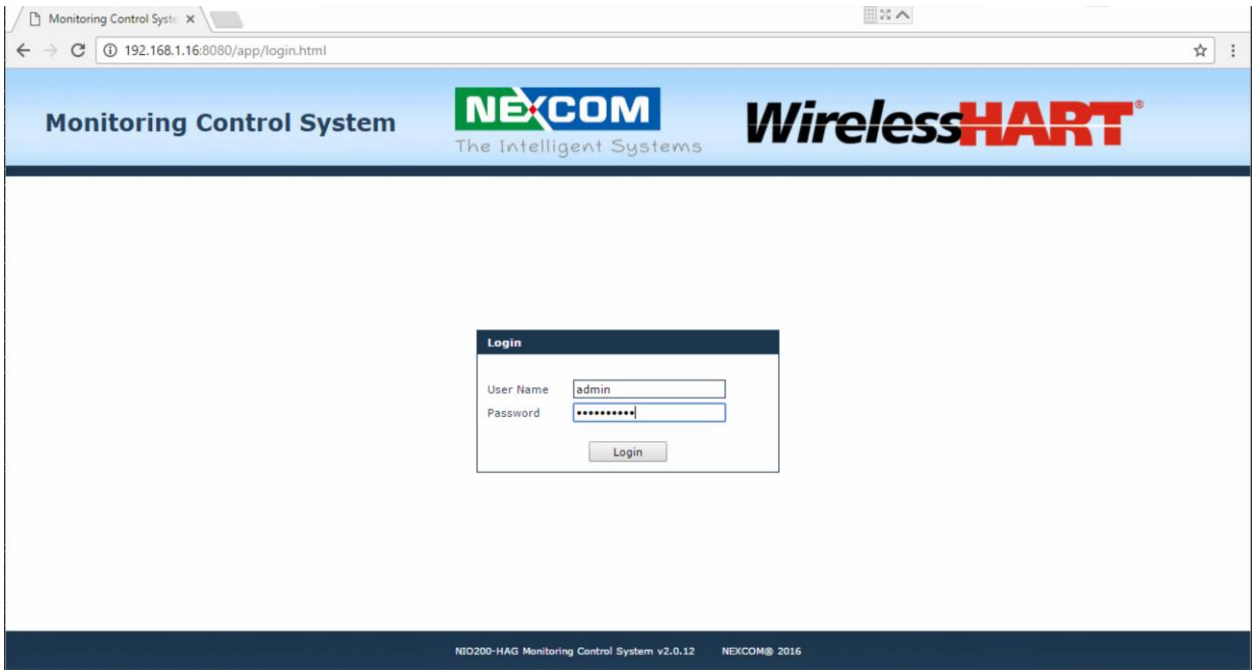


Figure 1

## 5 Home page

Once the credentials are entered and access is granted, the browser will display the Device List by default.

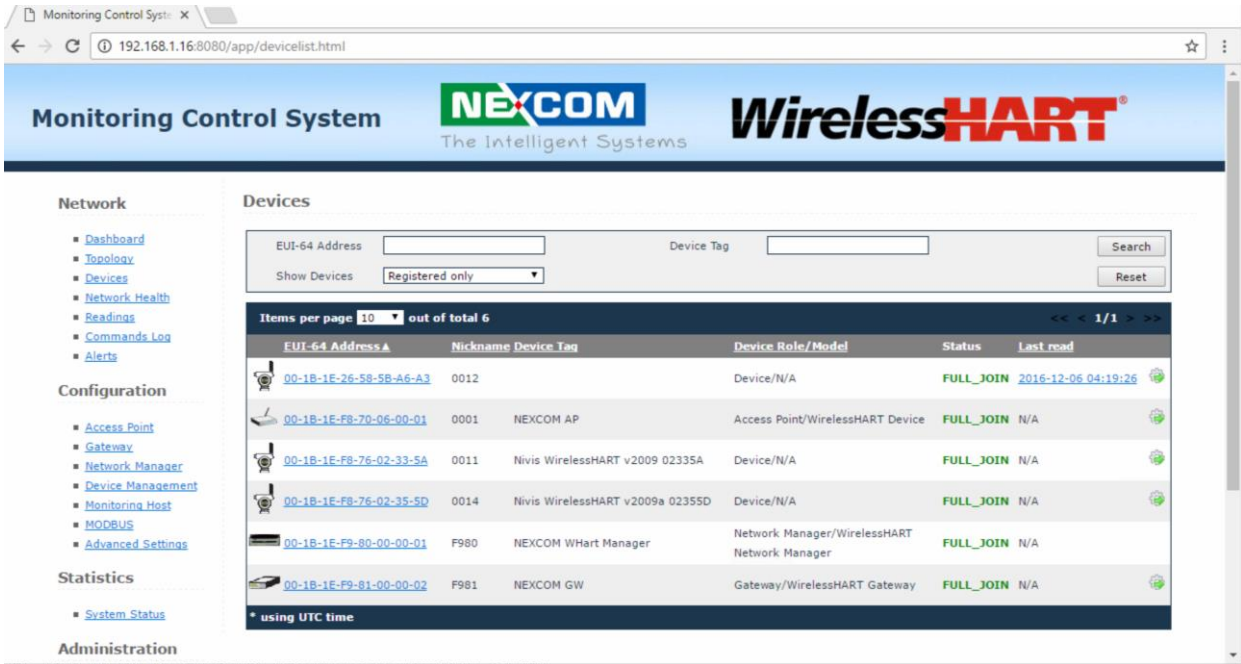


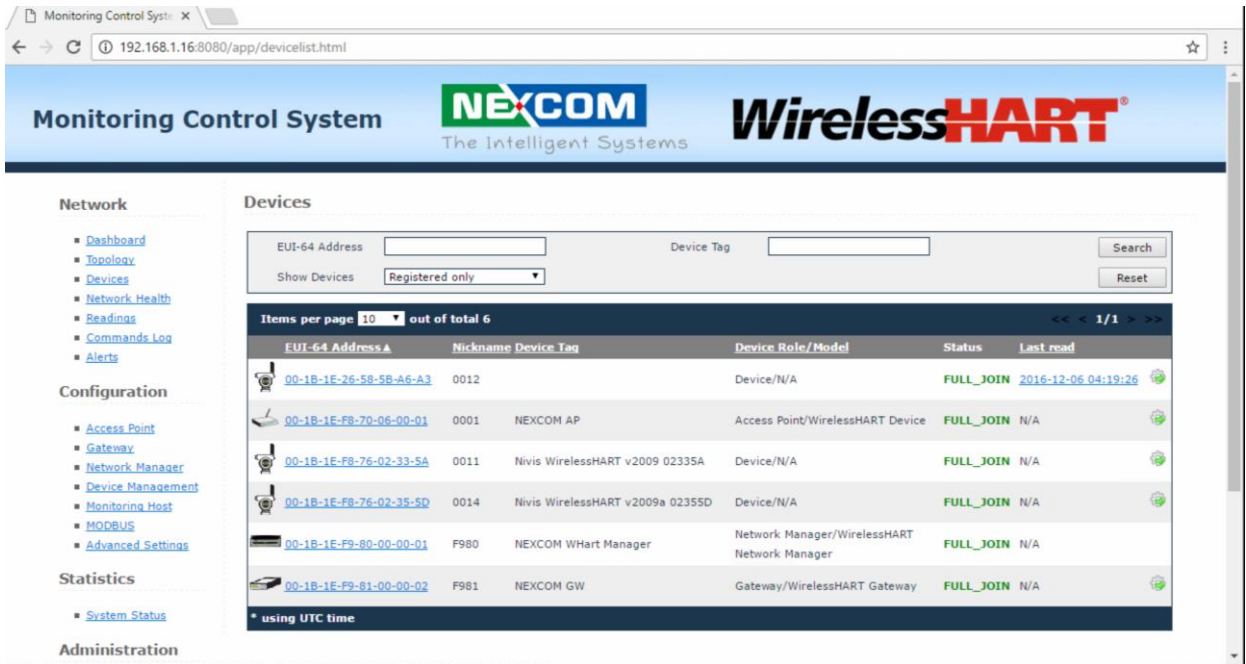
Figure 2

The user interface consists of two sections:

- The menus on the left, which allow you to navigate through the pages of the website
- The main section, which displays the contents of the selected page

# 6 Administration for the Network Devices

The Network section provides information about various network tasks accessed from the Monitoring Control System Webpage.



## 6.1 Dashboard

The **Dashboard** page is a report zone that allows you to monitor reading variations for selected devices. The Dashboard consists in a series of panes added by the user, which provide a visual representation of the information published by selected devices on selected channels.

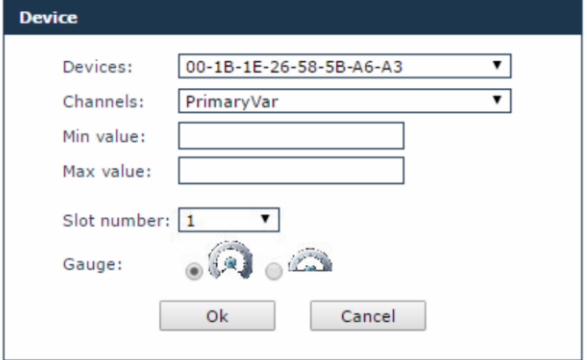
The information is refreshed automatically at regular intervals (10 seconds, 30 seconds, or 1 minute).




To delete a device from the dashboard, click  in the top right corner of the pane. No confirmation is required for the system to delete the pane.

To add a device to the dashboard, perform the following steps:

Step	Action
1.	Click on the <b>Add Device</b> button.

Step	Action
2.	<p>The <b>Device</b> dialog box will open:</p> <div data-bbox="571 376 1161 792" style="text-align: center;"> <p><b>Add device to dashboard</b></p>  </div> <p>Select a <b>Device</b> from the drop-down list.</p>
3.	Select the <b>Channel</b> that you wish to monitor from the drop-down list.
4.	Type the desired gauge value range for the readings; if the selected values are out of range, a message on the pane will notify you.
5.	Optional, select the <b>Slot number</b> (up to the current slot number); if you do not select a slot number, the system automatically assigns the next available slot.
6.	Select the desired <b>Gauge</b> type.
7.	Click <b>OK</b> to add the device to the dashboard.

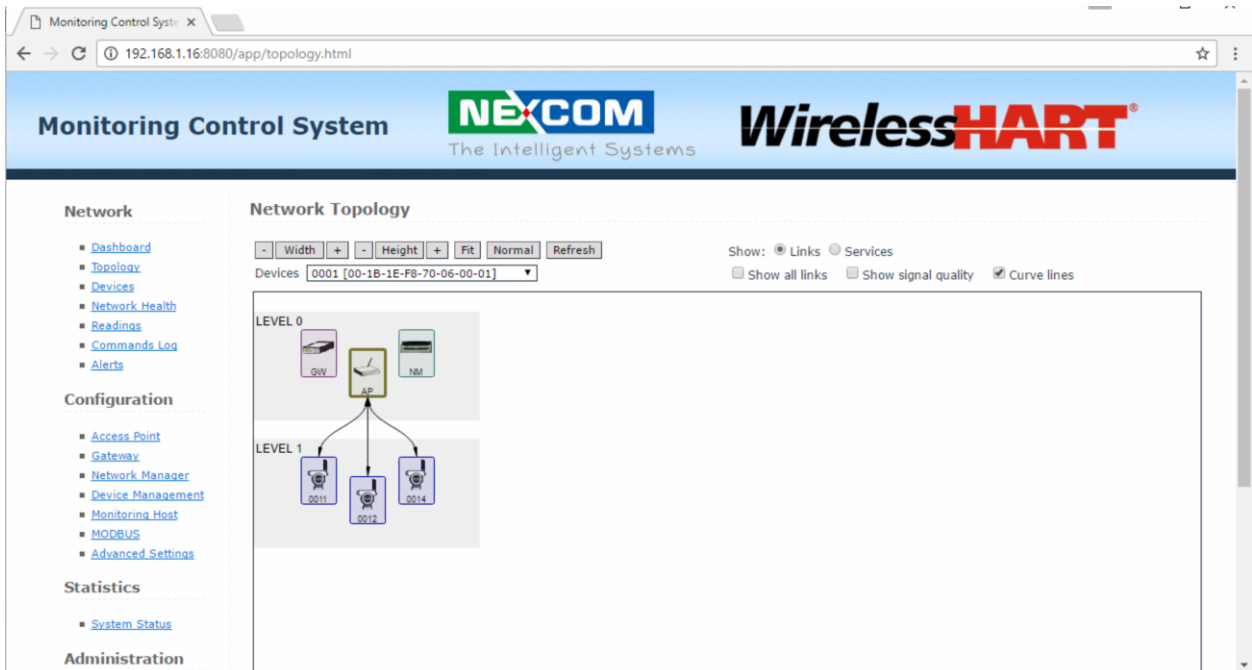
**NOTE:**

- You can also add a reading to the dashboard from the Device Details page: in the Information pane, click the **Add to dashboard (ATD)** icon  next to a reading.
- Up to 9 devices are supported in the dashboard.



## 6.2 Topology

The **Topology** page displays a graphical representation of the current network topology as well as allows users to view data about contracts and devices.



When you load the page, the topology graph is generated based on the latest topology information available. The system continuously updates this information in the background based on notifications sent by the Network Manager on network topology changes (device registering/leaving the network). The time of the last topology information update is indicated at the top of the page. To view the latest topology, press *Refresh*.

The **registered** devices are displayed on multiple levels represented as grey bands. The levels are numbered from 0 to  $n$ , where  $n$  is a natural number. The level number is indicated in the upper left corner of a level. The Gateway, the Network Manager, and the Access Point are found on level 0. For the field devices, the level represents the number of hops from device to Access Point on the clock source graph. A **hop** is a term used to describe the data being passed from one device to another as a means to lengthen the transmit distance.

Communication-wise, field devices are linked directly or via other devices to the Access Point, which is the central device in the RF network. The Access Point further relays to the Gateway, while the

Network Manager organizes the entire network. The field devices can have various sensors attached: temperature sensors, humidity sensors, etc.

The devices are identified in the topology by the last four characters of their EUI-64 address. For easier identification, the Access Point, the Gateway, and the Network Manager are identified with the abbreviations AP, GW, and NM. The devices are placed within a level in the order of their EUI64 address. They can be moved freely within the range of their level by *drag-and-drop* to obtain better legibility of the topology.

In addition, they are represented by suggestive icons and against backgrounds of different colors, to distinguish their roles:



- Gateway – purple background
- Access Point – light green
- Network Manager – dark green
- Field devices - blue


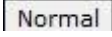
By positioning the cursor over an icon, you can view the tooltip, which includes the following details for a device:

- the EUI-64 address,
- the device role,
- the device tag,
- the manufacturer,
- the model.

The available Topology page elements and viewing options are described in the following paragraphs.

### Adjusting Width and Height

You can adjust the size of the topology representation using the buttons  and  for height and weight.

You can also adjust the height and weight to the size of the Topology pane by clicking , or revert to the original viewing settings by clicking .

## Links

To show the links between devices, check the “Links” option located above the topology graph (This option is checked by default when the page is loaded).

When the page is loaded for the first time, the Access Point is selected and its links to the devices and to the Gateway are shown as black lines.

1. To show the links for a particular device, click on that device in the topology graph, or select the device in the drop-down list located on top of the Topology pane.
2. To view all the other links formed between the network devices, check the *Show all links* option. This option is unchecked by default.
3. To view the RSQI signal values next to each link, check the *Show signal quality* option. For more information about the signal see section Settings.

## Services

To view the services for a selected device:

1. Check the “Services” option located at the top of the topology graph,
2. Choose a device by clicking on it in the topology graph or by selecting it in the Devices drop - down list located above the graph,
3. In the Services drop-down list you will view the selected device’s inbound and outbound services with the Network Manager and the Gateway.
- 4.

- a. To view all the inbound services for the selected device, click *Inbound* in the drop-down list.
- b. To view all the outbound services for the selected device on the graph, click *Outbound* in the drop-down list.
- c. To view a single service, select it in the list. There are four types of services, which are represented by differently colored lines:
  - Blue – for publish services
  - Red – for event services
  - Green – for maintenance services
  - Black – for block transfer services

The Services legend located in the lower right corner of the Topology page also indicates how the types of services and links are represented.

**Note:** A device can have multiple services with the same NM or GW at the same time.

### Network Topology

- Width +
- Height +
Fit
Normal
Refresh

Show:  Links  Services
 0: 00-1B-1E-26-5B-A6-A3 -> GW

Devices: 0012 [00-1B-1E-26-5B-A6-A3]

 Show all links
  Show signal quality
  Curve lines

LEVEL 0

LEVEL 1

**Service details:**

Service ID: 0,  
 Application Domain: Publish, 00-1B-1E-26-5B-A6-A3 -> 00-1B-1E-F9-81-00-00-02,  
 SourceFlag :yes, SinkFlag :no, IntermittentFlag :no,  
 Period :256000, RouteID :1, Timestamp :2016-12-06 04:43:42

**Service legend:**

- Publish Service
- Event Service
- Maintenance Service
- BlockTransfer Service

### Service details

In addition, when you select a service, information about the service parameters will be shown in the Service details section at the bottom of the page.

The service information includes the following parameters:

- Service ID – the service identifier based on the service owner,
- Application domain – the type of service,
- Source/destination device – the EUI64 address of the source device, and the destination device respectively,
- SourceFlag – indicates if selected device is the source of the communication,
- SinkFlag - indicates if selected device is the destination of the communication. If both SourceFlag and SinkFlag are set, indicate a bidirectional communication between selected device and the destination of service,
- IntermittentFlag - indicates if the service is used for acyclic/intermit communication,
- Period – the frequency for generating packets for cyclic communication (burst messages),
- RouteID – the ID of the route assigned to the service (each service having one Route ID assigned by Network Manager),
- Timestamp – the time and date the service was created.













## 6.3 Devices

The devices page features the list of devices that exist in the network and a search form that enables you to search devices based on their EUI-64 address, tag and/or state.

## Devices

EUI-64 Address  Device Tag    
Show Devices

Items per page **10** out of total **6** << < 1/1 > >>

EUI-64 Address▲	Nickname	Device Tag	Device Role/Model	Status	Last read
 <a href="#">00-1B-1E-26-58-5B-A6-A3</a>	0012		Device/N/A	FULL_JOIN	<a href="#">2016-12-06 04:48:14</a> 
 <a href="#">00-1B-1E-F8-70-06-00-01</a>	0001	NEXCOM AP	Access Point/WirelessHART Device	FULL_JOIN	N/A 
 <a href="#">00-1B-1E-F8-76-02-33-5A</a>	0011	Nivis WirelessHART v2009 02335A	Device/N/A	FULL_JOIN	N/A 
 <a href="#">00-1B-1E-F8-76-02-35-5D</a>	0014	Nivis WirelessHART v2009a 02355D	Device/N/A	FULL_JOIN	N/A 
 <a href="#">00-1B-1E-F9-80-00-00-01</a>	F980	NEXCOM WHart Manager	Network Manager/WirelessHART Network Manager	FULL_JOIN	N/A 
 <a href="#">00-1B-1E-F9-81-00-00-02</a>	F981	NEXCOM GW	Gateway/WirelessHART Gateway	FULL_JOIN	N/A 

\* using UTC time

### 6.3.1. Search devices

When the device page is loaded, the registered devices are displayed by default.

When the device page is loaded, the registered devices are displayed by default.

#### 1. Search by EUI-64 address

To search a device by its EUI-64 address, type the address in the EUI-64 Address input field and click *Search*.

For partial search:

- a. Type part of the EUI-64 address in the EUI-64 Address input field
- b. Select the desired state from the Show Devices drop -down list and click *Search*. The system will

retrieve all the devices whose EUI-64 addresses contain the characters provided by the user. To delete the search parameters, click *Reset*.

#### 2. Search by device tag:

A tag is a custom description that you can assign to a device in order to facilitate identification of that device in the plant. One tag can be assigned to a single device.

To search for devices based on their tag, type the tag in the Device Tag input field, and click *Search*.

*Note that the tag field is case sensitive.*

To delete the search parameters, click *Reset*.

### 3. Search by device state only:

To display devices based on their state at a given time, select the desired state from the Show Devices drop-down list. The device list will update automatically.

You can choose between two states:

- Registered – the device has successfully joined the network and is ready to operate,
- Unregistered – the device has lost connection with its neighbors in the network.

### 6.3.2. Device List

The **Device list** shows the network devices in a table, one item per line, with main information about each **logical** device:

- EUI-64 address (the MAC address),
- Nickname – the short address,
- Device tag,
- Device role (Gateway, Network Manager, Access Point, Field Router) and model (manufacturer information),
- Status (“Full Join” for registered devices; “Not Joined” for unregistered devices ), and
- Last Read (the date and time of the last reading from the device) and a link to the Readings page for the device in question.


In addition, the device list provides a quick link to the Run Commands page for that specific device.

When you load the page, the registered devices are displayed by default. In order to view unregistered devices, select “Unregistered only” in the Show Devices drop-down list.

The total number of rows in the table is indicated in the top left corner of the table . Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table .

### 6.3.3. Delete a device

In the devices page you have the option of deleting an unregistered device. When you delete a device, it will be removed from the network and any related data, including previous readings, will be deleted from the database.

To delete the device, click the icon  located next to the device. The system will require confirmation to perform the action. Click **OK** to delete the device or **Cancel** to abort the action.

## 6.4 Device Details

In this page you can see all the information available for the selected device and perform device-specific commands. The page is accessed by clicking on the device EUI-64 address in the device list.

The page is organized into several tabbed panes by types of information and also features a Back button to allow you to quickly revert to the Devices page.



## 6.4.1 Information

The Information pane displays general as well as activity specific information about the device. When the page is loaded, it shows the latest information available.

### Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Run Commands
EUI-64 Address:	00-1B-1E-26-58-5B-A6-A3			Manufacturer:	N/A
Nickname:	0012			Model:	N/A
Device Tag:				Revision:	2
Device Role:	Device			Generated:	135
Device Status:	FULL_JOIN			All Tx:	136
Last Read (UTC):	2016-12-06 04:56:46			No ACK:	6
Power Status:	0			Terminated:	37
				All Rx:	94
				DLL Failures:	0
				NL Failures:	0
				CRC Error:	2
				Nonce Lost:	1

Name	Burst Message	Device Variable Slot	Device Variable	Classification	Unit Code	Update Period	Max Update Period	ATD
PrimaryVar	0	0	246	0	32	8	3600	
SecondaryVar	1	0	247	183	98	16	60	
TertiaryVar	2	0	248	183	98	32	60	

The following details are shown in addition to those already indicated in the device list:

- Manufacturer – the name of the device manufacturer,
- Model – the model/type of the device,
- Revision – the radio firmware version,
- Power Status – not available in the current version,
- Data transmission statistics – the number of transmitted/received packages and the number of failed transmissions/receptions,
- Burst messages – the definition of burst messages that the device will publish to the Gateway.

### Burst messages

Burst messages are used to publish data to applications, in general to the Gateway, which is the entity providing access to the WirelessHART network and caching the data reported by devices.

The information about defined burst messages is displayed in a table with the following related information:

- Name – a user friendly name assigned to the published variable,
- Burst Message – the value can be between 0 and 2, indicating the number of burst message out of 3 burst messages currently supported by devices,
- Device Variable Slot – the value indicates the position of the variable in the burst packet,
- Device Variable – will have one of the values described in Common Table 34 Device Variable Code from HCF\_Spec-183 specification document,
- Classification – will have one of the values described in Common Table 21 Device Variable Classification Codes from HCF\_Spec-183 specification document,
- Unit Code – will have one of the values described in Common Table 2 Engineering Unit Codes from HCF\_Spec-183 specification document,
- Update Period – the value set through Command 103 at the configuration of burst message ,
- Max Update Period - the value set through Command 103.

