



NIO200WMR User Manual

V1.2

Content

Preface.....	4
1 General Information.....	10
1.1 Document Purpose.....	10
1.2 Definitions, Acronyms and Abbreviations.....	10
2 Product Overview.....	13
2.1 About the NIO200WMR.....	13
2.2 Package Contents.....	14
3 Getting Started.....	15
3.1 Installation background.....	15
3.2 Hardware installation Guide.....	15
3.2.1 Water proof connector installation.....	16
3.2.2 Power installation.....	19
3.2.3 Antenna installation.....	19
3.2.4 Earth grounding.....	20
3.2.5 Mounting of NIO200 Series.....	20
4 System configuration.....	23
4.1 Login.....	23
4.2 Status.....	25
4.2.1 Overview.....	25
4.2.2 Firewall.....	29
4.2.3 Routes.....	29
4.2.4 System Log.....	31
4.2.5 Kernel Log.....	31
4.2.6 Processes.....	32
4.2.7 Real-time Graphic.....	32
4.3 System.....	36
4.3.1 System.....	36
4.3.2 Administration.....	39
4.3.3 Backup/Flash Firmware.....	40
4.3.4 Reboot.....	43
4.4 Network.....	44
4.4.1 Interfaces.....	44
4.4.1.1 Configuration of IP address.....	44

4.4.2	Wi-Fi	50
4.4.2.1	Wireless Overview	50
4.4.2.2	Associated Stations	51
4.4.2.3	Wireless configuration	51
4.4.3	Mesh Advanced	55
4.4.3.1	Mesh Advanced	55
4.4.4	DHCP and DNS	58
4.4.4.1	General Settings	59
4.4.4.2	Resolve and Hosts Files	60
4.4.4.3	TFTP Settings	60
4.4.4.4	Advanced Settings	61
4.4.5	Hostnames	62
4.4.6	Static Routes	63
4.4.7	Diagnostics	65
4.4.8	Firewall	66
4.4.8.1	General Settings	66
4.4.8.2	Port Forwards	67
4.4.8.3	Traffic Rules	67
4.4.8.4	Custom Rules	68

Preface

This manual is for user to set up a network environment using the NIO200 series Product line. It contains step-by-step procedures and graphic examples to guide installer or individuals with slight network system knowledge to complete the installation.

Copyright

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written consent from NEXCOM International Co., Ltd.

Disclaimer

The information in this document is subject to change without prior notice and does not represent commitment from NEXCOM International Co., Ltd. However, users may update their knowledge of any product in use by constantly checking its manual posted on our website: <http://www.nexcom.com>. NEXCOM shall not be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of any product, nor for any infringements upon the rights of third parties, which may result from such use. Any implied warranties of merchantability or fitness for any particular purpose is also disclaimed.

Acknowledgements

IWF series are trademarks of NEXCOM International Co., Ltd. All other product names mentioned herein are registered trademarks of their respective owners.

Safety Information

Before installing and using the device, note the following precautions:

- Read all instructions carefully.
- Do not place the unit on an unstable surface, cart, or stand.
- Follow all warnings and cautions in this manual.
- When replacing parts, ensure that your service technician uses parts specified by the manufacturer.
- Avoid using the system near water, in direct sunlight, or near a heating device.

Installation Recommendations

Ensure you have a stable, clean working environment. Dust and dirt can get into components and cause a malfunction.

Use containers to keep small components separated.

Adequate lighting and proper tools can prevent you from accidentally damaging the internal components. Most of the procedures that follow require only a few simple tools, including the following:

- A Philips screwdriver
- A flat-tipped screwdriver
- A grounding strap
- An anti-static pad

Using your fingers can disconnect most of the connections. It is recommended that you do not use needle-nose pliers to disconnect connections as these can damage the soft metal or plastic parts of the connectors.