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

#### **6.4.2 Settings**

The settings reflect the current operation of the WIRELESSHART stack on a device.

The type of information displayed in this pane includes neighbor details, routes and graph details:

## Device Details

Information	Settings	Registration Log	Neighbors Health	Schedule Report	Run Commands		
EUI-64 Address: 00-1B-1E-F8-70-00-04-10							
Nickname: 0410							
<b>Services</b>							
Service	Peer	Application Domain	Is Source	Is Sink	Is Intermittent	Period	Route
1	F981	Publish	Yes	No	No	128000	1
129	F981	Maintenance	Yes	Yes	No	128000	1
<b>Routes</b>							
Route	Peer	Graph	Is Source Path	Source Path			
0	F980	536	No	N/A			
1	F981	536	No	N/A			
<b>Graphs Neighbors</b>							
	Neighbor	Graph					
	0001	382					
	0001	536					
	0001	538					
	0505	536					
	0509	383					
	0508	539					

## Services

The Services section lists all the services for the selected device in a table, with the following information:

- Service – the service ID,
- Peer – the destination device for the selected device,
- Application Domain – the service type (publish; event; maintenance; block transfer),
- Is Source – indicates whether the selected device is the source of the communication ,
- Is Sink – indicates whether the selected device is the destination of the communication,
- Is Intermittent – indicates whether the communication on the service in question is intermittent or not,
- Period – the publishing period on the service in question,
- Route – indicates the ID of the route of which the selected device is the source.

## Routes

The Routes section lists the routes of which the source is the selected device.

Routes are of two types:

- Graph routes – they are based on graphs, and therefore are a directed list of redundant communication paths that connect network endpoints,
- Source routes – they are single directed routes between a source and a destination device. The source route is statically specified in the packet itself.

Routes are listed in a table displaying the following information:

- Route – route identification data; ID's are given in the order of creation of the routes. For every device, Route with ID 1 is the default route established between the field device and the Network Manager, and Route with ID 2 is the default route established between the field device and the Gateway,
- Peer – the destination device, which is either the Gateway or the Network Manager,
- Graph – the ID of the graph used by the route (only for graph routes) ,
- Is Source Path – indicates whether the route is a source route,
- Source Path – for a source route, it indicates the hops of the selected path (source device, intermediate device and destination device).

To view the updated device settings, click the *Refresh* button. The **Request Topology**, **Request Routes and Source Routes**, and **Request Services** commands will be sent to the Network Manager. To view the command status, go the Commands Log.

When the command is generated, a message at the top of the screen will indicate that the device information is refreshing.

## Graphs Neighbors

This section lists the graph-neighbor pairs for the selected device, in a table. For each graph to which the selected device belongs, the table provides the ID of the graph and the ID's of the device's neighbors on the same graph.

### 6.4.3 Registration Log

The registration log displays the registration history for the selected device, at different dates and times, commonly known as timestamps.

#### Device Details

Information Settings **Registration Log** Neighbors Health Schedule Report Run Commands

EUI-64 Address: 00-1B-1E-26-58-5B-A6-A3 Back

Nickname: 0012 Device Tag:

Registration Status: All Search

Start Time: 12/5/2016 10:54 PM End Time: AM Delete

Items per page 10 out of total 5 << < 1/1 > >>

Timestamp ▲	Device Status
2016-12-06 04:31:45	DELETED
2016-12-06 04:39:26	JOIN_REQ
2016-12-06 04:39:26	AUTHENTICATED
2016-12-06 04:39:26	NET_JOINED
2016-12-06 04:42:00	FULL_JOIN

\* using UTC time

Use the Search functionality to view the behavior of the device over a specific period time :

- Choose the status you wish to view from the Registration Status drop-down list,
- Optionally, fill in the Start time and the End time fields, and then click *Search*.

The results are displayed in a table that indicates the timestamp and the device status at that specific timestamp. A device can have one of the following statuses at a given moment:

- NOT\_JOINED – The device is not joined,
- JOIN\_REQ – The Network Manager received the join request from the device,
- JOIN\_FAILED – The device was removed by the Network Manager from the network due to a timeout,

- AUTHENTICATED – The Network Key and Network Manager Session were established,
- NET\_JOINED - Normal superframes and links were obtained,
- FULL\_JOIN – The device is joined and configured and all information about it is available .

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

### 6.4.4 Neighbors Health

This pane provides a communication health report about the selected device’s neighbors.

#### Device Details

Information Settings Registration Log **Neighbors Health** Schedule Report Run Commands

EUI-64 Address: 00-1B-1E-26-58-5B-A6-A3 Back

Nickname: 0012 Device Tag:

Neighbor  Search

Start Time: 12/5/2016 10:55 PM End Time:  :  AM

Items per page: 10 out of total 1 << < 1/1 > >>

Neighbor	Timestamp	Flags	Transmitted	Failed	Received	Signal Level
00-1B-1E-F8-70-06-00-01	2016-12-06 04:56:20	yes	136	6	94	Excellent (-56)

\* using UTC time

The report includes:

- Neighbor identification information - the EUI-64 address,
- The timestamp of the report request,
- Flags – this column indicates whether or not the neighbor is a clocksource for the selected device; the values for this column are “yes” and “no”,
- Communication health information:
  - The number of DPDUs transmitted to the neighbor and the number of failed transmission attempts,
  - the number of DPDUs received from the neighbor, and

- The signal level – the RSL of the neighbor, expressed in dBm.

The following table indicates the RSL thresholds and the associated labels:

RSL	Signal Level
-99 ... -85	Poor signal
-85 ... -73	Fair signal
-72 ... -60	Good signal
-59... -10	Excellent signal

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table .

#### 6.4.5 Schedule Report

The schedule report pane provides information about time slot and channel allocation for the selected device.

#### Superframes and links

The superframes that the device uses for communication are listed in the page along with the following information:

- Time slots – the size of the superframe, expressed in number of time slots,
- Is Active – indicates whether the superframe is currently active (is being used) or not ,

- Is handheld – indicates whether the superframe in question is used for communication between a handheld device and the selected device,
- Links – the number of links allocated on each superframe.

### Device Details

The screenshot shows the 'Device Details' page for EUI-64 Address: 00-1B-1E-26-58-5B-A6-A3. The 'Schedule Report' tab is selected. A table displays the following data:

Superframe ID	Time Slots	Is Active	Is Handheld	Links
7	1600	Yes	No	0
6	800	Yes	No	<a href="#">2</a>
5	400	Yes	No	<a href="#">2</a>
15	400	Yes	No	<a href="#">2</a>

Clicking on the number of links will display a new page with link related information for each individual link allocated on the selected Superframe, as shown in the following screen:

### Device Details

The screenshot shows the 'Device Details' page for EUI-64 Address: 00-1B-1E-26-58-5B-A6-A3, with the 'Schedule Report' tab selected. The 'Superframe ID: 6' is selected. A search bar shows 'Nickname: All' and 'Link type: All'. A table displays the following data:

Nickname	Slot Index	Channel Offset	Transmit	Receive	Shared	Link Type
0001	164	5	No	Yes	No	Normal
0011	166	14	Yes	No	No	Normal
0011	287	12	No	Yes	No	Normal
0001	289	5	Yes	No	No	Normal
0001	664	5	Yes	No	No	Normal
0001	764	5	No	Yes	No	Normal
0011	791	12	No	Yes	No	Normal

The following details are shown:

- Nickname of the neighbor – the short address of the neighbor or the broadcast address FFFF:FFFF:FFFF:FFFF (used only for advertisements and receive links),



- Slot index – the ID of the slot within the superframe,
- Channel offset – the channel offset in the superframe’s underlying hopping pattern,
- Direction – reception or transmission,
- Shared – indicates whether the channel is shared with other devices for communication purposes,
- Link type, which can be:
  - Normal,
  - Broadcast,
  - Join,
  - Discovery.

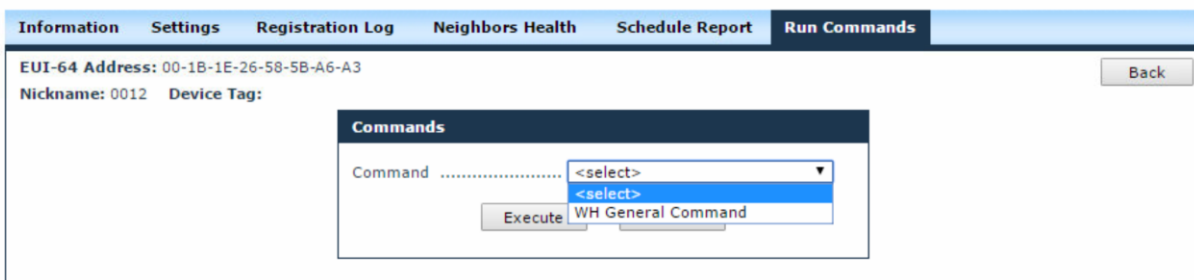
You can use the search form on the top of the page to sort links based on the nickname of the neighbor device and the link type.

In addition, in both the Superframes and Links tables you can view the information by the number of items listed per page. The default number is 10. Paging controls at the bottom of the table enable you to navigate through the pages of the table.

### 6.4.6 Run Commands

This pane enables you to perform device-specific commands.

#### Device Details



To go to a specific command, select it from the Commands drop-down list. After you generate the command, a message at the bottom of the screen will indicate its status (“Command sent successfully”, “Command sent error”). The tracking number of the command is also indicated, together with a link to the Commands Log, where you can view the results of the command.

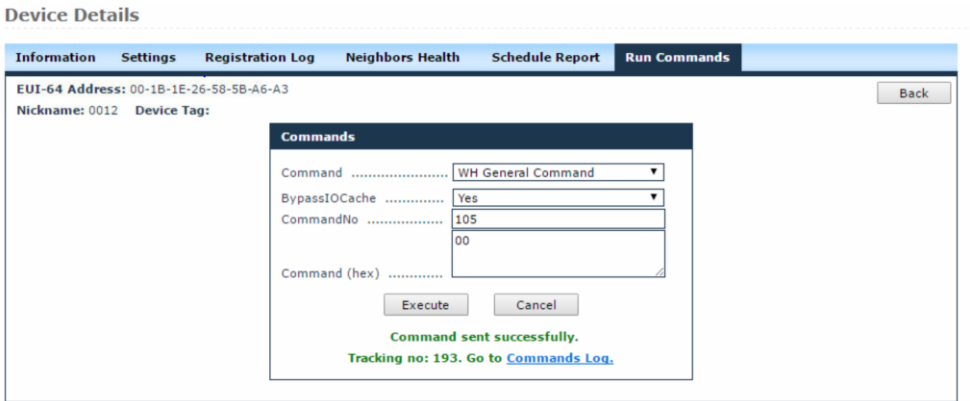
**Note:** Currently only the WirelessHART general command is supported. Other commands may be added in the future.

6.4.6.1 WH General Command

This set encompasses all the general commands that can be issued on the devices (e.g. 800 - read service list, 782 - read session list, etc.). To generate the command, follow the steps described below:

1. Select the WH General Commands set from the Command drop -down list;
2. Optionally, select the BypassIOCache value:
  - Yes – if you wish to retrieve the response to the command directly from the device ,
  - No – if you wish to obtain the response from the Gateway cache,
  - If you do not select a value, the default value “No” will be considered ,
3. Type the command number in the CommandNo field,
4. For commands that have parameters, type the content of the request in the Command (hex) field ,

Press *Execute*. A message at the bottom of the screen will indicate the command status (“Command sent successfully”, “Command sent error”). The tracking number of the command is also indicated, together with a link to Commands Log, where you can view the response.



6. Follow the Commands Log link to see the response of the command.

### Commands Log

Device	<input type="text" value="All"/>	Command Status	<input type="text" value="All"/>	<input type="button" value="Search"/>
Command	<input type="text" value="All"/>	<input type="checkbox"/>	Show system generated commands	<input type="button" value="Export"/>

Items per page <input type="text" value="10"/> out of total 1							<< < 1/1 > >>	
Tracking No.	EUI-64 Address	Command	Parameters	Status	Posted Time	Response Time	Response	
193	00-1B-1E-26-58-5B-A6-A3	WH General Command	<a href="#">CommandNo:105</a> , <a href="#">DataBuffer:00,...</a>	Responded	2016-12-06 05:04:35	2016-12-06 05:09:10	006900021FF6FAFAFAFAFAFA000300090003E8 0006DDD000004A5843060000	

\* using UTC time

## 6.5 Network Health

The Network Health page provides a communication health report at network level.

The page consists of two sections containing network summary statistics and device-specific communication health information.

### Network Health

<b>Devices Count:</b>	4	<b>Generated:</b>	19457	<b>DLL Failures:</b>	33
<b>Join Count:</b>	10	<b>All Tx:</b>	59508	<b>NL Failures:</b>	0
<b>Current Date (UTC):</b>	2016-12-02 04:07:36	<b>No ACK:</b>	2991	<b>CRC Error:</b>	513
<b>Start Date (UTC):</b>	2016-12-06 05:12:19	<b>Terminated:</b>	6980	<b>Nonce Lost:</b>	176
<b>All Rx:</b>	98375				

Show Devices

Items per page <input type="text" value="10"/> out of total 4												<< < 1/1 > >>	
EUI-64 Address	Join Count	Power Status	Generated	All Tx	No ACK	Terminated	All Rx	DLL Failure	NL Failure	CRC Error	Nonce Lost		
00-1B-1E-26-58-5B-A6-A3	7	0	155			40		0	0	1	0		
00-1B-1E-F8-70-06-00-01	1	0	6063			271		13	0	236	105		
00-1B-1E-F8-76-02-33-5A	1	0	12363			6003		10	0	225	35		
00-1B-1E-F8-76-02-35-5D	1	0	876			666		10	0	51	36		

\* using UTC time

In the network summary section the following information is indicated:

- Devices Count – the total number of registered devices, including the Access Point,
- Join count – the total number of joins of all the devices in the network,
- Start Date – the date and time the Network Manager application was started,
- Current Date – the present time,
- Transmission and reliability statistics, based on the summary report per device.

The device communication report section consists in a table displaying the following information for each device:

- EUI-64 Address – the network address of the device,
- Join Count – the total number of joins per device,
- Power Status – the battery status for the device in question; the power status can have one of the following values:
  - 0 –Nominal,
  - 1 – Low,
  - 2 – Critically low,
  - 3 – Recharging – Low
  - 4 – Recharging – High.

**Note:** *In version 1.x of the WirelessHART system, battery operation mode is not supported. All devices will report 0 - Nominal*

- Generated – the number of packets generated by the device,
- All Tx – all the packets transmitted but the selected device (including for routing purposes),
- No ACK – the number of packets that require acknowledgement and which were sent by the selected device but not acknowledged by the destination device,
- Terminated - the number of packets received by this device as a destination device,
- All Rx – all the packets received by the selected device (including for routing purposes),
- DLL Failure – the number of Data-Link Layer MIC (Message Integrity Check) failures detected,
- CRC Error – the number of CRC (cyclic redundancy check) errors detected,
- Nonce Lost – the number of Nonce Counter Values not received.

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table .

## 6.6 Readings

In this page you can view the readings received from the devices, which are generated either on demand by Read Value commands or by automatic burst messages. The readings can be filtered by device, variable name, command number or the device variable code.

### Readings

EUI-64 Address	<input type="text"/>	Command No	<input type="text"/>			<input type="button" value="Search"/>
Show Devices	<input type="text" value="Registered only"/>	Name	<input type="text"/>	Device Variable	<input type="text"/>	<input type="button" value="Export"/>

Items per page <input type="text" value="10"/> out of total 3							<< < 1/1 > >>		
EUI-64 Address	Timestamp	Name	Cmd No	Device Variable	Value	Unit Code	Update Period	Received	Missed
00-1B-1E-26-58-5B-A6-A3	2016-12-06 05:19:20	PrimaryVar	9	246	NaN	32	8	28	124
00-1B-1E-26-58-5B-A6-A3	2016-12-06 05:17:54	SecondaryVar	9	247	NaN	98	16	58	68
00-1B-1E-26-58-5B-A6-A3	2016-12-06 05:17:35	TertiaryVar	9	248	22.5	98	32	57	10

\* using UTC time

To search for readings, select a device or fill out the input fields as desired and click *Search*. The results are displayed in a table that contains the following information for each reading:

- Device EUI-64 address (MAC address of the device that reported the reading),
- Timestamp (date and time of the reading),
- Name (the variable name),
- Command No. (the number of the command triggering the reading),
- Device Variable (the variable code as per the WirelessHART specification),
- Value (the value received on that particular reading) – shown in engineering values,

- Classification (the type of variable, e.g. 64 - temperature); please consult the WirelessHART Common Table No. 21 for a comprehensive list of variables and associated classification codes ,
- Unit Code (the unit of measurement of the variable in question); please consult the WirelessHART Common Table No. 2 for a comprehensive list of unit codes and their descriptions,
- Update Period (the frequency configured for data publishing, in seconds),
- Last Update (the timestamp of the last value received in GW),
- Received (the number of packets received by the particular device),
- Missed (the number of packets that did not reach the particular device).

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table .

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking *Export*.

## 6.7 Commands Log

In this page you can view all the commands issued on the registered devices in the system. The commands can be filtered by Device, Command (type), or Command Status (New – command posted in database, Sent – command sent to device, Responded – device responded successfully to the command, Failed – command failed to execute).

To search for commands, select the desired device, command, and command status and click *Search*. The results will be displayed in a table, as shown in the screen above, with the following information for each command:

- Tracking Number (internal ID of the command),
- EUI-64 address (MAC address of the command destination device),
- Command (name of the executed command),

- Parameters (description of the parameters chosen for the command, if applicable),
- Status (current status of the command),
- Posted Time (date and time when the command was generated),
- Response Time (date and time when the command was responded), and

Response (the response for the issued command if the command was responded successfully or the error reason if the command failed), which can consist of:

- System generated commands:
  - 'success' or the hex value representing the response payload (if any), in case of success;
  - Error code and reason in case of command failure;
- WH General Command:
  - two bytes representing the command code, followed by one byte representing the command return code, followed by a hex value representing the response payload (if any).

### Commands Log

Tracking No.	EUI-64 Address	Command	Parameters	Status	Posted Time	Response Time	Response
193	00-1B-1E-26-58-5B-A6-A3	WH General Command	<a href="#">CommandNo:105</a> , <a href="#">DataBuffer:00,...</a>	Responded	2016-12-06 05:04:35	2016-12-06 05:09:10	006900021FF6FAFAFAFAFAFAFA000300090003E80006DDD000004A5843060000
192	00-1B-1E-26-58-5B-A6-A3	Auto Detect Burst Configuration		Responded	2016-12-06 04:42:05	2016-12-06 04:43:06	success
191	00-1B-1E-26-58-5B-A6-A3	Subscribe for Burst Notifications		Responded	2016-12-06 04:42:05	2016-12-06 04:42:05	success
190	00-1B-1E-26-58-5B-A6-A3	Auto Detect Burst Configuration		Responded	2016-12-06 03:05:31	2016-12-06 03:06:50	success
189	00-1B-1E-26-58-5B-A6-A3	Subscribe for Burst Notifications		Responded	2016-12-06 03:05:31	2016-12-06 03:05:31	success
188	00-1B-1E-26-58-5B-A6-A3	Auto Detect Burst Configuration		Responded	2016-12-06 02:14:19	2016-12-06 02:15:21	success
187	00-1B-1E-26-58-5B-A6-A3	Subscribe for Burst Notifications		Responded	2016-12-06 02:14:19	2016-12-06 02:14:19	success
186	00-1B-1E-26-58-5B-A6-A3	Auto Detect Burst Configuration		Responded	2016-12-06 00:42:25	2016-12-06 00:43:21	success
185	00-1B-1E-26-58-5B-A6-A3	Subscribe for Burst Notifications		Responded	2016-12-06 00:42:25	2016-12-06 00:42:25	success

Given the large number of commands generated automatically by the system at regular intervals, these commands are hidden by default. To view them, check the Show system generated commands option in the Search dialog and click Search.

The total number of rows in the table is indicated in the top left corner of the table. Here you can set the number of items to be displayed per page in the table. The default number is 10. Paging controls in the top right corner of the table also enable you to navigate through the other pages of the table.

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking Export.



## 6.8 Alerts

The Alerts page enables you to view alarms and events generated by devices.

Alerts consist in application messages that advise or warn the recipient of the presence of an impending or existing situation of interest.

### Alerts

The screenshot shows the Alerts page interface. At the top, there are search filters: Device Tag, EUI-64 Address, Alert Type (set to Path Down), Start Time (12/5/2016 5:25 AM), and End Time. There are Search and Export buttons. Below the filters, it shows 'Items per page 10 out of total 3' and navigation arrows. The main table has the following data:

Device Tag	Nickname	EUI-64 Address	Alert Time	Alert Type	PeerAddress/GraphID	MIC
Nivis WirelessHART v2009a 02355D	0014	00-1B-1E-F8-76-02-35-5D	2016-12-06 05:19:11	Path Down	00-1B-1E-F8-76-02-33-5A	1
Nivis WirelessHART v2009 02335A	0011	00-1B-1E-F8-76-02-33-5A	2016-12-06 01:49:34	Path Down	00-1B-1E-F8-76-02-35-5D	1
Nivis WirelessHART v2009 02335A	0011	00-1B-1E-F8-76-02-33-5A	2016-12-06 01:04:38	Path Down	00-1B-1E-F8-76-02-35-5D	-1079303088

\* using UTC time

To search for alerts:

- Select the device, the alert category, priority and type (Class) of alert,
- Optionally, fill in the Start time and the End time fields, and then click

*Search*. The results are displayed in a table that indicates the following

information:

- The device tag,
- The device nickname,
- EUI-64 address – the MAC address of the device generating the alert,
- Alert Time – the date and time when the alert condition was detected,
- Alert Type:
  - Path Down – when the device's path to a neighbor has failed,
  - Source Route Failed – when any neighbor is unreachable on a source route, hence the source route has failed,

- Graph Route Failed – when communication on any route of the graph has failed (in the given example, graph ID 303),
  - Transport Layer Failed – when there has been a Transport Layer connection failure in the communication between the selected device and its peer,
- Peer ID/ Graph ID – the nickname of the neighbor, peer or graph, depending on the type of alert ,
- MIC – the MIC value of the packet that failed routing on a source route that failed.

You can set the number of records to be displayed per page in the table. The default number is 10.

Paging controls at the bottom of the table allow you to navigate through different pages of the search results.

From this page you can also save the search results into a Microsoft Excel CSV file, by clicking *Export*.

# 7 Configuration

The configuration section enables you to view and edit certain settings for the configuration/provisioning of the devices and the network, including connection settings, publishers, alert subscriptions, and Modbus register mapping.

**IMPORTANT:** This section is intended for users with thorough technical knowledge, and certain configurations require advanced expertise, therefore they should be carefully planned, as any inconsistencies may render the devices/network inoperative.

**NOTE:** The changes you perform in the settings for each separate entity will also be reflected in the Advanced Settings page and vice-versa.

## 7.1 Access Point

The Access Point configuration page consists of 4 sections, as shown in the image below. On hover over an edit box a tooltip will appear, indicating the allowed format and range for each value.

The screenshot shows the 'Access Point' configuration interface. It is divided into four main sections:

- General Settings:** Contains three input fields: 'EUI64' with the value '00-1B-1E-F8-70-06-00-01', 'AP Tag' with the value 'NEXCOM AP', and 'Network ID' with the value 'AAAA'. Below these fields is a note: '\*The Access Point must be restarted for the new settings to take effect.'
- Provision/security:** Contains one input field: 'App Join Key' with the value '00001234000000000000000000000000'. Below this field is a note: '\*The Access Point must be restarted for the new settings to take effect.'
- Serial communication:** Contains one input field: 'Serial Name' with the value '/dev/ttyS1'.
- Logging:** Contains a 'Stack Logging level' section with three radio buttons labeled '1', '2', and '3'. Radio button '1' is selected.

At the bottom of the form are two buttons: 'Save' and 'Cancel'.

Under General Settings:

- Specify the EUI64 address, the tag and the Network ID. The Network ID is a unique numeric identifier for the WirelessHART network.

**Note:** *If you change any of these settings, you must restart the Access Point in order for the new settings to take effect.*

Under Provision/security:

- Specify the Join Key.

**Note:** *If you change this value, you must restart the*

*Access Point in order for the new setting to take effect.*

Under Serial communication, provide the name of the serial port.

Under Logging:

- Select the application and stack logging level. The numbers suggest the degree of detail provided in the Access Point logs:
  - 1 (ERROR) for error messages only,
  - 2 (WARN) for error and warning messages,
  - 3 (DEBUG) for error, warning and debug messages.

When you have finished editing the settings, click **Save**. As mentioned previously, depending on the settings that you modify, the Access Point may need to be restarted for the changes to take effect.

## 7.2 Gateway

The Gateway configuration page consists of 3 sections, as shown in the table below.

The screenshot shows the Gateway configuration interface with three main sections:

- General Settings:** Gateway Tag (text input: "NEXCOM GW"), Cache Read Response Timeout (text input: 60), and Cache Burst Response Timeout (text input: 3600). A note below states: "\*The Gateway must be restarted for the new settings to take effect."
- Provision/security:** App Join Key (text input: 00001234000000000000000000000000). A note below states: "\*The Gateway must be restarted for the new settings to take effect."
- Logging:** App Logging level (radio buttons: 1, 2, 3, with 3 selected) and Stack Logging level (radio buttons: 1, 2, 3, with 2 selected).

At the bottom are "Save" and "Cancel" buttons.

Under General Settings:

- Specify the tag for the gateway (optional) and the timeout period, in seconds, for cache read response and cache burst response.

**Note:** If you change any of these settings, you must restart the Gateway in order for the new settings to take effect.

Under Provision/security:

- Specify the Join key.

**Note:** If you change any of these settings, you must restart the Gateway in order for the new settings to take effect.

Under Logging:

- Select the application and stack logging level. The numbers suggest the degree of detail provided in the Gateway logs:
  - 1 (ERROR) for error messages only,
  - 2 (WARN) for error and warning messages,
  - 3 (DEBUG) for error, warning and debug messages.

When you have finished editing the settings, click *Save*. As mentioned above, depending on the settings that you modify, the Access Point may need to be restarted for the changes to take effect.

### 7.3 Network Manager

The Network Manager configuration page consists of 3 sections, as shown in the screen capture below. On hover over an edit box a tooltip will appear, indicating the allowed format and range for each value.

**Network Manager**

---

**General Settings**

Network Manager Tag

\*The Network Manager must be restarted for the new settings to take effect.

**Operational Settings**

Max Device Number (NSD)

Management Bandwidth (s)

Gateway Bandwidth (s)

Join Bandwidth (s)

Health Reports Period (m)

Discovery Reports Period (m)

Keep Alive Period (s)

Compatibility Mode  On  Off

Dynamic Management Bandwidth  On  Off

**Channel maps**

NetworkID	RF Channels															
	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Under General Settings:

- Specify the tag of the Network Manager.

**Note:** *If you change this setting, you must restart the Network Manager in order for the new setting to take effect.*

Under Operational Settings:

- Fill in the bandwidth fields with the desired/appropriate values;
- Enable/Disable Compatibility Mode for the old Emerson devices starting with revision 2;
- Enable/Disable Dynamic Management Bandwidth for the Network Manager to dynamically adjust devices bandwidth.

Under Channel maps:

- Enable the desired frequency channels for communication with the network devices for each Network ID. Click *Add* for a new Network ID\* or ✖ to remove it.
- If you are using more than one Network ID be sure that each channel is used only by one network.

When you have finished editing the settings, click *Save*.

## 7.4 Device Management

This section enables you to edit network configuration information in the “whart\_provisioning.ini” file for existing devices and to add new devices or access points to the network.

Manage those sections with care, incorrect values may render the devices dysfunctional, or may cause difficulty to trace malfunctions.

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.

The screenshot displays the 'Device Management' web interface. It features four main sections: Gateway, Access Points, Devices, and Manage device list. The Gateway section has a text input field containing '00-1B-1E-F9-81-00-00-02, 00 00 12 34 00 00 00 00 00 00 00 00 00 00 00 00'. The Access Points section has a text input field containing '00-1B-1E-F8-70-06-00-01, 00 00 12 34 00 00 00 00 00 00 00 00 00 00 00 00' and 'Save' and 'Delete' buttons. The Devices section has radio buttons for 'Join Key is' (unique per Network, per Device) and an 'Activate' button. The Manage device list section has 'Upload devices' (Choose File, No file chosen), 'Download devices', and 'Load the new device list into Network Manager' (Activate) buttons. A help popup is open over the Access Points section, providing details on the 'Access Point' configuration format: {<EUI64>, <KEY>[, <EUI64\_REDUNDANCY>][, <NETWORK\_ID>]}. It defines EUI64 (8 bytes, hex, separated by minus), KEY (16 bytes, hex, separated by spaces), EUI64\_REDUNDANCY (like EUI64), and NETWORK\_ID (4 bytes, hex). Examples are provided for each field. The popup also includes a 'Gateway, Device' format: {<EUI64>, <KEY>}, with similar definitions and examples for EUI64 and KEY. A 'Close' button is at the bottom of the popup.

### Notes:

1. The EUI-64 address is unique in a network,
2. All the devices in a network must have the Network ID of one of the Access Points.

When adding a device, you have the possibility to select whether the Join Key is unique per network or per device.



If the Join Key is unique per network, any device that has the correct key provisioned, regardless of its network address, will join the network.

If the Join Key differs from device to device, you must enter the correct EUI-64 address and join key for each device, for the devices to be able to join. Afterwards, click **Save** to save the data in the “whart\_provisioning.ini” file.

At the end, click **Activate**, to activate the configuration settings.

### 7.4.1. Configuring Access Point

To add an Access Point in the network, type its EUI64, security key, and Network ID in an empty edit box and click **Save**. The new Access Point will be added to the Access Points list.

To edit an Access Point:

1. Click on the entry that you want to edit in the Access Points list,
2. Edit the security key and/or Network ID, and click **Save** to save the changes in the “whart\_provisioning.ini” file.

Considering Note 1 above, if you change the EUI64 address of an existing Access Point, the Network Manager will recognize it as a new entity and will add the new Access Point to the current list.

Considering Notes 2 above, if you edit an Access Point, it will be removed from an existing network and the devices in that network will be unable to join the network, unless you edit the same parameters for all the field devices in that network.

To delete an Access Point:

1. Select the desired Access Point in the list and click *Delete*,
2. You will be asked for confirmation. Click **Yes** to delete the Access Point or **No** to abort the action.

When you delete an Access Point the devices in its network will be unable to join until a new Access Point provisioned with the same security key and Network ID is added to that network.

After you perform any of the above operations, click *Activate* to load the changes into the Network Manager. The changes will be visible in the network topology and where applicable in the device list.

### 7.4.2. Configuring Gateways

To edit the Gateway:

1. Click on the entry that you want to edit in the Gateways list
2. Edit the security key and/or Network ID, and click *Save* to save the changes in the “whart\_provisioning.ini” file.

After you edit the Gateway section, click *Activate* to load the changes into the Network Manager. The changes will be visible in the network topology and where applicable in the device list.

### 7.4.3. Configuring Devices

#### **Adding devices:**

You can add devices either individually, one device at a time, or you can add multiple devices at a time.

To add a single device in the network type its EUI64, security key, and Network ID in the empty edit box and click *Save*. The new device will be added to the Devices list.

#### **To edit a device / multiple devices:**

1. In the device list, click on the entry that you want to edit,
2. Edit the security key and/or Network ID,
3. Click *Save* to save the changes in the “whart\_provisioning.ini” file.

### **To delete a device / multiple devices:**

1. Select the desired entry in the list and click *Delete*,
2. You will be asked for confirmation. Click *Yes* to delete the device(s) or *No* to abort the action.

After you perform any of the above operations, click *Activate* to load the changes into the Network Manager. The changes will be visible in the network topology and where applicable in the device list.

### **Loading a List of Devices:**

You can add multiple devices at the same time by importing them from a file. The file will contain a list of devices with the <EUI64>, <Key>, and <NetworkID> when appropriate, comma separated values.

To load a list:

1. Click on *Browse* to locate the text file that you wish to load, and click *Upload*,
2. Click *Activate*, to load the new device list into the Network Manager. The current “whart\_provisioning.ini” file will be overwritten and all previous settings will be lost.

### **Exporting the Settings**

This page also enables you to export the configuration settings, by clicking *Save* in the “Manage device list” section.

## 7.5 Monitoring Host

This section enables you to configure burst messages (data publishing from devices to Gateway and visualization in MCS web interface). The configuration settings are stored in the “Monitor\_Host\_Publishers.conf” file.

By default, the system will automatically discover the settings for burst messages for devices joined to the network, provided that such information was not manually entered in Monitor\_Host\_Publishers.conf” file or a discovery process was not ran previously, filling the appropriate settings in the file.

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.

The screenshot shows the Monitoring Control System (MCS) web interface. The main content area is titled "Monitoring Host" and contains several sections:

- Burst Messages:** A table listing burst message definitions. Each row contains an EUI64 address, a command number, a burst message, and an update period. For example: 00-1B-1E-F8-70-00-44-02, 9, 0, 8, 3600.
- Variables:** A section for defining variables, currently empty.
- Trigger:** A section for defining triggers, with an input field containing "1, 0" and a "Del" button.

On the right side, a "Burst Messages Format" help window is open, displaying the syntax for burst messages and variables. The format is: <EUI64>, <COMMAND NUMBER>, <BURST MESSAGE>, <UPDATE PERIOD>, <MAXIMUM UPDATE PERIOD>[, <SUBDEVICE MAC>]. The help text explains the meaning of each field and provides examples of valid values.

### 7.6.1. Burst Messages

To add a burst message definition:

1. In the empty edit box, type the parameters of a burst message definition from a particular device, following the order and format indicated in the Help form: EUI64 address, the number of command of which response will be published through the burst message, the index of the

burst message, the update period and maximum update period in 1/32 ms not exceed 3600s as configured through command 103,

2. Click *Save*. The burst message definition will be added to the list and the changes will be saved in the Monitoring Host configuration file,
3. Add the variables to be published, by following the steps described under 7.3.5.2 Variables,
4. Add the burst trigger, by following the steps described under 7.3.5.3 Triggers.

You can also add a burst message based on an existing one:

1. Click on a burst message in the list,
2. In the edit box, change the EUI64 and burst message index into that of the new burst message,
3. Change other parameters, if applicable,
4. Click *Save*. The burst message will be added to the list; the variables and triggers of the original burst message are preserved in the newly added burst message.

To edit a burst message:

1. In the burst message list, click on the entry that you want to edit,
2. Edit the desired parameters and click *Save*. The changes will be stored in the `Monitor_Host_Publishers.conf` file.

To delete a burst message:

1. Select a burst message in the list and click *Delete*,
2. You will be asked for confirmation. Click *Yes* to delete the burst message or *Cancel* to abort the action.

After you perform any of the above operations, click *Activate* to load the changes into the Monitoring Host.

## 7.6.2. Variables

This section enables you to configure the Device Variables being published through the burst message. We will be calling these Variables for simplicity.

To add a Variable to a burst message definition:

1. In an empty edit box, type the variable parameters in the order and format indicated in the Help form: the device variable code (see Common Table 34 and device family codes), the name on the variable to be displayed in the Readings page, the slot of device variable (value in 0-7 range: 0-3 for command 33 and 0-7 for command 9), the device variable classification (see Common Table 21 and Command 104; required for commands 3 and 33), the units code (see Common Table 2 and Command 4; required for commands 3, 9 and 33),

The command number and burst message index are the same as those used in the burst message definition and are not editable in the interface.

2. Click *Save*. The variable will be added to the variables list for that specific burst message and the changes will be saved in the Monitoring Host configuration file.

To edit a variable:

1. In the variables list, click on the entry that you want to edit
2. Edit the desired parameters and click *Save*. The changes will be stored in the "Monitor\_Host\_Publishers.conf" file

To delete a variable:

1. Select a variable in the list and click *Delete*.
2. You will be asked for confirmation. Click *Yes* to delete the variable or *Cancel* to abort the action.

After you perform any of the above operations, click *Activate* to load the changes into the Monitoring Host.

### 7.6.3. Triggers

This section is optional and enables you to configure the trigger of a burst message. To add a Trigger to a burst message definition:

1. In an empty edit box, type the trigger parameters in the order and format indicated in the Help form: the burst trigger mode selection, having one of the values: Continuous, Window, Rising, Falling, On-Change (see Cmd 104, Common Table 33), the device variable classification (see Common Table 21 and Cmd 104), the units code (see Common Table 2 and Cmd 4), the trigger level (float value). The command number and burst message index are the same as those used in the burst message definition and are not editable in the interface,
2. Click *Save*. The trigger will be added for the selected burst message and changes will be saved in the Monitoring Host configuration file.

To edit a trigger:

1. In the trigger edit box, edit the desired parameters and click *Save*. The changes will be stored in the  
  
Monitor\_Host\_Publishers.conf" file.

To delete a variable:

1. Click *Delete* button near the trigger edit box,
2. You will be asked for confirmation. Click *Yes* to delete the trigger or *Cancel* to abort the action.

After you perform any of the above operations, click *Activate* to load the changes into the Monitoring Host.

#### Loading a List of Burst Message Definitions

You can add multiple burst message definitions from different devices at the same time by importing them from a file. The file will contain the list of devices and their burst message definitions, with the associated parameters respectively expressed as comma separated values.

To load a list:

1. Click on *Browse* to locate the text file that you wish to load, and click *Upload*,
2. Click *Activate*, to load the new burst messages list into the Monitoring Host. The current *Monitor\_Host\_Publishers.conf* file will be overwritten.

Exporting the Burst Message Definitions:

This page also enables you to export the publisher list (including channels), by clicking *Download* in the “Manage burst messages list” section.

## 7.6 MODBUS

This section enables you to map WIRELESSHART attributes to Modbus registers.

Click **Help** in the upper right corner of the window to view information and examples of the accepted data formats in all the sections.

The screenshot shows the 'Monitoring Control System' interface for 'MODBUS Server' configuration. The left sidebar contains navigation links for Network, Configuration, Statistics, and Administration. The main area is divided into 'Input registers' and 'Holding registers'. The 'Input registers' table lists the following registers:

Address	Device Variable
0,3,001B1EF981000002	device_variable,9,245,0
3,3,001B1EF981000002	device_variable,9,246,0
6,3,001B1EF981000002	device_variable,33,245,0
9,3,001B1EF981000002	device_variable,33,246,0
48,2,001B1EF870004403	device_variable,9,245,2
50,2,001B1EF870004403	device_variable,9,246,2
52,2,001B1EF870004403	device_variable,33,245,2
54,2,001B1EF870004403	device_variable,33,246,2

The 'Holding registers' section is currently empty. A 'Help' window is open on the right, showing the following information:

**INPUT/HOLDING REGISTER:**

**Format1:** {<START ADDRESS>, <WORD COUNT>, <EUI64>, <REGISTER TYPE>, <BURST MESSAGE>, <DEVICE VARIABLE CODE>, <DEVICE STATE>}

START ADDRESS: integer in [0-65535]  
WORD COUNT: integer in [1-125]  
EUI64: 8 bytes grouped by 2, represented as hex, separated by minus  
REGISTER TYPE: device\_variable  
BURST MESSAGE: integer in [0-255]  
DEVICE VARIABLE CODE: integer in [0-255]  
DEVICE STATE: integer in {0, 2}

**Format2:** {<START ADDRESS>, <WORD COUNT>, <EUI64>, <REGISTER TYPE>}

START ADDRESS: integer in [0-65535]  
WORD COUNT: 5  
EUI64: 00-1B-1E-F9-81-00-00-02, 00-00-00-00-00-00-00-00 or FF-FF-FF-FF-FF-FF-FF-FF  
REGISTER TYPE: gw\_info

**Format3:** {<START ADDRESS>, <WORD COUNT>, <EUI64>, <REGISTER TYPE>}

START ADDRESS: integer in [0-65535]  
WORD COUNT: integer in [1-16]  
EUI64: 00-1B-1E-F9-81-00-00-02, 00-00-00-00-00-00-00-00 or FF-FF-FF-FF-FF-FF-FF-FF  
REGISTER TYPE: gw\_code\_word

Close



### 7.6.1. Mapping Registers

The mapping area contains two sections listings the two different groups of registers: Input Registers and Holding Registers.

The mapping between a register and a device variable is achieved by adding register line in the appropriate section. Please note that mapping read-only variables to holding registers will not make the variables themselves writable.

To add a register line:

1. In an empty edit box, type the parameters in the order and format indicated in the Help form:
  - start address - decimal integer, between 0 and 65535, representing the start address of the Modbus register;
  - word count - decimal integer, between 1 and 125, representing the number of 16-bit modbus words allocated for this Wireless HART data element;
  - EUI-64 - string of 16 hex digits, representing the 8 bytes of a device's EUI-64 address;
  - register type: *device\_variable*, *gw\_info* or *gw\_code\_word* are the three register types
  - supported;

When register type is "device\_variable", the following parameters must be specified:

- the burst message you want to map;
- device variable code;
- device state - decimal integer, 0 and 2 with the following meaning:
  - 0 – the Wireless Hart device variable is mapped onto the chunk of registers, starting from address <start\_addr>. The value should be interpreted as 4 bytes float. Wireless Hart Communication errors (e.g. device not joined) will make addressing these registers return the MODBUS exception 0x04 (slave device failure);
  - 2 – the Wireless Hart device variable is mapped onto the chunk of registers, starting from address <start\_addr>+1. The value should be interpreted as 4 bytes float. At address <start\_addr> there is a "device state register" generated by the MODBUS server which reflects the

state of the Wireless Hart communication. The value should be interpreted as 16 bit big-endian integer with the following values:

- 128: Device Joined with fresh data
- 8: Device NOT joined and no data read so far
- 20: Device NOT joined but with stale data
- 24: Device Joined but no data read so far
- 4: Device Joined but with stale data

When register type is “gw\_info”, general gateway information will be exposed to Modbus, using the following registers:

Register	Item exposed	Observation
<start_addr> + 0	Number of devices currently connected.	16bit big-endian integer
<start_addr> + 1	Total number of burst messages.	16bit big-endian integer
<start_addr> + 2	Versa Router MAC	3 words * 16bit big-endian unsigned integer

**Note:** For register type “gw\_info” the <word\_cnt> must be 5.

When register type is “gw\_code\_word”, the gateway’s “code word” will be exposed to Modbus. The “code word” is read-only.

**Note:** For register type “gw\_code\_word”, the <word\_cnt> should be 16 or less.

The <EUI64> in “gw\_info” and “gw\_code\_word” register lines should identify the WirelessHart Gateway.

Accepted values: 001B1EF981000002, 0000000000000000, FFFFFFFFFFFFFFFF.

2. Click Save to add the new register line in the Registers list.

**Note:** For register type “gw\_info” the <word\_cnt> must be 5.

When register type is “gw\_code\_word”, the gateway’s “code word” will be exposed to Modbus. The “code word” is read-only.

**Note:** For register type “gw\_code\_word”, the <word\_cnt> should be 16 or less.

The <EUI64> in “gw\_info” and “gw\_code\_word” register lines should identify the WirelessHart Gateway.

Accepted values: 001B1EF981000002, 0000000000000000, FFFFFFFFFFFFFFFF.

3. Click Save to add the new register line in the Registers list.

**Notes:**

- When mapping the Modbus registers on the WirelessHART data entities, you must consider the size of the WirelessHART data entity and allocate a contiguous chunk of Modbus 16-bit registers in the Modbus addressing space to hold the entire data entity (plus an additional Modbus register to hold the auto-generated status, if applicable). When the chunk is bigger than the size of the data entity, it will be filled with the actual data from the lowest addressed register to the highest, and from the MSB of each register to the LSB. If the data entity does not entirely fill the last register, the register will have the data on the MSB and the LSB will be set to zero.
- If the address range of a register line overlaps an existing register line in the same group, or if it does not fit in the range 0-65535, it will be ignored

Loading a List of Registers

You can import the register map from a file that includes the input and holding registers lines with their parameters which are expressed as comma separated values.

To load the list:

1. In the “Manage registers list” section click on *Browse* to locate the text file that you wish to load, and click *Upload*.
2. Click *Activate*, to load the new host list into Modbus. The current “modbus\_gw.ini” file will be overwritten.

Exporting the Registers:

This page also enables you to export the registers, by clicking *Download* in the “Manage registers list” section.

## 7.7 Advanced Settings

### Advanced Settings

**Sections/variables**

Section ..... GLOBAL ▼

Variable ..... AN\_ID ▼

Value ..... 00 000002

\*The associated application must be restarted for the new settings to take effect.

**Restart**

Applications	<input type="button" value="Restart"/>
NIO200 Hardware	<input type="button" value="Restart"/>

\*After a restart the NIO200 Monitoring Control System becomes inoperable for a few minutes.

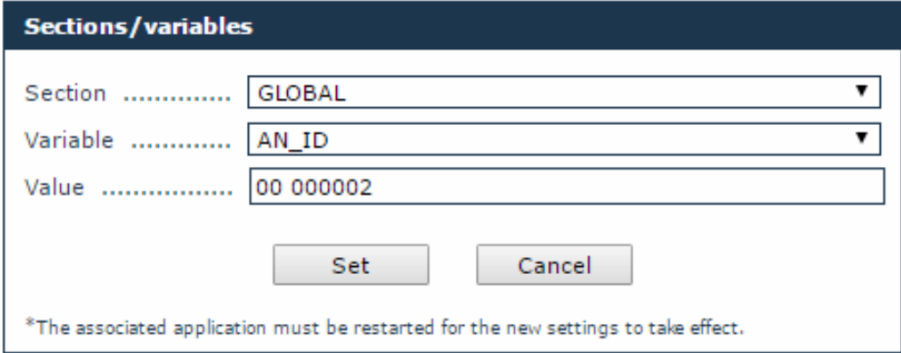
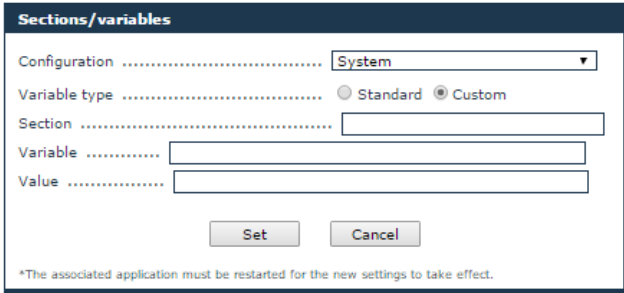
**Mesh WiFi & NTP Settings**

Open NEXCOM NIO200 admin website:

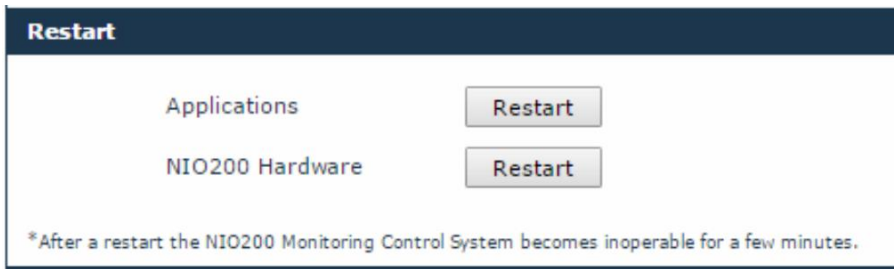
### 7.6.2. Edit Configuration Variables

This page allows you to view/set less common configuration variables, which cannot be changed using the classic MCS web interface.