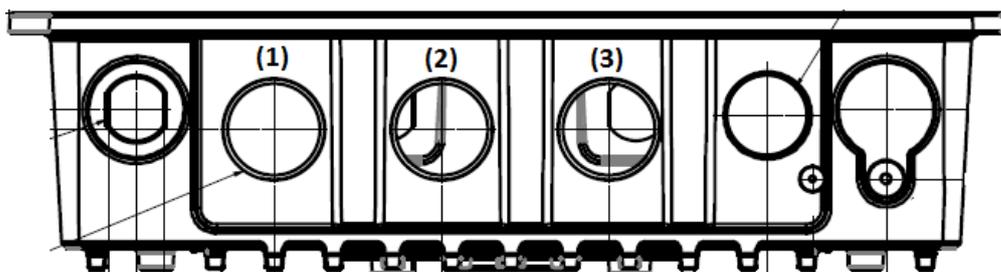
Safety Precautions

1. Read these safety instructions carefully.
2. Keep this User Manual for later reference.
3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
4. For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
5. Keep this equipment away from humidity.
6. Put this equipment on a stable surface during installation. Dropping it or letting it fall may cause damage.
7. The openings on the enclosure are for air convection to protect the equipment from overheating. **DO NOT COVER THE OPENINGS.**
8. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
9. Place the power cord in a way so that people will not step on it. Do not place anything on top of the power cord. Use a power cord that has been approved for use with the product and that it matches the voltage and current marked on the product's electrical range label. The voltage and current rating of the cord must be greater than the voltage and current rating marked on the product.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.

12. Never pour any liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If one of the following situations arises, get the equipment checked by service personnel:
 - a. The power cord or plug is damaged.
 - b. Liquid has penetrated into the equipment.
 - c. The equipment has been exposed to moisture.
 - d. The equipment does not work well, or you cannot get it to work according to the user's manual.
 - e. The equipment has been dropped and damaged.
 - f. The equipment has obvious signs of breakage.
15. Do not place heavy objects on the equipment.
16. Be sure to ground the 0.75mm² with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit and to a good ground connection. Earth, Green/Yellow wire, 18AWG, the minimum cross-sectional area of Earth conductor shall equal to Input wiring cable.
17. The front of the Equipment requires wiring terminals with the following specifications:
 - **Wire size: 30-12 AWG** (0.0509-3.3088 mm²)
 - **Wire Type: copper wire only**
 - **Terminal Blocks Torque: 5 lb In.** (0.565 N-m).
 - For supply connections, use wires suitable for at least 75 degree C ambient environment

- **There must be a disconnect device in front of "NIO200 series" to keep the worker or field side maintainer be cautious and aware to close the general power supply before they start to do maintenance. The disconnect device hereby means a 20A circuit-breaker. Power installation must be performed with qualified electrician and followed with National Electrical Code, ANSI/NFPA 70 and Canadian Electrical Code, Part I, CSA C22.1.**

18.



- (1) DC IN: 12-48Vdc, 2.1-0.6A
- (2) LAN
- (3) WAN(POE):57Vdc, 600mA

19. This equipment is intended to Ex nA IIC T4 Gc.

Note:

This equipment is intended to be mounted on a pole with the mounting bracket, wall mounting or DIN mounting; the mounting should always let water proof connectors down to bottom position.

Cet équipement est destiné à être monté à la place avec le support de montage, montage mural ou montage DIN; Le montage doit toujours laisser les connecteurs imperméable à la base.

This equipment is suitable for use in Class I, Division 2, Groups A, B, C, and D or non-hazardous locations only.

Cet équipement est adapté à une utilisation en Classe I, Division 2, Groupes A, B, C et D ou des zones non dangereuses uniquement.

- WARNING – EXPLOSION HAZARD. DO NOT CONNECT OR DISCONNECT WHEN ENERGIZED.”
- AVERTISSEMENT - RISQUE D'EXPLOSION. NE PAS CONNECTER NI DÉCONNECTER LORSQU'IL EST EN CHARGE.
- Product is UL Listed with UL Listed Fittings for use with liquid-tight flexible metal conduit. This wiring method is suitable for flexible connections in accordance with Article 501.10(B)(2) of the National Electrical Code (ANSI/NFPA 70). Suitability for installation in particular applications is at the discretion of the Authority Having Jurisdiction (AHJ) or similar.
- Le produit est homologué UL avec des accessoires homologués UL pour conduit métallique flexible étanche aux liquids.
ette méthode de câblage convient aux flexibles connexions conformément
- à l'article 501.10 (B) (2) du National Code électrique (ANSI / NFPA 70). Pertinenced'installation dans certaines applications à

la discrétion de l'Autorité ayant Jurisdiction (AHJ) Ou similaire.