**IMPORTANT:** This page is for advanced users only – do not use unless you have been instructed exactly by a NEXCOM representative on what values to change. Incorrect values may render the router dysfunctional, or may cause difficulty to trace malfunctions.

Step	Action
1.	<p>The following form will open to the right of the operation list:</p> 
2.	<p>In the form, select a Section in the drop-down list. The Variable list will change accordingly.</p>
3.	<p>Select a Variable in the drop-down list.</p> <p><b>IMPORTANT: Do not change [GLOBAL].AN_ID under any circumstance.</b></p>
4.	<p>Set/edit the Value field, then click <b>Set</b>.</p>
5.	<p>To add a new variable, select <b>Custom</b> under Variable type. The Sections/variables form will be empty.</p> 
6.	<p>Type the desired information in the Section, Variable, and Value fields, then click <b>Set</b>.</p>

### 7.6.3. Restart



This section enables the user to restart the applications running on the NIO 200HAG Gateway.

The “**Restart Applications**” restart all applications, without rebooting the board.

The “**Restart NIO200 Hardware**” reboots the NIO 200HAG Gateway.

**NOTE:** After restarting the applications or rebooting the NIO 200HAG Gateway, the Monitoring Control System becomes inoperative for a few minutes.  
After Stopping the applications, the Monitoring Control System becomes inoperative until the next power cycle.

### 7.6.4. Access NEXCOM NIO200 admin website



This section allows the user to navigate to NEXCOM NIO200 admin website, where the NIO200 Network Configuration (WiFi settings, IP Addresses, NTP Server, etc) can be changed.

## 8 System Status

The Statistics page displays statistical information regarding processor and memory usage, and load average on the NIO 200HAG Gateway.

System Status	
<b>Access Point</b>	Status: <b>Running</b> Memory: 2.34 MB (0.31%) Processor: 0.5 %
<b>Gateway</b>	Status: <b>Running</b> Memory: 4.88 MB (0.64%) Processor: 0.0 %
<b>Network Manager</b>	Status: <b>Running</b> Memory: 6.8 MB (0.90%) Processor: 0.0 %
<b>MODBUS</b>	Status: <b>Running</b> Memory: 4.7 MB (0.62%) Processor: 0.0 %
<b>Monitor Host</b>	Status: <b>Running</b> Memory: 5.75 MB (0.76%) Processor: 0.0 %
<b>System memory</b>	Total: 757.34 MB Used: 195.96 MB (25.88%) Free: 561.38 MB (74.12%)
<b>Flash memory</b>	Total: 20 MB Used: 4.08 MB (20.39%) Free: 15.92 MB (79.61%)
<b>Load average</b>	Load average (1',5',15'): 0.01 0.03 0.05 1/65 12526
<input checked="" type="checkbox"/> Auto refresh page (every 1 minute)	

The System Status page displays statistical information regarding processor and memory usage, and load average on the NIO200.

The first five sections indicate the status (“Running” or “Not Running”), memory usage and processor usage for the Access Point, Gateway, Network Manager, MODBUS, and Monitor Host processes.

The following two sections display system memory and flash memory availability information.

The Load average section indicates:

- The system's load average over the past one, five and fifteen minutes respectively,
- The number of running processes out of the total number of processes,
- The ID of the last started process.

If you wish to regularly update the system status information, enable the Auto refresh page option at the bottom of the page. The page will auto refresh at one-minute intervals.



# 9 Administration

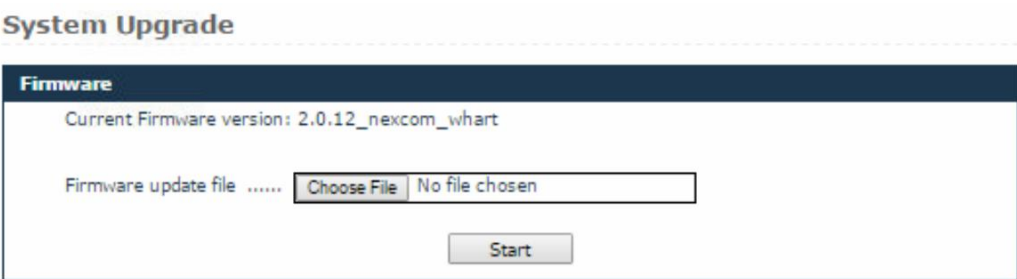
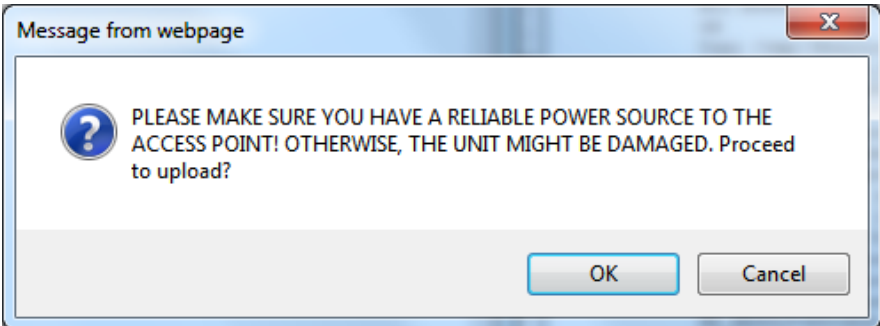
The administration section encompasses tools for the management of the WirelessHART based system. It allows the users with proper rights to update system firmware and to manage device icons.

## 9.1 System Upgrade

The System Upgrade page enables you to upgrade the system components hosted on the connected NIO 200HAG Gateway.

The Firmware form indicates the current system version on the NIO 200HAG Gateway.

### To initiate the upgrade

Step	Action
1.	Click <b>Browse</b> to locate and open the upgrade package that you wish to use:  
2.	Click the <b>Upload Firmware</b> button to initiate the process.
3.	Make sure the NIO200 has a reliable power source. When asked click OK  

Step	Action
4.	<p>When the upgrade is complete, the page indicates the result of the upgrade:</p> <p style="text-align: center;"><b>System has been upgraded successfully.</b></p> <p style="text-align: center;">System rebooting...</p> <p style="text-align: center;"><a href="#">Main Page</a></p>

## 9.2 Custom Icons

This page enables you to assign custom icons for the devices in a network based on their role, with a view to better distinguishing them.

When the page is loaded, the existing custom icons are displayed in a table, with the following information:

- Model – the device model
- Role – the device role
- Icon – shows the existing picture

The default icons are not listed.

To add an icon:


1. Click the *Add Icon* button. The Custom Icon form will open:

### Add Custom Icon

2. Select the Device Model (Role) from the drop-down list,
3. Click *Browse* to locate the icon you want to use. The maximum icon size must be 32x32 pixels and the maximum file size must be 100 Kb. Supported formats are jpg, png, and gif,

4. Click *Add*. A message will appear, indicating that the icon has been added successfully,
5. Click *Back* in the form or **Custom Icons** under Administration to return to the Icons list,
6. The newly added icon will be visible in the Icons list, the Topology page, and the Devices page.

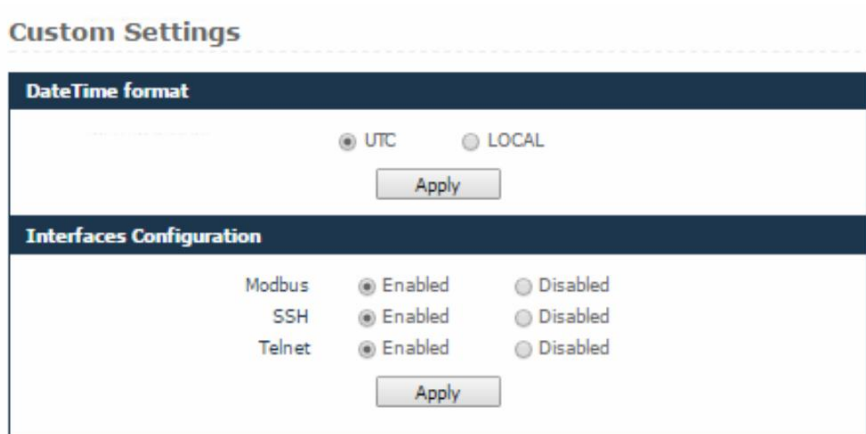
To delete an icon:

1. In the Icons list, click  next to the icon entry,
2. You will be asked for confirmation. Click *OK* to delete the icon or *Cancel* to abort the action.

**Note:** When you delete an icon, it will be automatically replaced with the default icon for the selected device model/role in the Topology and Devices pages.

### 9.3 Custom Settings

This page enables user to define whether the timestamps get shown using browser local time zone or UTC; and enable/disable various high-side interfaces.



**Custom Settings**

**DateTime format**

UTC  LOCAL

Apply

**Interfaces Configuration**

Modbus	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
SSH	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Telnet	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled

Apply

Date Time Format devined the format to display timestamps: using the browser local time zone settings or using UTC.

The Interfaces configuration allow enabling/disabling the high-side interfaces.

## 9.4 Device Codes

This page features a list of all the WirelessHART devices that have been approved by HART Communication Foundation (HCF). The devices are listed in a table with the following information:

- Code – the device code assigned by HCF,
- Model – the device model (name) as given by the vendor,
- Company – the device vendor.

### Device Codes

**Add Device Code**

Code	<input type="text"/>	Model	<input type="text"/>	<input type="button" value="Search"/>
Company	<input type="text"/>			

Items per page **10** out of total **774** << < 1/78 > >>

<u>Code</u> ▲	<u>Model</u>	<u>Company</u>	
<a href="#">772</a>	NEWTHERMOX	Ametek	✘
<a href="#">2561</a>	TRI20	Brooks Instrument	✘
<a href="#">2562</a>	38XXVA	Brooks Instrument	✘
<a href="#">2563</a>	99XXOVAL	Brooks Instrument	✘
<a href="#">2564</a>	QUANTIM	Brooks Instrument	✘
<a href="#">3348</a>	Gas USM	Daniel Industries	✘
<a href="#">3368</a>	Liquid USM	Daniel Industries	✘
<a href="#">3585</a>	HT	Delta Controls	✘
<a href="#">4355</a>	FMU860	Endress & Hauser	✘
<a href="#">4356</a>	FMU861	Endress & Hauser	✘

When a new device joins the Nivis WirelessHART network and reports a device code that is not part of the list, the new device code will be automatically added to the list, having the Model and Company fields populated with ,N/A'. You must change the model and company names manually. To learn how to change these fields, see section Editing a Device Code.

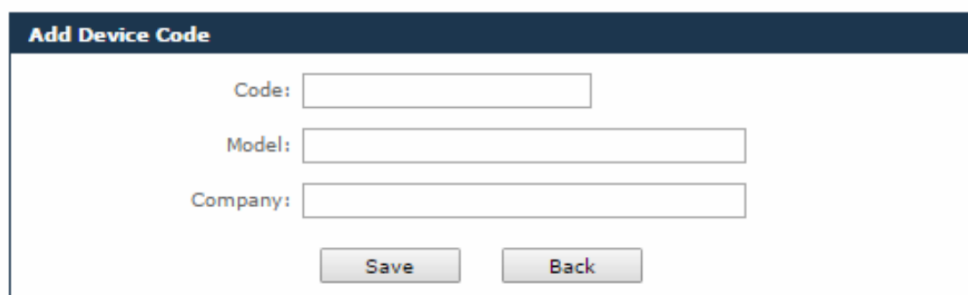
You can sort or search for entries in the table by code, model and company.

To search for specific entries:

1. In the search form located on top of the list, type the desired code, model, or company (or part of the selected criterion) in the corresponding field. *Note that you can use multiple search criteria at the same time,*
2. Click *Search*. The MCS will display all the entries that match your search criteria. If no entries match your selected criteria, the system will display the message “No records! ”

### 9.4.1 Adding a Device Code

#### Add/Edit Device Code



**Add Device Code**

Code:

Model:

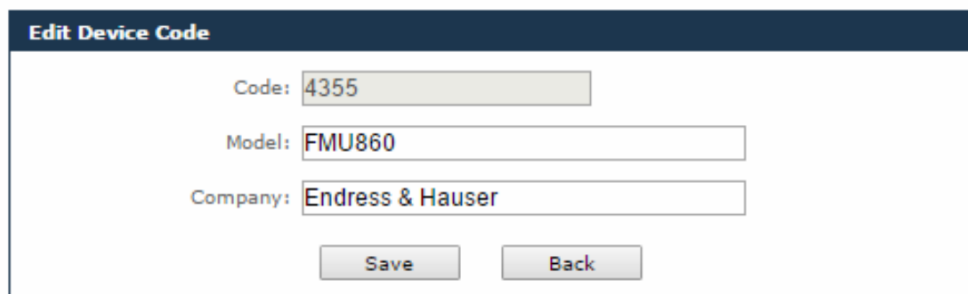
Company:

To add a device code:

1. Click the *Add Device Code* button located on top of the search form. The *Add Device Code* form will open
2. In the form, fill in the edit fields with the desired information,
3. Click *Save* to add the device to the list, or *Back* to cancel the action and return to the Device Codes page.

### 9.4.2 Editing a Device Code

#### Add/Edit Device Code



**Edit Device Code**

Code:

Model:

Company:


To edit a device code:

1. Click on the code in the list. The *Edit Device Code* form will open
2. In the form, edit the desired information under Model and Company,

*Note that you cannot change the device Code in this form. To change a device code, you can delete a device code and add it again.*

3. Click *Save* to save your changes, or *Back* to cancel the action and return to the Device Codes page.

### 9.4.3 Deleting a Device Code

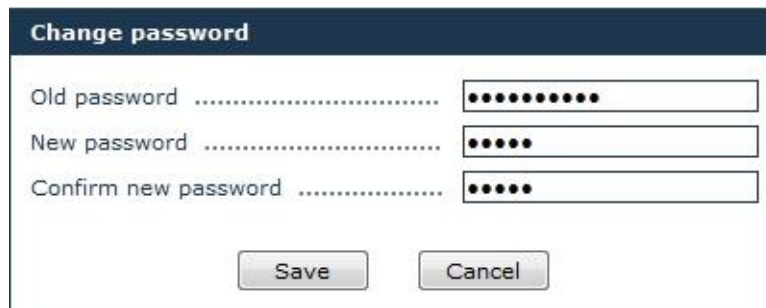
To delete a device code, click the icon  located next to the corresponding entry in the table. The system will require confirmation to perform the action. Click *OK* to delete the device code or *Cancel* to abort the action.

**Note:** *When you remove a device from the Device Codes list, the device will no longer be visible in the MCS, even when it is joined.*

# 10 Session

## 10.1 Change Password

This page enables you to change your own password.



The image shows a 'Change password' dialog box. It has a dark blue header with the text 'Change password'. Below the header are three input fields: 'Old password', 'New password', and 'Confirm new password'. Each field contains a series of black dots representing masked text. At the bottom of the dialog box are two buttons: 'Save' and 'Cancel'.

Step	Action
1.	In the form, type your current password in the Old Password field.
2.	Type the new password in the New password field.
3.	Retype the new password in the Confirm new password field, for verification. <b>NOTE:</b> The passwords are case sensitive.
4.	Click <b>Save</b> at the bottom of the page to save the new password, which will become your current password.

**Tip:** To prevent unauthorized persons to gain access to your account, use a strong password in order to make it difficult for others to determine it and do not disclose your password to anyone.

# Appendix

---

## **Advanced configuration about Wi-Fi features**



# 1. Login

To access the NIO200HAG device, you may open a browser to access the Web GUI via default IP address 192.168.1.1. The login Web page requires login information as below:



Default login information is:

Login: root

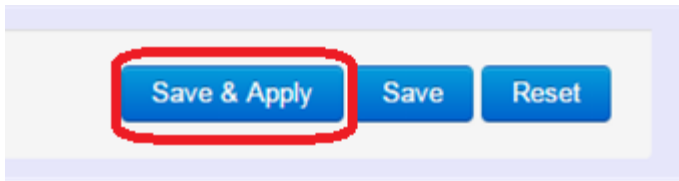
Password: admin

After successful login, you will see the “Status” page of the device Web UI.



## Saving Changes

Saving & apply the configuration in WebUI after you do the changes at the bottom of WebUI.



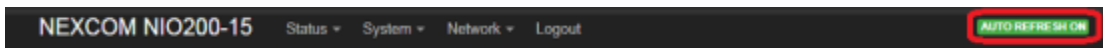
## Unsaved Changes



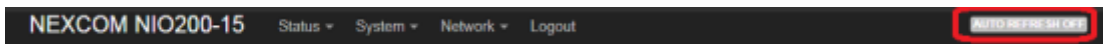
“UNSAVED CHANGES” provides the help to see the parameters which were not saved & applied,

Click “Save & Apply” button to save the parameters.

## Auto Refresh

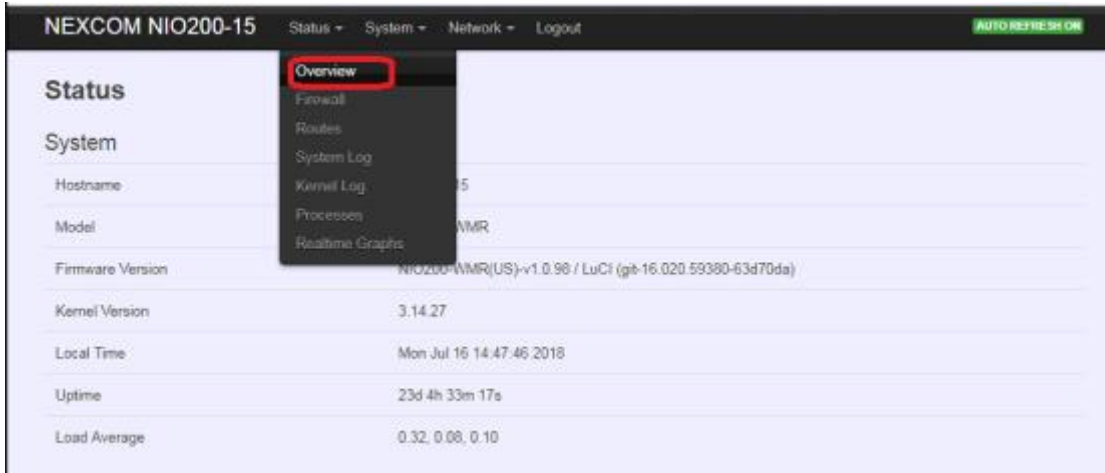


Toggle “AUTO REFRESH” button to turn on/off WebUI refresh function automatically



## 2. Status

To display more detailed status, you can click the “Status” under the page bar. This allows users to select the item of Overview, Firewall, Routes, System Log, Kernel Log, Process, and Real-time Graphs from the pull-down list like below screen:



### 2.1 Overview

To see NIO200 over all status, click “Overview” to displays the current system information and interface connection status.

### System



**Hostname:** Displays NIO200 host name

**Model:** Displays NIO200 HW basic information

**Firmware Version:** Displays NIO200 firmware version.

**Kernel Version:** Displays NIO200 Kernel version.

**Local Time:** Displays NIO200 current date and time.

**Uptime:** Displays how long NIO200 has been operating since last boot-up.

**Load Average:** CPU average loading in recent time frame.

For example,



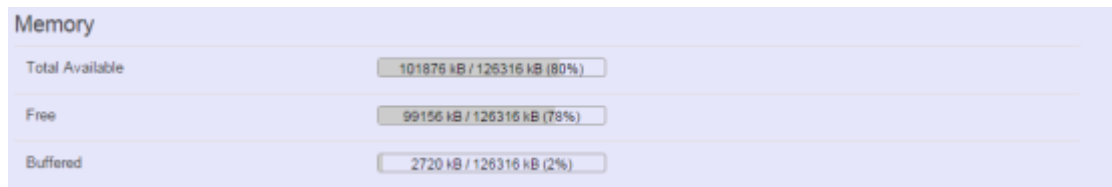
CPU average loading:

94% in the past 1 minute.

43% in the past 5 minutes

24% in the past 15 minutes.

## Memory

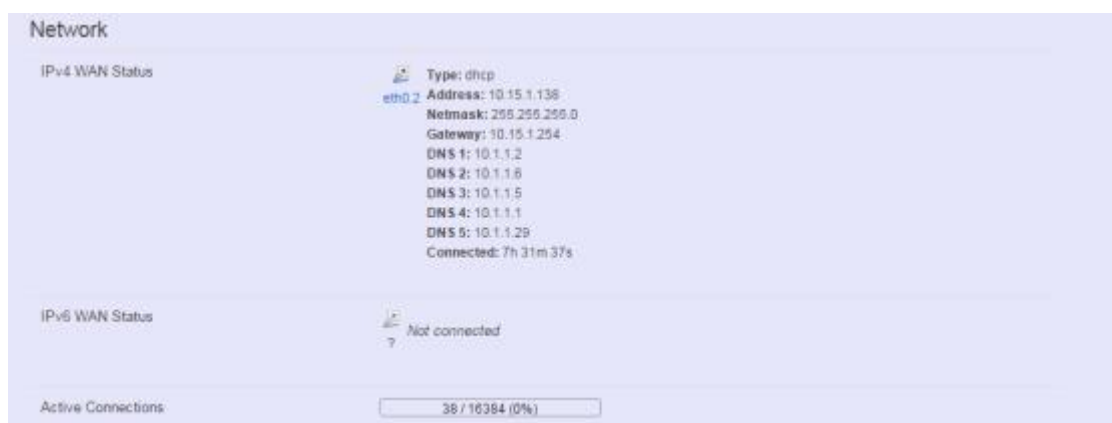


**Total Available:** Displays the available memory in percentage.

**Free:** Displays free memory of NIO200.

**Buffered:** Displays buffer memory used in the system.

## Network



**IPv4 WAN Status:** Displays current connecting IPv4 information.

**IPv6 WAN Status:** Displays current connecting IPv6 information.

**Active Connections:** Displays current active connections.

## DHCP Leases

DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
IM03-AndrewWang1	192.168.1.219	08:3e:8e:67:64:03	10h 25m 0s
IM03-JonesChen	192.168.1.215	9c:2a:70:1b:4c:9d	6h 1m 34s
?	192.168.1.142	94:a1:a2:87:6f:08	9h 22m 13s
NEXCOM-SQA	192.168.1.105	00:0d:f0:ac:c8:63	10h 34m 24s
River-Ubuntu	192.168.1.118	80:19:34:c9:04:00	6h 51m 48s

This displays information about hosts (Personal Computers or electronic devices) that are connected to NIO200 including IPv4, MAC address and leasing time

## DHCPv6 Leases

DHCPv6 Leases			
Hostname	IPv6-Address	DUID	Leasetime remaining
River-Ubuntu	fdcf:68c3:19eb::10b/128	0004767fc-d07324b68c-bab02958b2991f645	6h 51m 39s
NEXCOM-SQA	fdcf:68c3:19eb::3b0/128	000100011e1b93b70010f32db9b8	10h 34m 17s
IM03-JonesChen	fdcf:68c3:19eb::d25/128	000100011b2c6cb9206a8a9612c0	4h 14m 5s
NIFE-3600-SQA	fdcf:68c3:19eb::ed2/128	000100011e1c6e5e0010f32db9b8	5h 13m 27s

This displays information about hosts (Personal Computers or electronic devices) that are connected to NIO200 including IPv6, DUID and leasing time.

## Wireless

Wireless	
Generic 802.11an Wireless Controller (radio0)	<b>SSID:</b> backbone <b>Mode:</b> Mesh <b>Channel:</b> 36 (5.180 GHz) <b>Bitrate:</b> 43 Mbit/s <b>MAC:</b> 00:10:F3:6D:48:B4 <b>Encryption:</b> NONE
Generic 802.11an Wireless Controller (radio1)	<b>SSID:</b> management-15 <b>Mode:</b> Master <b>Channel:</b> 0 (0.000 GHz) <b>Bitrate:</b> ? Mbit/s <b>MAC:</b> 00:00:00:00:00:00 <b>Encryption:</b> unknown













This displays Wireless information about NIO200 for radio 0&1.

**SSID:** Displays the name of the wireless network.

**Mode:** Displays the mode in this radio

- Channel:** Displays current channel using.
- Bitrate:** Displays current wireless data rate.
- BSSID:** Displays MAC address of this radio
- Encryption:** Displays current encryption setting.

## Associated Stations

Associated Stations					
	Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
 wlan0	Mesh "backbone"	00:10:F3:77:28:5D	?	 -69 / -93 dBm	45.0 Mbit/s, MCS 2, 40MHz 28.9 Mbit/s, MCS 3, 20MHz
 wlan0	Mesh "backbone"	00:10:F3:6E:E6:A2	?	 -77 / -93 dBm	30.0 Mbit/s, MCS 1, 40MHz 27.0 Mbit/s, MCS 1, 40MHz
 wlan0	Mesh "backbone"	00:10:F3:6D:48:75	?	 -64 / -93 dBm	150.0 Mbit/s, MCS 7, 40MHz 135.0 Mbit/s, MCS 7, 40MHz
 wlan0	Mesh "backbone"	00:10:F3:62:38:87	?	 -66 / -93 dBm	120.0 Mbit/s, MCS 5, 40MHz 121.5 Mbit/s, MCS 6, 40MHz
 wlan0	Mesh "backbone"	00:10:F3:62:38:81	?	 -78 / -93 dBm	6.5 Mbit/s, MCS 0, 20MHz 27.0 Mbit/s, MCS 1, 40MHz
 wlan0	Mesh "backbone"	00:10:F3:35:26:25	?	 -68 / -93 dBm	108.0 Mbit/s, MCS 5, 40MHz 81.0 Mbit/s, MCS 4, 40MHz

Displays current associated device information (Personal Computers or electronic devices) with NIO200HAG, including device's MAC address, signal level, noise, connecting data rate.

## 2.2 Firewall

Firewall setting is a particular function which allows user to connect or block two or more interfaces in device with sophisticated and specifically defined parameters in this Web page.

It's highly recommended to keep this Firewall setup page as it is.

**Firewall Status**

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 2816060, Traffic: 210.85 MB)

Pkts.	Traffic	Target	In	Out	Source	Destination	Options	
2816060	210.85 MB	delegate_input	all	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options
0	0.00 B	delegate_forward	all	*	*	0.0.0.0/0	0.0.0.0/0	-

## 2.3 Routes

This section display information about routing list for current connecting device.

### ARP

IPv4.Address	MAC.Address	Interface
192.168.1.105	00:0d:f0:ac:c8:63	br-lan
192.168.1.118	80:19:34:c9:04:00	br-lan
10.15.1.142	00:10:f3:50:99:c0	eth0.2
10.15.1.254	78:48:59:64:5b:44	eth0.2
192.168.1.142	94:a1:a2:87:6f:08	br-lan
192.168.1.110	c4:54:44:de:fe:a5	br-lan
192.168.1.206	94:a1:a2:87:6f:48	br-lan
192.168.1.219	08:3e:8e:67:64:03	br-lan
10.15.1.201	00:26:73:29:15:7c	eth0.2

Displays APR table information of NIO200 including IPv4 address, MAC address and connecting interface.

### Active IPv4-Routes

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	10.15.1.254	0	main
wan	10.15.1.0/24		0	main
lan	192.168.1.0/24		0	main

Displays active WAN and LAN port's IPv4 routing table.

## Active IPv6-Routes

Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fdfc:68c3:19eb:0:e5df:2aba:f91:5221		0	main
lan	fdfc:68c3:19eb::/64		1024	main
wan	:::1		0	local
wan	:::2		0	local
wan	:::c		0	local
wan	:::1:2		0	local
wan	:::1:3		0	local
wan	:::1:#f50:9e09		0	local
lan	:::fB		256	local
(eth0)	:::fB		256	local
wan	:::fB		256	local
lan	:::fB		256	local
lan	:::fB		256	local

Displays active IPv6 routing table of WAN and LAN port.

## IPv6 Neighbors



IPv6 Address	MAC Address	Interface
fd1c:68c3:19eb:0:114:f243:8e92:a881	80:19:34:c9:04:00	lan
fd1c:68c3:19eb:0:e5df:2aba:f91:5221	80:19:34:c9:04:00	lan
fd1c:68c3:19eb::3b0	00:0d:f0:ac:c8:63	lan
fd1c:68c3:19eb:0:21cf:7bb5:a2c:9:e438	00:0d:f0:ac:c8:63	lan
fd1c:68c3:19eb:0:b815:35a6:d8b7:d868	00:0d:f0:ac:c8:63	lan
fd1c:68c3:19eb:0:691a:9a70:b879:924d	80:19:34:c9:04:00	lan
fd1c:68c3:19eb:0:468:1e7:d4fe:8c9a	9c:2a:70:1b:4c:9d	lan
fd1c:68c3:19eb:0:f118:d10c:ab71:1676	80:19:34:c9:04:00	lan
fd1c:68c3:19eb:0:7c3a:bc4c:52e3:da5a	00:0d:f0:ac:c8:63	lan
fd1c:68c3:19eb:0:6046:1236:d9c8:82c:1	00:0d:f0:ac:c8:63	lan
fd1c:68c3:19eb:0:c654:44ff:fedc:fea5	c4:54:44:de:fe:a5	lan
fd1c:68c3:19eb:0:a151:5f16:a221:fc7c	c4:54:44:de:fe:a5	lan
fd1c:68c3:19eb:0:61ad:92b6:99e2:bf9b	80:19:34:c9:04:00	lan

Display connected device with IPv6 information.

## 2.4 System Log

The “System Log” Web page contains the events log in NIO200 system for trouble shooting reference.

System Log
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:58:46 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:58:46 2018 kern.info kernel: [1439056.639602] br-lan: port 4(wlan1) entered learning state
Tue Jul 10 01:58:46 2018 kern.info kernel: [1439056.639811] br-lan: port 4(wlan1) entered forwarding state
Tue Jul 10 01:59:04 2018 daemon.notice netifd: Interface 'lan' is now down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_br_up: br-lan was up. Set down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan: eth1:0 entering disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.062970] br-lan: port 4(wlan1) entered disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.063040] br-lan: port 3(wlan0) entered disabled state
Tue Jul 10 01:59:04 2018 kern.info kernel: [1439075.065882] br-lan: port 1(eth1) entered disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan: eth2:0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan: wlan0:0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: MSTP_OUT_set_state: br-lan: wlan1:0 entering disabled state
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan1 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan1: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan0: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth1 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth2 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth2 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port eth2 : down
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up
Tue Jul 10 01:59:04 2018 daemon.info mstpd: error, ethtool_get_speed_duplex: Cannot get speed/duplex for wlan0: Operation not supported
Tue Jul 10 01:59:04 2018 daemon.info mstpd: set_if_up: Port wlan0 : up

## 2.5 Kernel Log

The “Kernel Log” displays the record of kernel activities. The administrator can monitor the system status by checking this log.



## 2.6 Processes

This Webpage is designed for detailed trouble shooting/status monitoring by professional personnel in the field. Any improper terminating or killing individual process tasks may cause device malfunction. **It's highly recommended to keep this Firewall setup page as it is.**

**Processes**  
This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/procd	0%	0%			
2	root	[kthreadd]	0%	0%			
3	root	[ksoftirqd/0]	0%	0%			
5	root	[kworker/0.0H]	0%	0%			
7	root	[rcu_sched]	0%	0%			
8	root	[rcu_bh]	0%	0%			
9	root	[migration/0]	0%	0%			
10	root	[migration/1]	0%	0%			

## 2.7 Real-time Graphic

This section provides utilities to monitor NIO200 system information including real-time load, real-time Ethernet traffic, Real-time wireless signal and real-time associated device traffic.

To monitor status in this section, please make sure WebUI “auto refresh” function must be “**turn on**”.

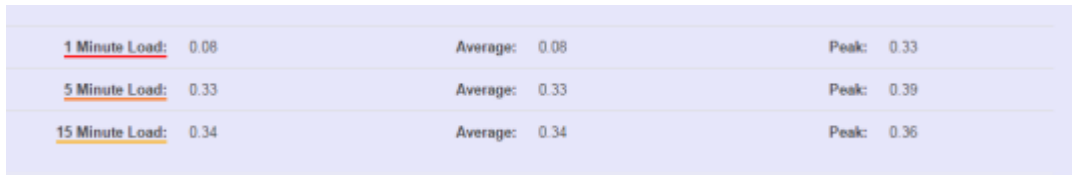


## Load



Display real-time CPU average loading percentage.

i.e.



Time Window	Minimum	Average	Peak
1 minute	8%	8%	33%
5 minutes	33%	33%	39%
15 minutes	34%	34%	36%

## Traffic

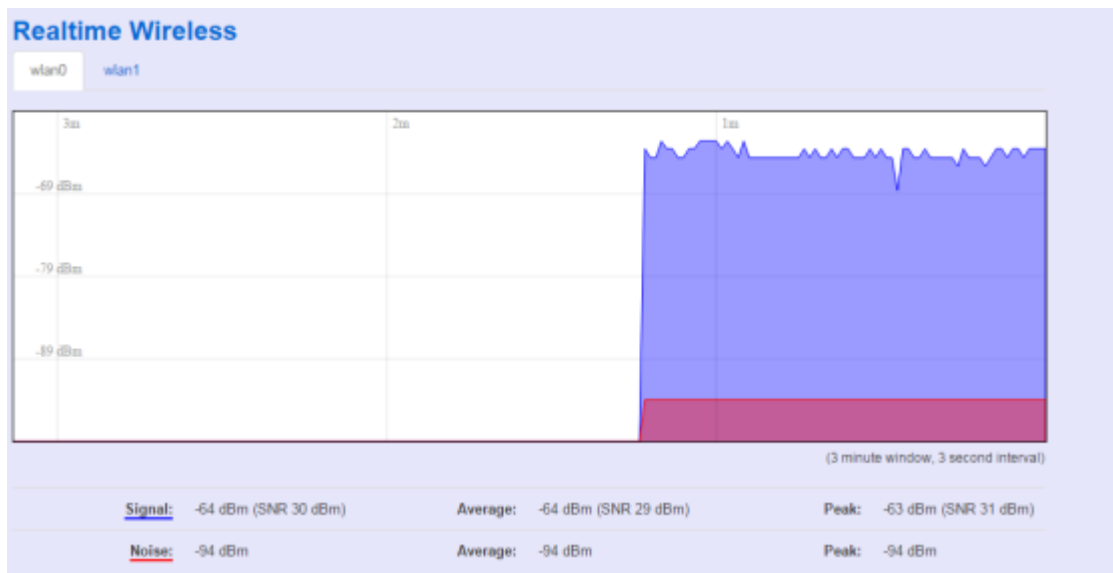


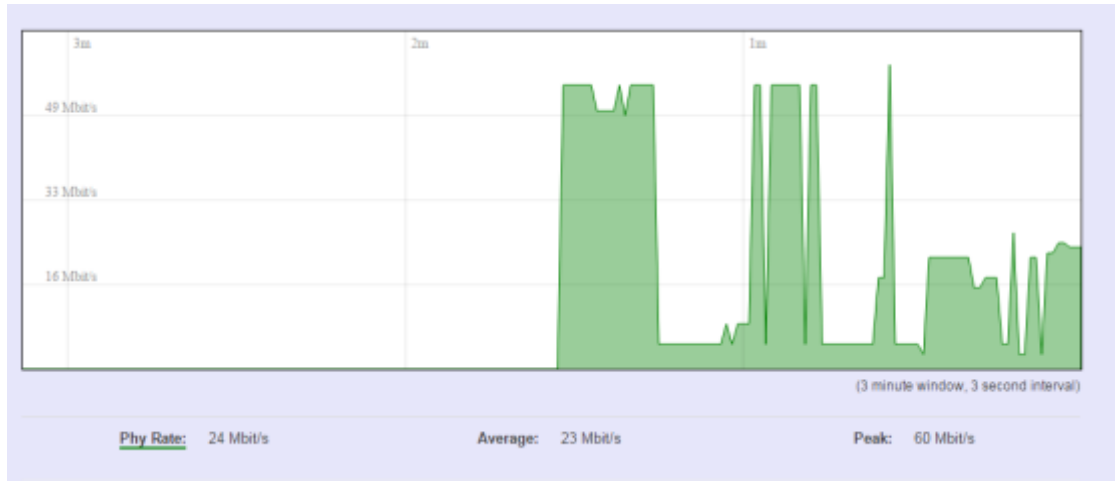
Display NIO200 real-time traffic loading of Ethernet, WLAN and internal bridge interfaces.

**Inbound:** Incoming data throughput of the observed interface.

**Outbound:** Outgoing data throughput of the observed interface.

## Wireless





Display Wireless real-time signal quality including signal level, noise and data rate.

**wlan0:** Radio0 information.

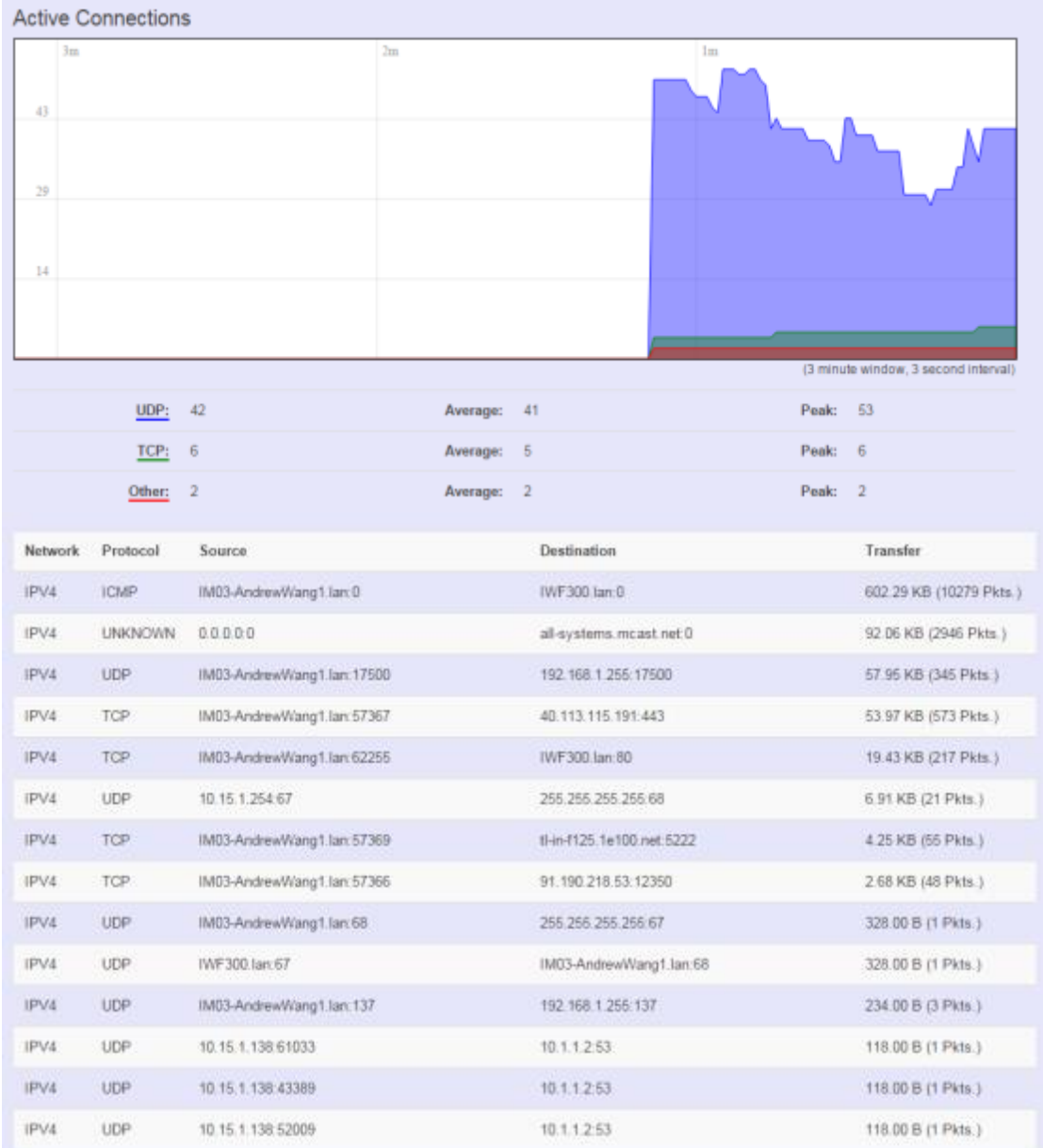
**wlan1:** Radio1 information.

Note:

There will be no radio information when the WLAN interface is disabled.

## Connections

This “Connections” displays NIO200 real-time active TCP/UDP/ICMP,... connection information for trouble shooting reference.



## 3. System

To setup detail configuration about NIO200 system, click the “System” under the page bar, then select the item of System, Administration, SNMP, Backup/Flash Firmware and Reboot from the pull-down list like below screen.

### 3.1 System General Settings

This section provide general settings of NIO200 including Time, Host name, Time zone and NTP.

**System**  
Here you can configure the basic aspects of your device like its hostname or the timezone.

**System Properties**

General Settings | Logging | Language and Style

Local Time: Tue Jan 5 02:04:39 2015

Hostname: IWF300

Timezone: UTC

**Time Synchronization**

Enable NTP client

Provide NTP server

NTP server candidates:

- 0.openwrt.pool.ntp.org
- 1.openwrt.pool.ntp.org
- 2.openwrt.pool.ntp.org
- 3.openwrt.pool.ntp.org

Click “Sync with browser” let NIO200 sync time with your computer. And select country from the pull-down list in the Timezone.

**System Properties**

General Settings | Logging | Language and Style

Local Time: Thu Nov 8 14:27:56 2018

Hostname: NIO200

Timezone: Asia/Taipei

To make NIO200 system get time synchronization with NTP server, user may enable the NTP client and input the address of an NTP server to get the time updates.

### Time Synchronization

Enable NTP client

Provide NTP server

NTP server candidates

0.openwrt.pool.ntp.org	✖
1.openwrt.pool.ntp.org	✖
2.openwrt.pool.ntp.org	✖
3.openwrt.pool.ntp.org	+

## Logging

This section provides the setting of log configuration.

### System Properties

General Settings **Logging** Language and Style

System log buffer size   
 ⓘ kiB

External system log server

External system log server port

Log output level  ▼

Cron Log Level  ▼

**System log buffer size:** The size of log information. Unit: Kbytes.

**External system log server:** The server address of external log server.

**External system log server port:** The port number of external log server.

**Log output level:** The output information of log, including Debug, Info, Notice, Warning, Error, Critical, Alert, and Emergency.

**Cron Log Level:** The minimal level for cron messages to be logged to syslog.

## Language and Style

This section provides setting of language and WebUI style. NIO200 only provides English as default style.



## System Properties

General Settings

Logging

Language and Style

Language

auto



Design

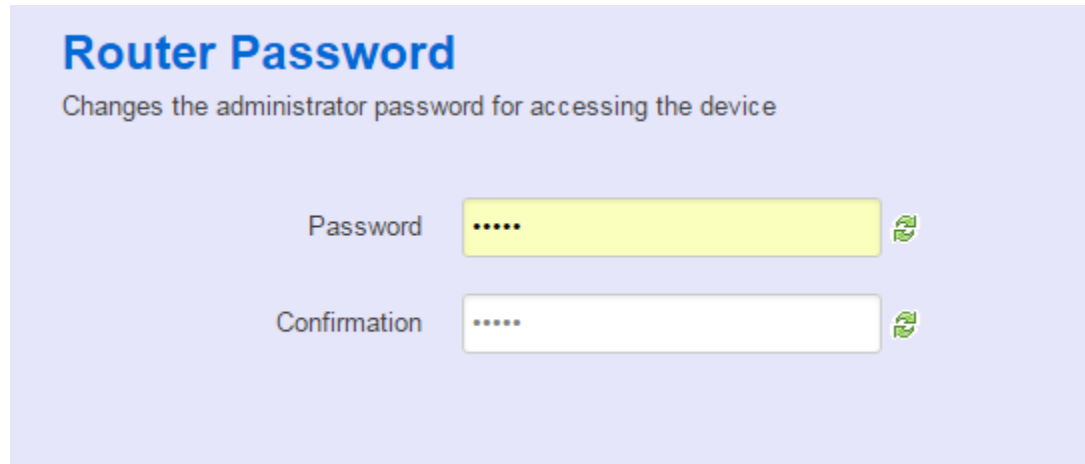
Bootstrap




## 3.2 Administration


### Router Password

To change default password, enter new password and confirm new one.



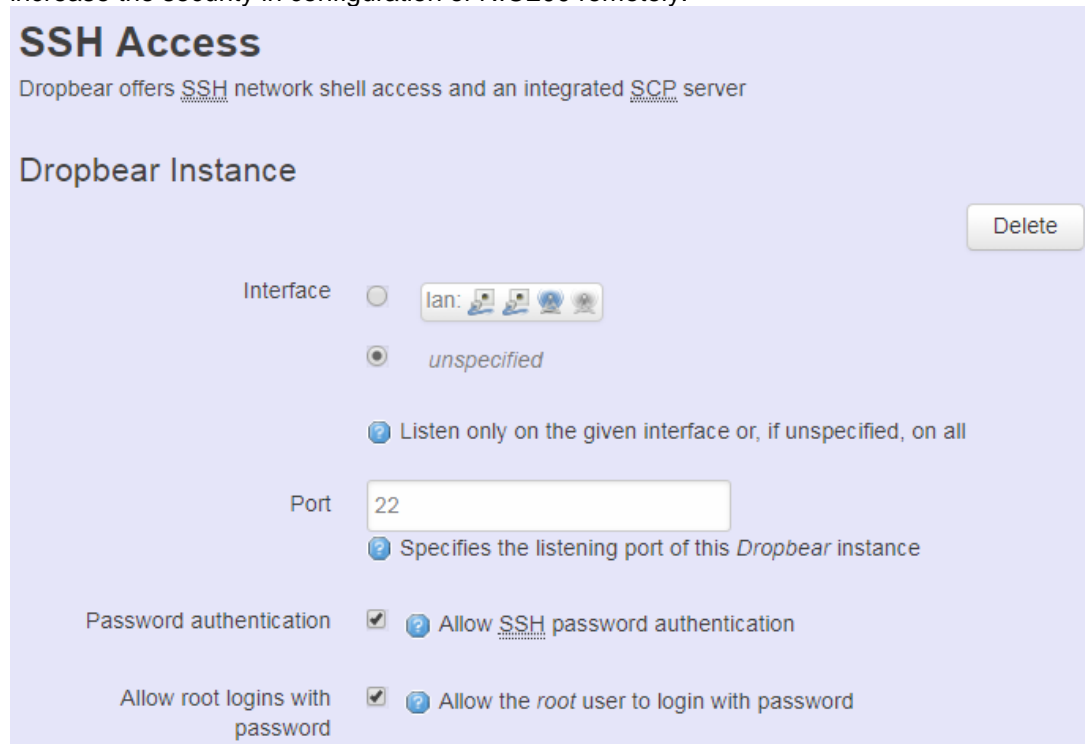
**Router Password**  
Changes the administrator password for accessing the device

Password  

Confirmation  


### SSH Access

Secure Shell(SSH). Enable NIO200 to be accessed via SSH-based application. This increase the security in configuration of NIO200 remotely.




**SSH Access**  
Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server


Dropbear Instance Delete

Interface  lan:   unspecified

Listen only on the given interface or, if unspecified, on all

Port    
 Specifies the listening port of this *Dropbear* instance

Password authentication   Allow [SSH](#) password authentication

Allow root logins with password   Allow the *root* user to login with password

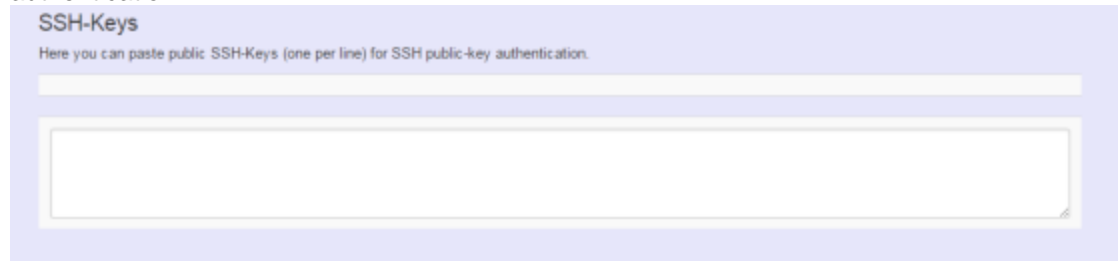
**Interface:** Select the interface.

**Port:** Enter the port number for the communication via SSH.

**Password authentication:** Enable/Disable SSH password authentication.

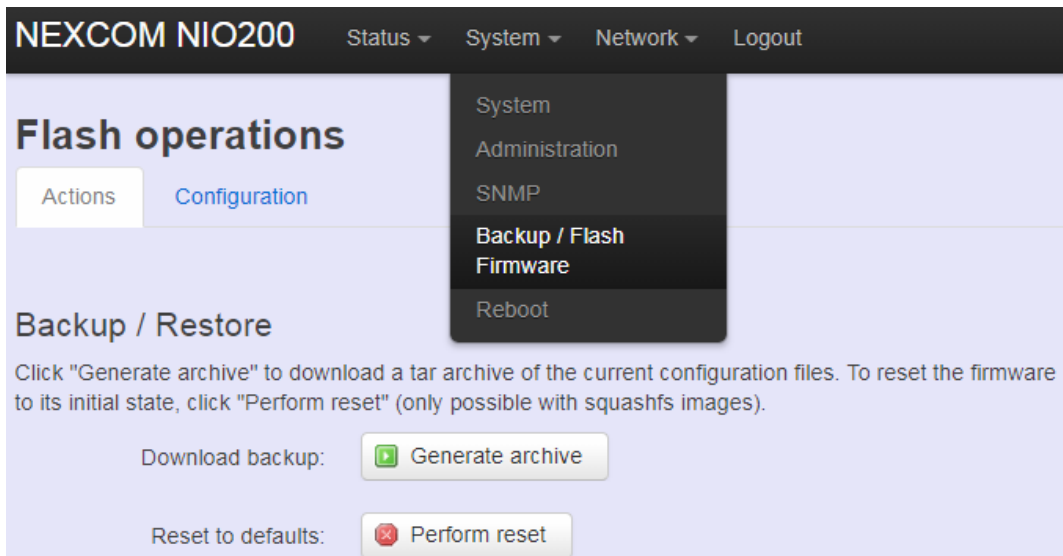
**Allow root logins with password:** Enable/Disable the *root* user to login with password.

User may paste the public SSH-Keys (one per line) for additional SSH public-key authentication.



### 3.3 Backup/Flash Firmware

To **upgrade** new firmware on device, user may choose “Backup/Flash Firmware” from “Systeme” in tool bar as below:

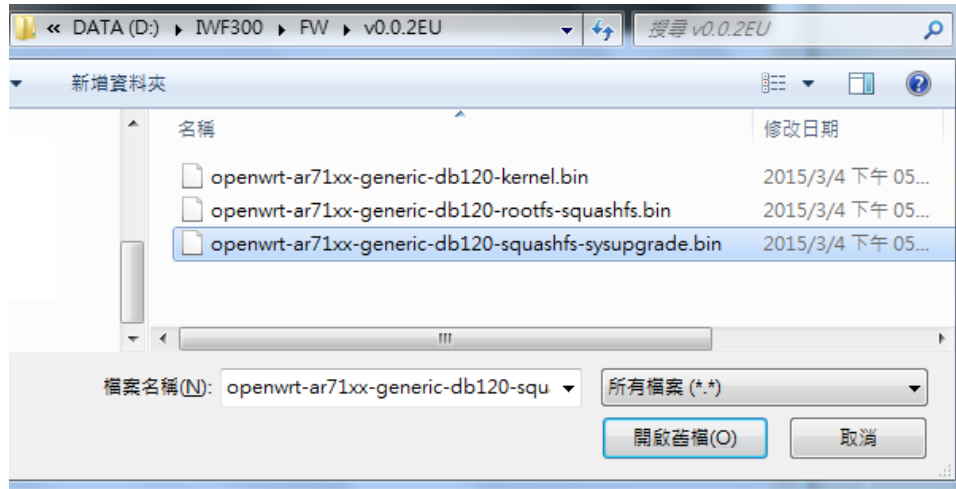


### Upgrade Firmware

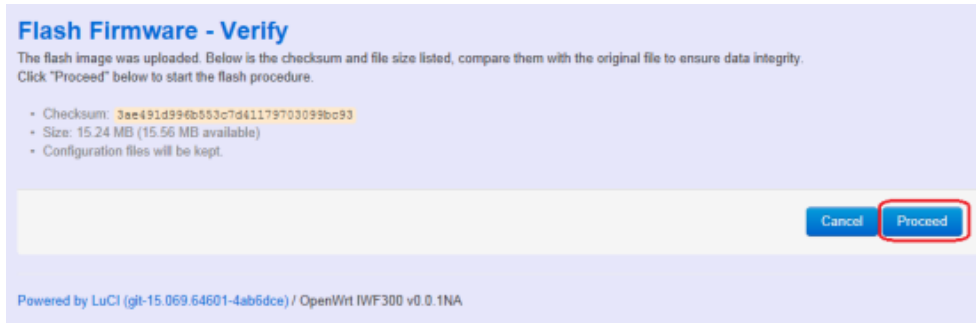
To flash a new firmware image to NIO200, user may press the button of “Flash image” as below:



Then select the correct firmware file from the file browser:

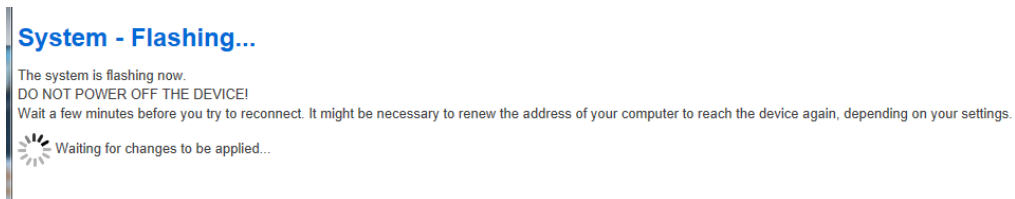


Then, WebUI displays the file checksum.



You can choose "Proceed" to start the upgrading.

**Note:** After you click "Proceed", the DUT firmware will be upgraded with the file you selected, and the upgrade progress will display like below:

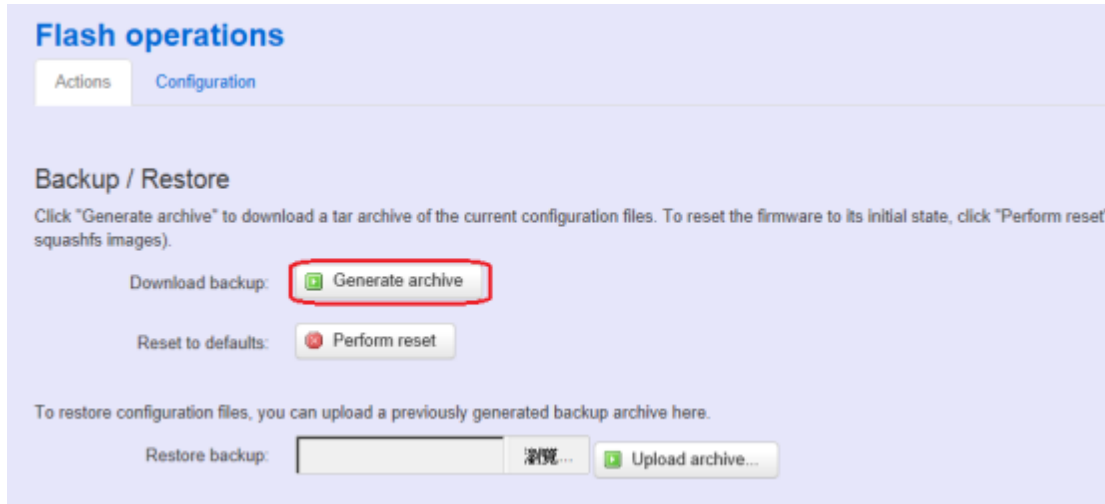


**Note:** The whole firmware image may take several minutes to complete the flash writing. **PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole progress.

If the firmware upgrade is successful, the WebUI should switch to the Login page. User can also confirm the firmware image is successfully upgraded via “Status” Web page.

## Backup Configuration

To back up the configuration file, user may select the “Generate archive” button as below:



Then save it as a file in your PC.

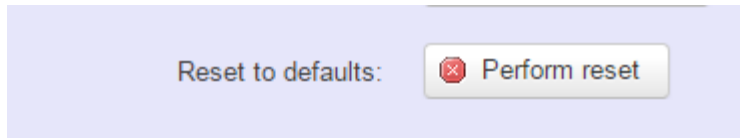
To restore previous configuration, user need to browse the backup file and then press “Upload archive...” button as below:



**Note:** After restore the file, system will apply the changes and automatically reboot. Due to configuration backup may cause IP address change, you have to enter new IP address accordingly. Otherwise, the new web page may not be accessible.

## Reset to default

To reset NIO200 to factory default configuration, user will need to press “Perform reset” button as below.

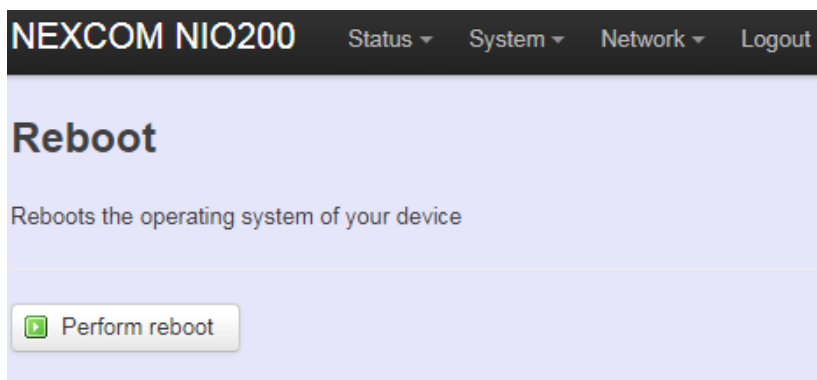


**Note:** The whole process may take several minutes to complete.

**PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole process being successfully done.

### 3.4 Reboot

Click the “Perform reboot” button will help to warm start the system. After system finish reboot process, it will back to Login page.

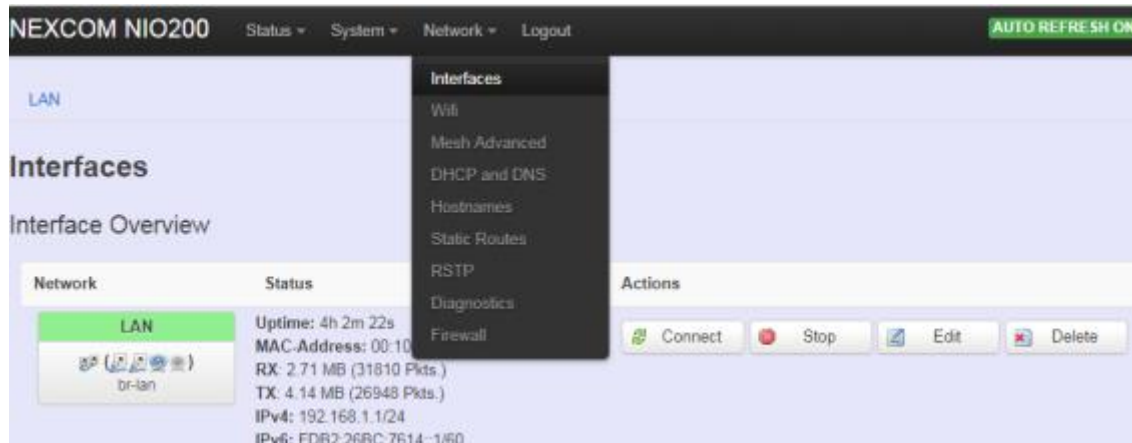


# 4 Network

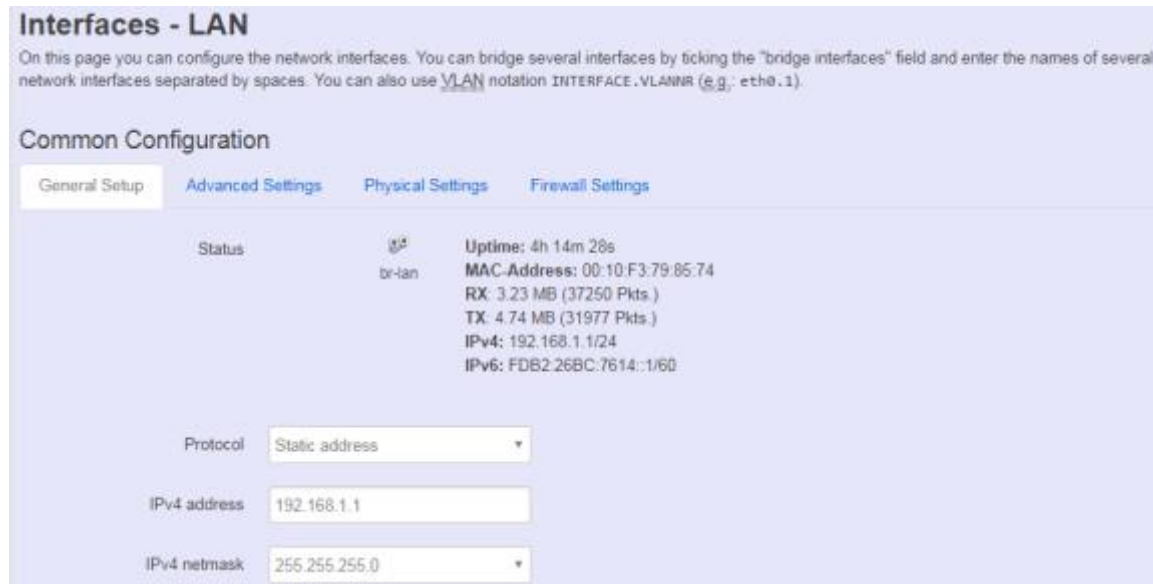
## 4.1 Interfaces

### Configuration of IP address

To set up a new IP address, please click “Network” from page bar, then select the “Interface”, and then click “Edit”



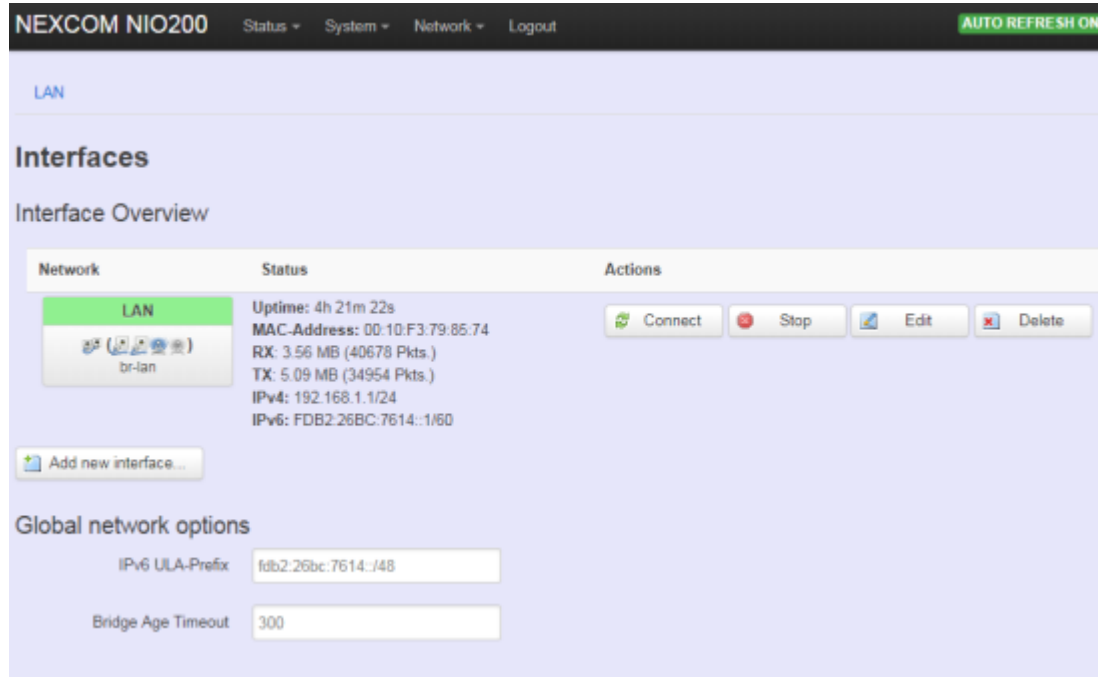
Edit IP address:



When modifying the IP address, user needs to input the IP address, netmask, gateway,.. for this device and then click “Save & Apply” to save this new IP address into flash and apply it immediately.

**Note:** after apply new IP, it would take several minutes to switch to the Status page via the new IP address. Please enter the new IP address on browser again if the browser does not switch to new Web page after 5 minutes.

## Interfaces overview



The screenshot shows the NEXCOM NIO200 web interface. At the top, there is a navigation bar with 'Status', 'System', 'Network', and 'Logout' menus, and an 'AUTO REFRESH ON' button. The main content area is titled 'LAN' and 'Interfaces'. Below this, there is an 'Interface Overview' section. A table lists the network interfaces, with 'LAN' selected. The table has columns for 'Network', 'Status', and 'Actions'. The 'LAN' interface is shown with its status and various actions. Below the table, there is an 'Add new interface...' button and a 'Global network options' section with input fields for 'IPv6 ULA-Prefix' and 'Bridge Age Timeout'.

Network	Status	Actions
LAN br-lan	Uptime: 4h 21m 22s MAC-Address: 00:10:F3:79:85:74 RX: 3.56 MB (40678 Pkts.) TX: 5.09 MB (34954 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDB2:26BC:7614::1/60	Connect Stop Edit Delete

Global network options

IPv6 ULA-Prefix: fdb2:26bc:7614::/48

Bridge Age Timeout: 300

**Connect:** Press this button to re-connect LAN interface to Ethernet network.

**Stop:** Shutdown this interface.

**Edit:** Modify WAN port setting or LAN port group settings

**Delete:** Delete this Interfaces from group

### Note:

- Do not perform "Stop" LAN interface when this is the only available interface, otherwise, the system will not be able to work.
- Under such condition, please press the button longer than 10 sec. to get system back to factory default setting. User can go on the configuration with default IP address "192.168.1.1".

## WAN(LAN) Interface overview

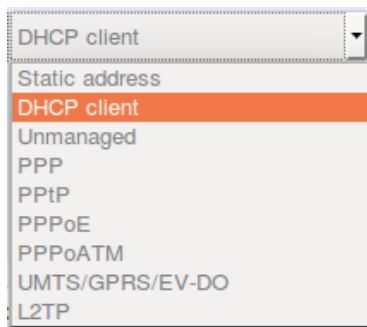
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces.





### <General Setup>

You can change your Protocol to link worldwide Internet.



The default setting is DHCP client, send discover to find DHCP server.

#### **Static address**

Static IP (Manual):. Choose this option if you do not have a DHCP server in your network, or if you wish to assign a static IP address to NIO200HAG

#### **DHCP client**

When Dynamic IP (DHCP) is selected, the DHCP client to be functional once this selection is made

#### **Unmanaged**

This Interface have no configuration interface or options.

#### **PPP**

For old serial modem, provided point to point link for NIO200HAG

#### **PPPoE**

For cable modem or ADSL user, link NIO200HAG to your Internet provider.

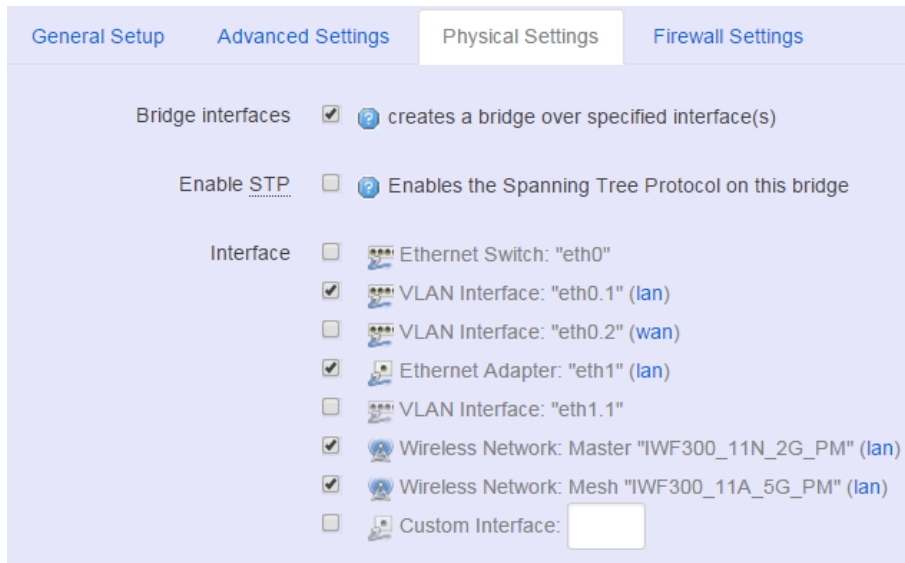
### <Advanced Settings>

This is used for advanced settings and configure, strongly recommend user do not make change to this web page.

Bring up on boot	<input checked="" type="checkbox"/>
Use builtin IPv6-management	<input checked="" type="checkbox"/>
Use broadcast flag	<input type="checkbox"/> <a href="#">?</a> Required for certain ISPs, e.g. Charter with DOCSIS 3
Use default gateway	<input checked="" type="checkbox"/> <a href="#">?</a> If unchecked, no default route is configured
Use DNS servers advertised by peer	<input checked="" type="checkbox"/> <a href="#">?</a> If unchecked, the advertised DNS server addresses are ignored
Use gateway metric	<input type="text" value="0"/>
Client ID to send when requesting DHCP	<input type="text"/>
Vendor Class to send when requesting DHCP	<input type="text"/>
Override MAC address	<input type="text" value="00:00:00:00:00:00"/>
Override MTU	<input type="text" value="1500"/>

### <Physical Settings>

etup	Advanced Settings	Physical Settings	Firewall Settings
Bridge interfaces	<input type="checkbox"/>	<a href="#">?</a> creates a bridge over specified interface(s)	
Interface	<input type="radio"/>	Ethernet Switch: "eth0"	
	<input type="radio"/>	VLAN Interface: "eth0.1" (lan)	
	<input checked="" type="radio"/>	VLAN Interface: "eth0.2" (wan)	
	<input type="radio"/>	Ethernet Adapter: "eth1" (lan)	
	<input type="radio"/>	VLAN Interface: "eth1.1"	
	<input type="radio"/>	Wireless Network: Master "IWF300_11N_2G_PM" (lan)	
	<input type="radio"/>	Wireless Network: Mesh "IWF300_11A_5G_PM" (lan)	
	<input type="radio"/>	Custom Interface: <input type="text"/>	



### Bridge interfaces

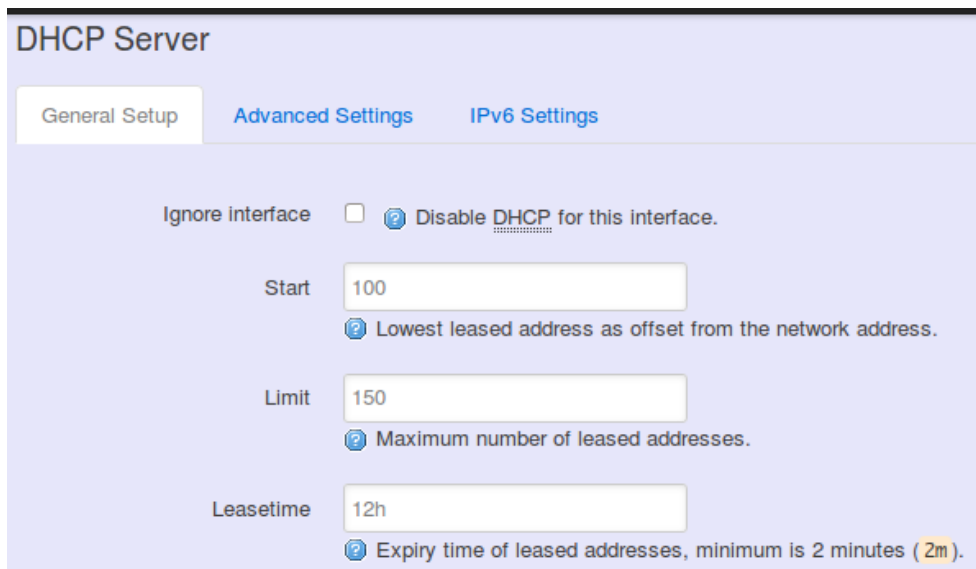
You can bridge an interfaces group for your WAN or LAN interface. Normally, only LAN interface need to enable bridge interfaces. After enable bridge interfaces, select interfaces to bridge.

### Interface

Select interfaces for your bridge group. Select both the Ethernet adapter ( most likely eth0.1' eth1) and the wireless network.

### DHCP Server

<General Setup>



**Ignore Interface:** Select this option to disable your DHCP server, you will need static IP or another DHCP server for your network interfaces. Default is “enable DHCP”

### <Advanced Settings>



The screenshot shows the 'DHCP Server' configuration page with three tabs: 'General Setup', 'Advanced Settings' (selected), and 'IPv6 Settings'. Under 'Advanced Settings', there are four main sections:

- Dynamic DHCP:** A checkbox is checked. Description: "Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served."
- Force:** A checkbox is unchecked. Description: "Force DHCP on this network even if another server is detected."
- IPv4-Netmask:** An empty text input field. Description: "Override the netmask sent to clients. Normally it is calculated from the subnet that is served."
- DHCP-Options:** An empty text input field with a help icon. Description: "Define additional DHCP options, for example '6,192.168.2.1,192.168.2.2' which advertises different DNS servers to clients."

**Dynamic DHCP:** Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.

**Force:** Force DHCP on this network even if another server is detected.

## 4.2 Wi-Fi

### Wireless Overview

The screenshot displays the 'Wireless Overview' section of a network management interface. At the top, three radio interfaces are listed: 'radio0: Mesh "Test"', 'radio0: Mesh "backbone"', and 'radio1: Mesh "MESH\_CAN4"'. Below this, the 'Wireless Overview' section is divided into two main parts: 'Generic MAC80211 802.11an (radio0)' and 'Generic MAC80211 802.11an (radio1)'. Each part shows the current configuration for a radio interface, including SSID, Mode, MAC, BSSID, and Encryption. For 'radio0', two configurations are shown: one for 'backbone' (disabled) and one for 'Test' (enabled). For 'radio1', one configuration for 'MESH\_CAN4' (enabled) is shown. Each configuration has buttons for 'Scan', 'Add', 'Disable', 'Enable', 'Edit', and 'Remove'. Below the radio configurations is the 'Associated Stations' section, which contains a table with columns for SSID, MAC-Address, IPv4-Address, Signal, Noise, RX Rate, and TX Rate. One station is listed with SSID 'backbone', MAC-Address '00-10-F3-6E-E6-A0', and various performance metrics.

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
backbone	00-10-F3-6E-E6-A0	?	-68 dBm	-92 dBm	43.3 Mbit/s, MCS 10, 20MHz	72.2 Mbit/s, MCS 7, 20MHz

To set up the Wireless configuration, please select “Network” in the tab , then select “Wi-Fi”, which would show you the current radio interfaces status.

Wireless Overview includes channel' SSID' MAC address and security setting information.

**Scan:** Scan can explore how many AP signals can be detected. This is a good way to get the idea about how noisy the installation site is. User can choose a channel which is less interference with other APs.

The screenshot shows the 'Join Network: Wireless Scan' interface. It lists four detected APs with their signal strength, SSID, Channel, Mode, BSSID, and Encryption. The APs are: NEXCOM\_2.4G (92% signal), O2O4 (62% signal), 168 (75% signal), and NEXCOM\_2.4G (48% signal). Each entry includes the channel, mode, BSSID, and encryption type.

Signal	SSID	Channel	Mode	BSSID	Encryption
92%	NEXCOM_2.4G	1	Master	00 10 F3 32 7C 6F	WPA2 - 802.1X
62%	O2O4	1	Master	84 C9 B2 6B 4D B2	WPA2 - PSK
75%	168	1	Master	B4 B3 62 C2 A0 7D	WPA2 - PSK
48%	NEXCOM_2.4G	1	Master	00 10 F3 32 7B 7F	WPA2 - 802.1X

**Add:** Add new virtual AP in the same radio interface. You will see new interface after click “add”



**Disable:** Disable the radio interface

**Edit:** Configure the radio interface

**Remove:** Remove radio interface. Please note that disable radio first when you don't want to use the radio interface.

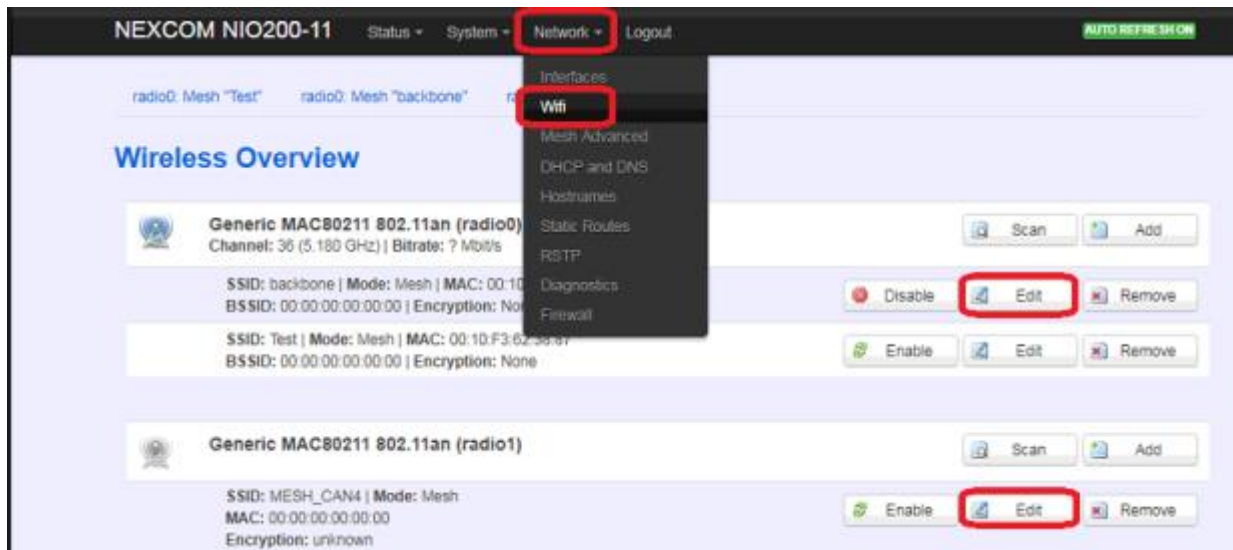
## Associated Stations

Associated stations show wireless client connection information. It includes the SSID wireless client connect' wireless client MAC/ IP address' RSSI signal strength and Tx/Rx rate.

Associated Stations						
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
IWF300_11N_2G_PM	9C:2A:70:1B:4C:9D	192.168.1.215	-53 dBm	-93 dBm	162.0 Mbit/s, MCS 12, 40MHz	104.0 Mbit/s, MCS 13, 20MHz

## Wireless configuration

Please select "network" -> "Wi-Fi" and click Edit to configure Radio0 or Radio1.



The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power...etc.

### Device Configuration

General Setup **Advanced Settings**

Status **Mode:** Master | **SSID:** IWF300\_11N\_2G\_PM  
 81% **BSSID:** 00:10:F3:30:8A:22 | **Encryption:** WPA PSK (TKIP, CCMP)  
**Channel:** 7 (2.442 GHz) | **Tx-Power:** 20 dBm  
**Signal:** -53 dBm | **Noise:** -93 dBm  
**Bitrate:** 300.0 Mbit/s | **Country:** US

Wireless network is enabled

Operating frequency  
 Mode: N | Channel: auto | Width: 40 MHz(AP or Client mode)

Transmit Power: 20 dBm (100 mW)

**<General setup>**

**Wireless network is enabled: Enable or disable the radio interface**

**Operating frequency: Select radio frequency and channel bandwidth for signal transmission.**

**For channel bandwidth, please note you need to confirm AP/ client mode or mesh mode and which channel you will use**

Width

- 40 MHz(AP or Client mode)
- 20 MHz(AP or Client mode)
- 40 MHz(AP or Client mode)
- 40 plus MHz(Mesh mode,2.4G(ch <= 6),5G(ch=36,40,44,149)
- 40 minus MHz(Mesh mode,2.4G(ch >= 7),5G(ch=48,153,157,161,165)

**Transmit Power: Control the transmit power of a radio by selection of Transmission Power.**

**<Advanced settings>**

radio0: Mesh "test" radio0: Mesh "backbone" radio1: Mesh "MESH\_CAN4"

### Wireless Network: Mesh "backbone" (wlan0)

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.

Device Configuration

General Setup **Advanced Settings**

Country Code: US - United States  
 Use IEEE 3166 alpha2 country codes.

Distance Optimization:   
 Distance to farthest network member in meters

Fragmentation Threshold:

RTS/CTS Threshold:

Transmitter/Receiver Antenna:  1Tx1R  2Tx2R

**Distance Optimization:** Specify the ACK timeout by entering the value manually. ACK timeout can be entered by defining the link distance. Too short value of the ACK timeout may cause transmission time out and no packet can be received. Too long value may cause low throughput rate.

**Fragmentation Threshold:** Default=off. Specify the Fragmentation threshold by entering the value manually [300-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended

**RTS/CTS Threshold:** Default=off. RTS/CTS (Request to Send / Clear to Send) is the optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem. RTS/CTS is an additional method to implement virtual carrier sensing in Carrier sense multiple access with collision avoidance (CSMA/CA). Specify the RTS threshold by entering the value manually [0-2346 bytes]. Typically, sending RTS/CTS frames does not occur unless the packet size exceeds this threshold.

This Interface Configuration section covers SSID' operation mode and encryption.

The screenshot displays the configuration page for the NEXCOM NIO200-11 device. At the top, there are navigation links for Status, System, Network, and Logout, along with an AUTO REFRESH ON button. The main configuration area includes fields for Distance Optimization, Fragmentation Threshold, and RTS/CTS Threshold, each with a help icon and a description. Below these is a Transmitter/Receiver Antenna section with radio buttons for 1Tx1R and 2Tx2R. The Interface Configuration section is expanded to show the General Setup tab, which contains fields for ESSID/Mesh ID (set to 'backbone'), Mode (set to 'Mesh\_802.11s'), and Network (set to 'lan'). A 'create' field is also present for defining a new network. A note at the bottom of the Interface Configuration section states: 'Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.'

### <General setup>

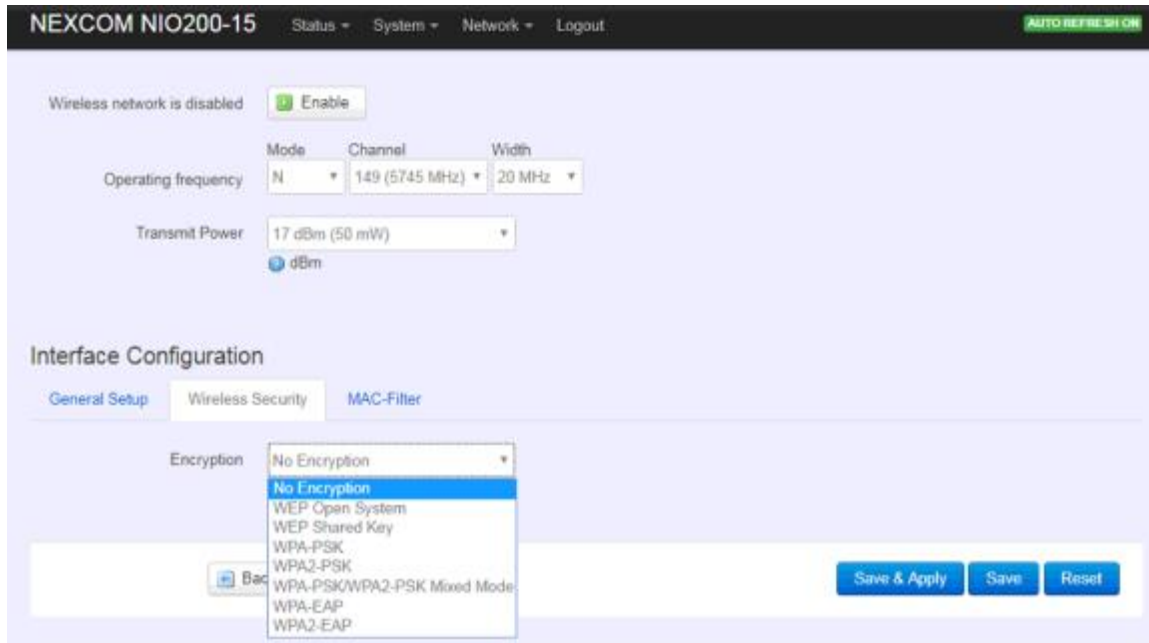
**ESSID:** Edit the SSID or Mesh ID.

**Mode:** Select operation mode

- AP
- Client Router
- 802.11s ( Mesh mode)

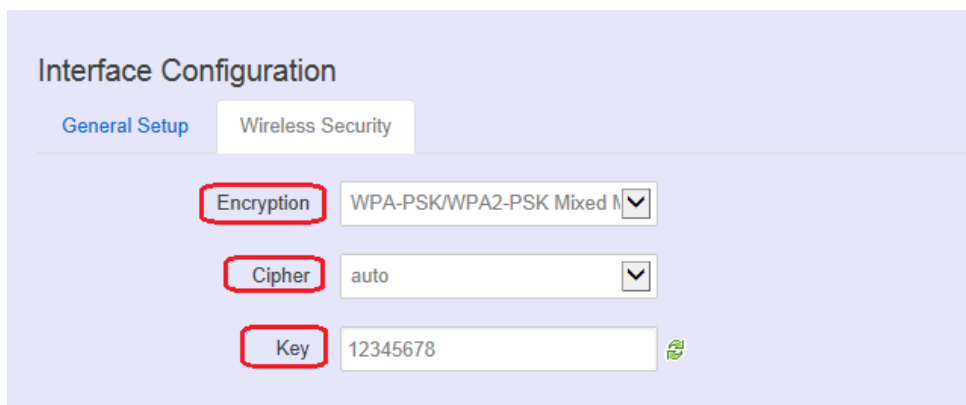
### <Wireless Security>





**Encryption:** To setup the Security on Radio, please select one of the Encryption:

- No Encryption
- WEP Open System: WEP provides a basic level of security, preventing unauthorized access to the network. WEP uses static shared keys that are manually distributed to all clients that want to use the network
- WEP Shared Key: WEP provides a basic level of security, preventing unauthorized access to the network, and encrypting data transmitted between wireless clients and an access point. WEP uses static shared keys that are manually distributed to all clients that want to use the network
- WPA-PSK: Clients using WPA for authentication
- WPA2-PSK: Clients using WPA2 for authentication
- WPA-PSK/WPA2-PSK Mixed Mode: Clients using WPA or WPA2 for authentication



**Cipher :** To select cipher, recommend to select TKIP and CCMP(AES)

- Force CCMP(AES)
- Force TKIP
- Force TKIP and CCMP(AES)

Encryption WPA-PSK/WPA2-PSK Mixed N

Cipher Force TKIP and CCMP (AES)

Key 12345678 

The cycle icon will display the characters you just input.

**<MAC filter>**

Interface Configuration

General Setup Wireless Security MAC-Filter

MAC-Address Filter Allow listed only

MAC-List disable Allow listed only Allow all except listed

Select MAC Filtering. Specifies the MAC address to block or allow traffic from.

## Mesh Advanced

Mesh Advanced setting contains the important information about real Mesh connection path and Neighbor node signal strength and blocking status. This is an advanced mechanism to keep Mesh network in stable and optimized condition.

radio0: Mesh "backbone"    radio1: Mesh "MESH\_CAN4"

### Mesh Advanced Settings

Block RSSI threshold:   
0: Disable, -60 ~ -90(dBm). Enter RSSI threshold to set blocking criteria of existing mesh points.

Block/Reopen Sensitivity:  High(2 secs)  Medium(5 secs)  Low(10 secs)

Whitelist (MAC addr):   
Add whitelist by MAC address (ex: 00-AA-BB-11-22-33). The data of mesh point will always be forwarded even though the Wi-Fi Signal lower than Block RSSI threshold.

Blacklist (MAC addr):   
Add blacklist by MAC address (ex: 00-AA-BB-11-22-33). The data of mesh point will never be forwarded by the blacklist.

### Mesh Neighbor Table

MAC-Address	iface	Inactive time	Signal	State	Type
00:10:F3:6E:E6:A2	wlan0	944 ms	-82 dBm	BLOCKED	Auto block

- Block RSSI threshold: This is used to set the threshold of blocking current associated Mesh points.
  - 0: Disable
  - Input value between -60 ~ -90 (dBm)
- Block/Reopen Sensitivity: This is a criteria for choosing the sensitivity level in Mesh path availability.
  - High:
    - After continuous 2 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
    - After continuous 2 seconds with signal level lower than Block threshold, the active Mesh link will be blocked.
  - Medium:
    - After continuous 5 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
    - After continuous 5 seconds with signal level lower than Block threshold, the active Mesh link will be blocked.
  - Low:
    - After continuous 10 seconds with signal level higher than Block threshold, the blocked Mesh link can be available again.
    - After continuous 10 seconds with signal level lower than Block threshold, the active Mesh link will be blocked.
- Whitelist (MAC addr):

The Mesh device in Whitelist will be regarded available connecting path for data forwarding no matter the RSSI value is high or low.

- Blacklist (MAC addr):

The Mesh device in Blacklist will NOT be used for data forwarding no matter the RSSI value is high or low.

- Mesh Neighbor Table

Mesh Neighbor Table					
MAC-Address	iface	Inactive time	Signal	State	Type
00:10:F3:6E:E6:A2	wlan0	828 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:B6	wlan0	288 ms	-81 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:A0	wlan0	8 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:62:38:87	wlan0	96 ms	-65 dBm	ESTAB	Normal
00:10:F3:77:28:5D	wlan0	116 ms	-79 dBm	BLOCKED	Auto block
00:10:F3:6E:E6:9C	wlan0	512 ms	-80 dBm	BLOCKED	Auto block
00:10:F3:62:38:81	wlan0	324 ms	-68 dBm	ESTAB	Normal
00:10:F3:6D:48:B4	wlan0	872 ms	-85 dBm	BLOCKED	Auto block

- Iface: display the Mesh interface used in the Wi-Fi radio
- Inactive time: the elapsed time since last forward data by the according Mesh path.
  - Shorter inactive time implies more frequently used in data forwarding by Mesh network.
  - Too long inactive time means the Mesh path is almost un-used.
- Signal: display the dynamic RSSI signal strength when refresh
- State: display the current status is ESTAB ( established ) or BLOCKED ( blocked ). When BLOCKED, implies the signal strength is too low to use in data forwarding.

Mesh Path Table		
Dest addr	Next hop	iface
00:10:F3:62:38:87	00:10:F3:62:38:87	wlan0
00:10:F3:62:38:81	00:10:F3:62:38:81	wlan0
00:10:F3:6E:E6:9C	00:10:F3:62:38:81	wlan0

- Dest addr/Next hop:

When Dest (Destination) MAC address and Next hop MAC address is the same, the destination is available to connect directly from source Mesh node.

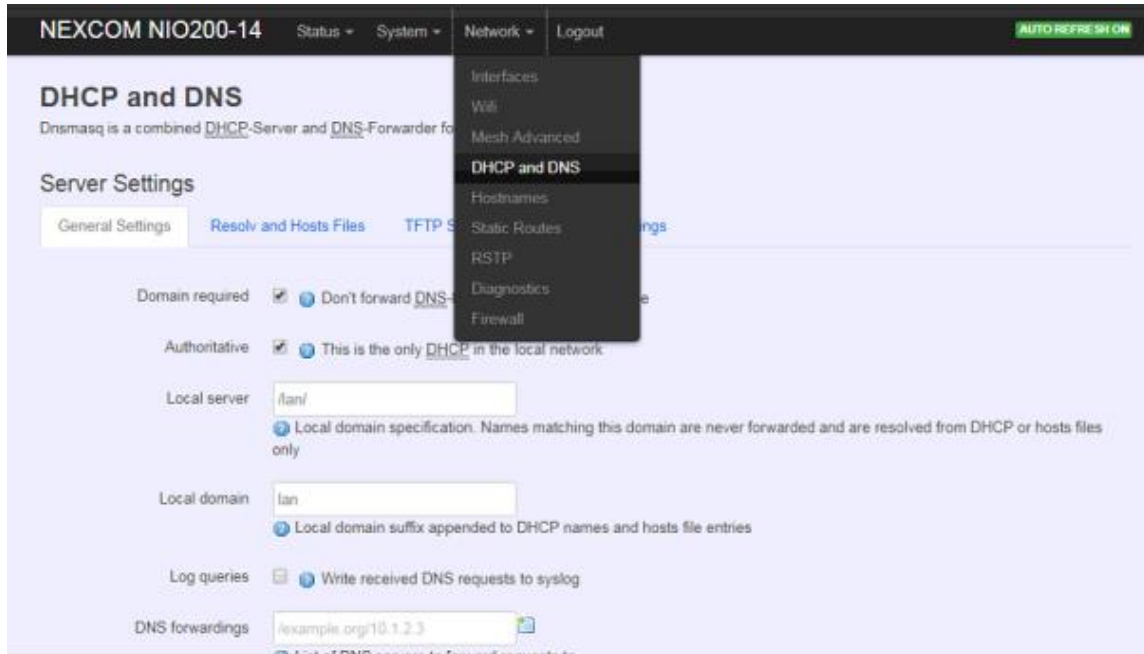
When the two MAC address is different, the data forwarding to Destination MAC address should be routed via Next hop path.

- Iface: display the Mesh interface used in the Wi-Fi radio

## 4.3 DHCP and DNS

A combined DHCP-Server and DNS-Forwarder for NAT firewall is provided in NIO200HAG.

Click the “Network” -> “DHCP and DNS” in the GUI menu. The “DHCP and DNS” page will appear. There are four categories of settings or lease status: “Active DHCP Leases”, “Active DHCPv6 Leases”, “Static Leases”, and “Server Settings”.



Scroll to the following screen in the “DHCP and DNS” window.



This screen displays the lease information to which DHCP server assigns automatically, including **Hostname**, **IP address**, **MAC address(or DUID)**, and Remaining Lease-time (DUID stands for the DHCP Unique Identifier). Please look at the frame in red above.

The next category that users can scroll to is “Static Leases” as follows.

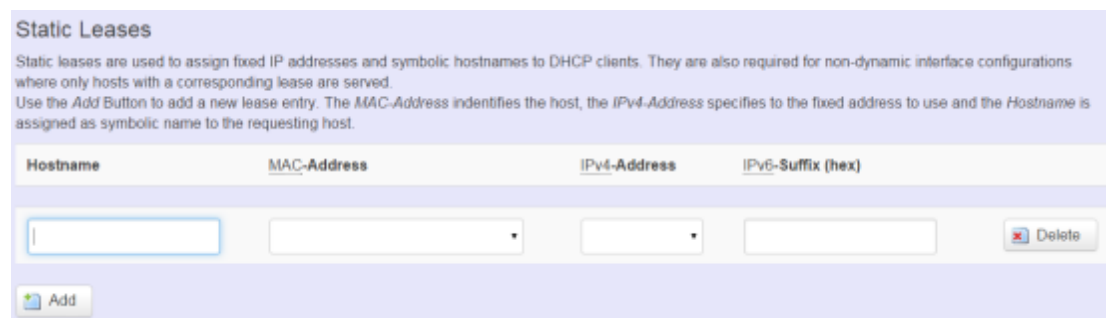
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients by calculating MAC-Address. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.



The screenshot shows the 'Static Leases' configuration page. At the top, there is a title 'Static Leases' and a descriptive paragraph: 'Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.' Below this is a table with four columns: 'Hostname', 'MAC-Address', 'IPv4-Address', and 'IPv6-Suffix (hex)'. The table is currently empty, with the text 'This section contains no values yet' below it. At the bottom left, there is an 'Add' button with a red arrow pointing to it.

**Add:** Add a new lease entry.

After clicking “Add” button, a new entry with 4 blank input boxes will appear. Allow users to fill in the information such as The **MAC-Address** (identifies the host), the **IPv4-Address** (specifies the fixed address to use) and the **Hostname** (is assigned as symbolic name to the requesting host).



The screenshot shows the 'Static Leases' configuration page after clicking the 'Add' button. The table now has one row with four input fields: 'Hostname', 'MAC-Address', 'IPv4-Address', and 'IPv6-Suffix (hex)'. A 'Delete' button is located to the right of the input fields. Below the table, there is an 'Add' button.

**Delete:** delete the followed entry.

Scroll to the screen identified as “Server Settings” category.

There are 4 tabs to select more options for DHCP and DNS services in the NIO200HAG.

## General Settings

Server Settings

General Settings | [Resolve and Hosts Files](#) | [TFTP Settings](#) | [Advanced Settings](#)

Domain required  [Don't forward DNS-Requests without DNS-Name](#)

Authoritative  [This is the only DHCP in the local network](#)

Local server   
[Local domain-specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only](#)

Local domain   
[Local domain suffix appended to DHCP names and hosts file entries](#)

Log queries  [Write received DNS requests to syslog](#)

DNS forwardings   
[List of DNS servers to forward requests to](#)

Rebind protection  [Discard upstream RFC1918 responses](#)

Allow localhost  [Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services](#)

Domain whitelist   
[List of domains to allow RFC1918 responses for](#)

**Domain required:** default value is checked.

**Authoritative:** default value is checked.

## Resolve and Hosts Files

Server Settings

[General Settings](#) | [Resolve and Hosts Files](#) | [TFTP Settings](#) | [Advanced Settings](#)

Use `/etc/ethers`  [Read /etc/ethers to configure the DHCP-Server](#)

Leasefile   
[file where given DHCP-leases will be stored](#)

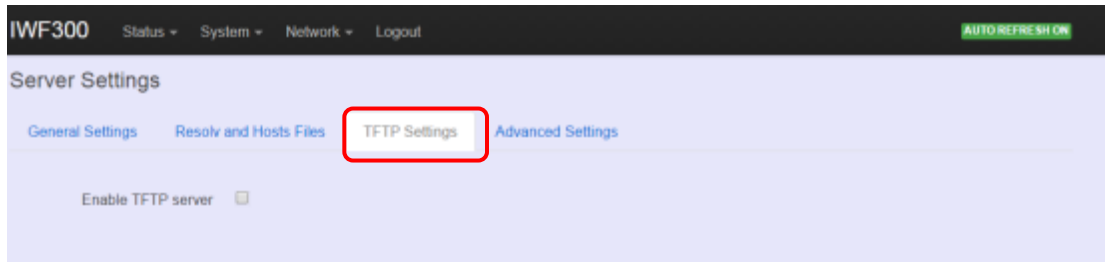
Ignore resolve file

Resolve file   
[local DNS file](#)

Ignore `/etc/hosts`

Additional Hosts files

# TFTP Settings



By default, TFTP server is not enabled.



## 4.4 Advanced Settings

**NEXCOM NIO200-14** Status System Network Logout AUTO REFRESH ON

### Server Settings

General Settings | **Resolve and Hosts Files** | TFTP Settings | **Advanced Settings**

- Filter private**  Do not forward reverse lookups for local networks
- Filter useless**  Do not forward requests that cannot be answered by public name servers
- Localise queries**  Localise hostname depending on the requesting subnet if multiple IPs are available
- Expand hosts**  Add local domain suffix to names served from hosts files
- No negative cache**  Do not cache negative replies, e.g. for not existing domains
- Additional servers file**   
This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.
- Strict order**  DNS servers will be queried in the order of the resolvfile
- Bogus NX Domain Override**   
List of hosts that supply bogus NX domain results

- DNS server port**   
Listening port for inbound DNS queries
- DNS query port**   
Fixed source port for outbound DNS queries
- Max. DHCP leases**   
Maximum allowed number of active DHCP leases
- Max. EDNS0 packet size**   
Maximum allowed size of EDNS0 UDP packets
- Max. concurrent queries**   
Maximum allowed number of concurrent DNS queries

#### Active DHCP Leases

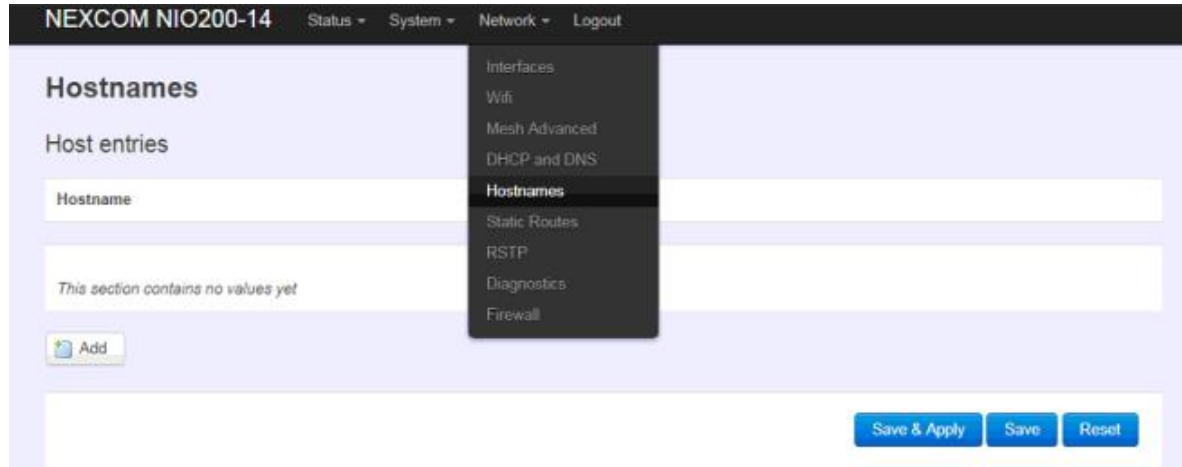
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
----------	--------------	-------------	---------------------

**Max. DHCP Leases:** default value is unlimited.

**Max. concurrent queries:** default value is 150

## 4.5 Hostnames

Clicking the “Network” -> “Hostnames” in the GUI menu will appear the “Hostnames” page.



For those device does not have hostname or does not resolve automatically, users manually assign hostname-IP pair to specific devices.

**Add:** create a host entry (hostname-IP pair) for a specific device.

(For example, **Hostname** => “Test-Device”; **IP address** => “192.168.1.251”)

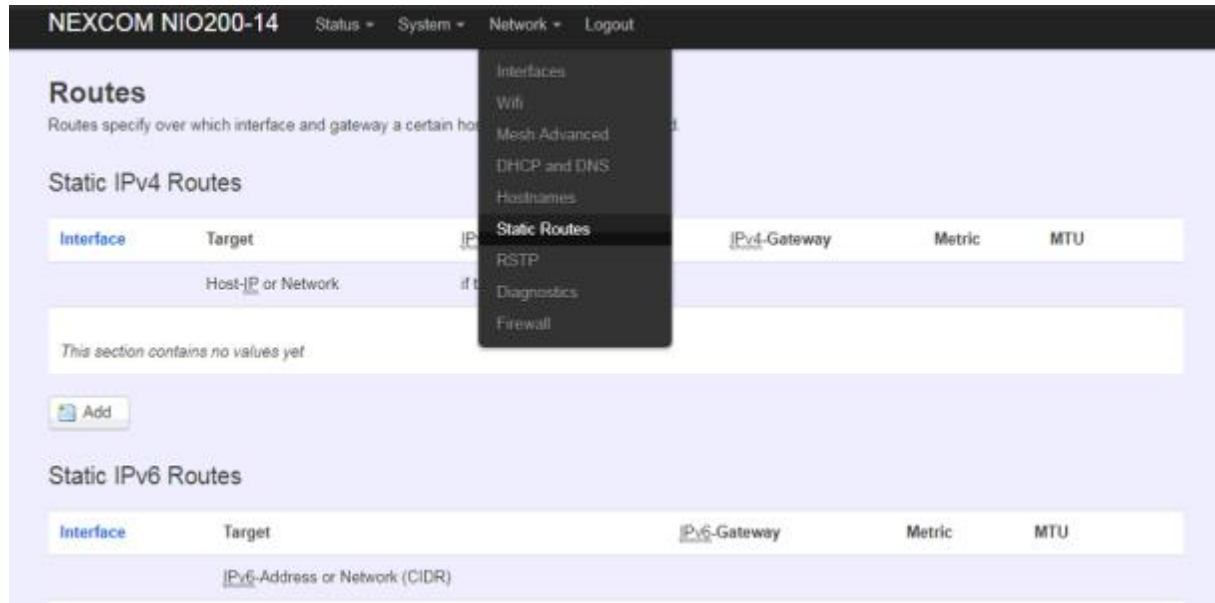


**Delete:** delete the followed host entry.

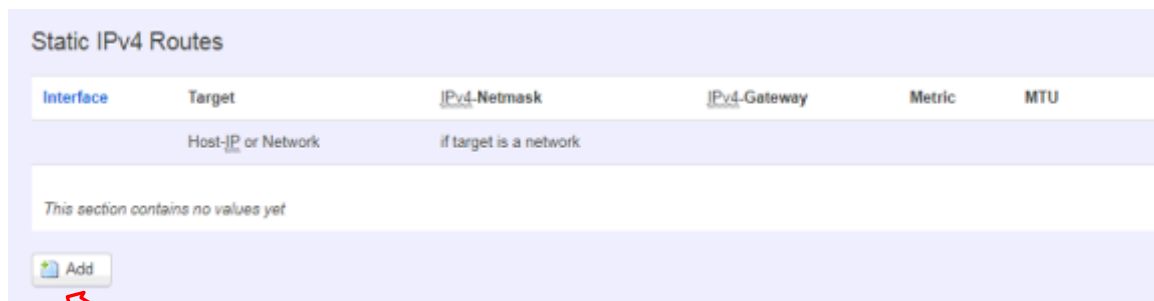
## 4.6 Static Routes

Clicking “Network” -> “Static Routes” in the GUI menu will appear the “Routes” page for two categories: “Static IPv4 Routes” and “Static IPv6 Routes”.

Static routes specify interface and gateway which certain host or network can be reached over. Such pair (interface and gateway) is called route.



For IPv4 network, scroll down to “Static IPv4 Routes” screen as follows.



**Add:** add an entry for route to an IPv4 network or host.

**For example:** *Target network=192.168.10.0; Netmask=255.255.255.0; NIO200HAG WAN IP=192.168.0.1;*

The route to be assigned will be “wan” for interface and “192.168.0.253” for gateway.

Leave “Metric” and “MTU” field to have default values as 0 and 1500 respectively.

**Routes**  
Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	
Host-IP or Network						
If target is a network						
lan	192.168.10.0	255.255.255.0	192.168.0.253	0	1500	Delete

Add

**Delete:** delete a followed route entry.

For IPv6 network, scroll down to “Static IPv6 Routes” screen as follows.

IWF300 Status System Network Logout

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
IPv6-Address or Network (CIDR)				
This section contains no values yet				

Add

**Add:** add an entry for route to an IPv6 network or host.

Clicking “Add” button has an entry as follows.

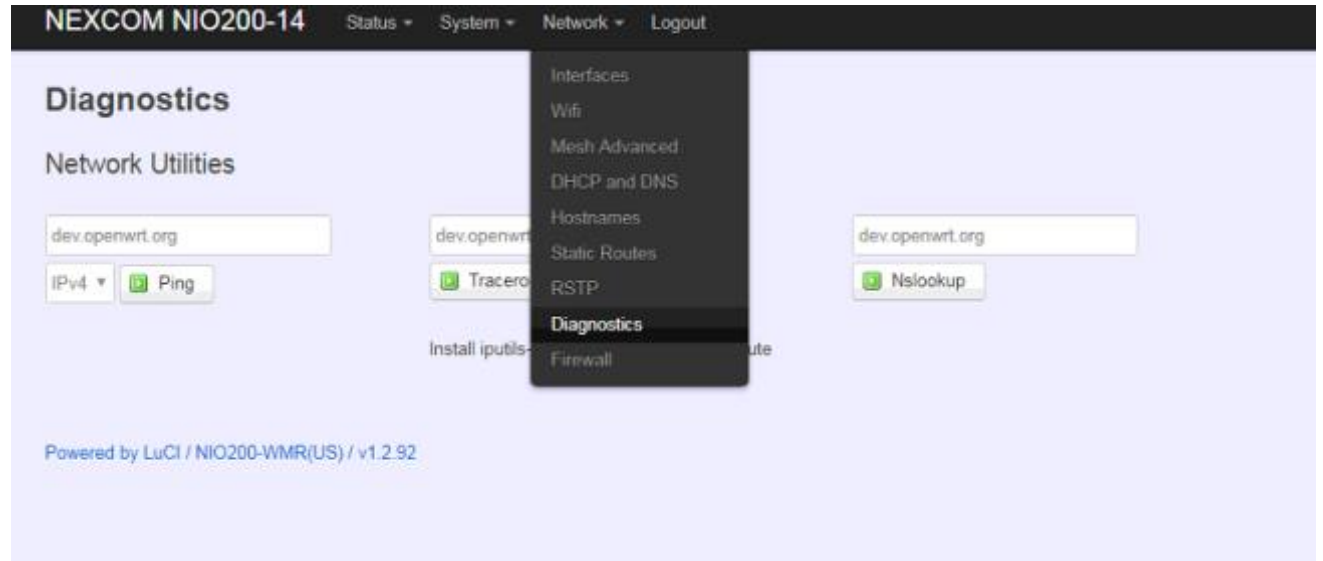
Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU	
IPv6-Address or Network (CIDR)					
lan			0	1500	Delete

Add

## 4.7 Diagnostics

Click “Network” -> “Diagnostics” in the GUI menu, and navigate to “Diagnostics” web page.



In this page, there are 3 utilities for users to diagnose interface settings and network paths: Ping, Traceroute, and Nslookup.



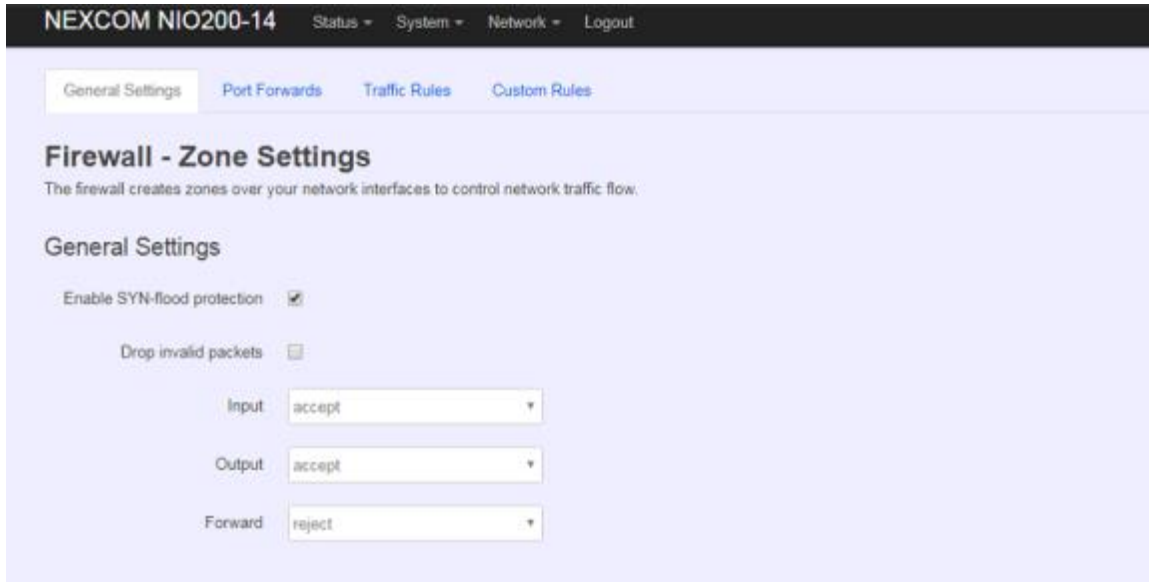
**Ping:** test the reachability of a [host](#) on an [Internet Protocol](#) (IP) network and measure the [round-trip time](#) for messages sent from the originating host to a destination host and back. The only required parameter is the name or IP address of the destination host.

**Traceroute:** track the route packets taken from an IP network on their way to a given destination host. The only required parameter is the name or IP address of the destination host.

**Nslookup:** query the [Domain Name System](#) (DNS) to obtain [domain name](#) or [IP address](#) mapping.

## 4.8 Firewall

Click “Network” -> “Firewall” in the GUI menu, and navigate to page configuring firewall attributes in the NIO200HAG.



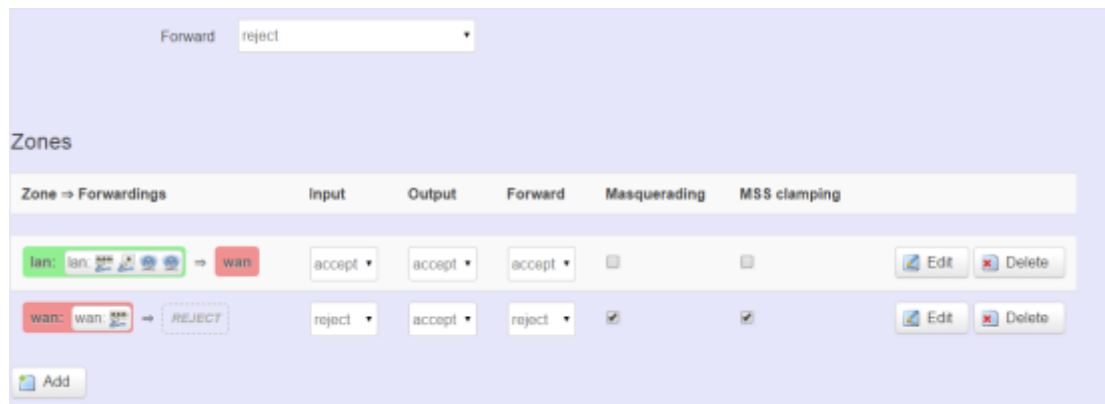
### General Settings

Clicking “General Settings” tab on the top of screen will show the “Zone Settings” configuration including “General Settings” and “Zones” categories.

In the “General Settings” category, there are 5 basic options for traffic control over interfaces:

“Enable SYN-flood protection” (default: enabled), “Drop invalid packets” (default: disabled), “Input” (default: accept), “Output” (default: accept), and “Forward” (default: reject)

In the “Zones” category, users create or edit zones over your network interfaces to control network traffic flow.



There 3 control buttons as follows for “Zones” settings:

**Edit:** edit the followed flow entry.

**Delete:** delete the followed flow entry.

**Add:** create a new entry for traffic flow among zones over interfaces.

## Port Forwards

Clicking the “Port Forwards” tab on the top of screen will show the tables for port forwarding. Adding or editing specific forwarding table allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

General Settings **Port Forwards** Traffic Rules Custom Rules

### Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

**New port forward:**

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
<input type="text" value="New port forward"/>	TCP+UDP	wan	<input type="text"/>	lan	<input type="text"/>	<input type="text"/>

In the “New port forward” category, there is only one button for flow editing:

**Add:** create a new flow entry for port forwarding among zones.

## Traffic Rules

Clicking the “Traffic Rules” tab on the top of screen will appear the policy tables of 2 categories: “Traffic Rules” and “Source NAT”.

General Settings Port Forwards **Traffic Rules** Custom Rules

### Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From any host in wan To any router IP at port 68 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-Ping	IPv4-ICMP with type echo-request From any host in wan To any router IP on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
Allow-DHCPv6	IPv6-UDP From IP range fe80::/10 in wan with source port 547 To IP range fe80::/10 at port 546 on this device	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

In the “Traffic Rules” category, the flow entries of traffic rule define policies for packets traveling between different zones (for example, to reject traffic between certain hosts or to open WAN ports on the router).

In “Source NAT” category, specific flow entries of masquerading that allow fine grained control over the source IP used for outgoing traffic(For example, to map multiple WAN addresses to internal subnets) can be added or edited.

**Source NAT**

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

**New source NAT:**

Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	<input type="text" value="-- Please choose"/>	<input type="text" value="Do not rewrite"/>

**Add and edit:** create a new entry with default values, and edit at once if required.

Please remember clicking “Save & Apply” button to activate the new settings.

## Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall re-start, right after the default rule-set has been loaded.

General Settings Port Forwards Traffic Rules Custom Rules

### Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```