Technical Support and Assistance

1. For the most updated information of NEXCOM products, visit NEXCOM's website at www.nexcom.com.
2. For technical issues that require contacting our technical support team or sales representative, please have the following information ready before calling:
 - Product name and serial number
 - Detailed information of the peripheral devices
 - Detailed information of the installed software (operating system, version, application software, etc.)
 - A complete description of the problem
 - The exact wordings of the error messages

Warnings

Read and adhere to all warnings, cautions, and notices in this guide and the documentation supplied with the chassis, power supply, and accessory modules. If the instructions for the chassis and power supply are inconsistent with these instructions or the instructions for accessory modules, contact the supplier to find out how you can ensure that your computer meets safety and regulatory requirements.

1. Handling the unit: carry the unit with both hands and handle it with care.
2. Opening the enclosure: disconnect power before working on the unit to prevent electrical shocks.
3. Maintenance: to keep the unit clean, use only approved cleaning products or cleans with a dry cloth.

Safety Warning: This equipment is intended for installation in a Restricted Access Location only

Avertissement de sécurité: Cet équipement est destiné à être installé uniquement dans un lieu d'accès restreint

Cautions

Electrostatic discharge (ESD) can damage system components. Do the described procedures only at an ESD workstation.

If no such station is available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the computer chassis.

Conventions Used in this Manual



Warning: Information about certain situations, which if not observed, can cause personal injury. This will prevent injury to yourself when performing a task.



Caution: Information to avoid damaging components or losing data.



Note: Provides additional information to complete a task easily.



**WARNING
HOT SURFACE
DO NOT TOUCH**

Note: The surface temperature of enclosure may exceed 70°C under working condition.

Remarque: La température de surface de l'enceinte peut dépasser 70 °C dans des conditions de travail.

1 General Information

1.1 Document Purpose

This quick installation guide is designed to let user quickly get necessary installation information about hardware as well as software so that the field installation can be well done through this first aid.

1.2 Definitions, Acronyms and Abbreviations

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

Term	Description
API	Application Programming Interface
Backbone	Any data network (e.g. industrial Ethernet, IEEE 802.11, etc.) within a facility interfacing to the plants network.
Backbone Router	An entity in the ISA100.11a network with routing capability which serves as an interface between the radio network and the backbone network.
BBR	Backbone Router
Blacklisted channel	A channel on which transmission is prohibited.
Broadcast	Transmission intended for all the devices in an ISA100.11a network (used for advertisements with all devices including the BBR, or for receive links for field devices only).
CCA backoffs	The count of transmissions on an RF channel that were aborted due to CCA.
CGI	Common Gateway Interface
Channels	Divisions of radio frequencies supported in a wireless network.
Contract	An agreement between the system manager and a device in the network involving the allocation of network resources by the system manager to support a particular communication need of that device.
Device role	Device capabilities that will be accepted by the Security Manager.

Term	Description
DHCP	Dynamic Host Configuration Protocol – a method to automatically configure the IP settings of a host connected in a LAN.
EUI64, EUI-64	The 64-bit address of a device in the network; it is a unique identifier usually set at the manufacturing of the device.
Field	The geographic space that contains all the nodes of a wireless network.
Field device	A physical device designed to meet the rigors of plant operation that communicates via DPDU's conforming to the ISA100.11a protocol.
Gateway	An entity in the ISA100.11a network that serves as an interface between the ISA100.11a network and a client.
Graph (communication)	A collection of unidirectional interconnected devices, which defines a set of communication paths between a source device and a destination device.
Graph (Topology)	A graphical representation of the network topology.
GW	Gateway
Input/output	A device with minimum characteristics required to participate in an ISA100.11a network and which provides or uses data from other devices.
ISA100.11a	A communication protocol used in wireless networks, set up by the Wireless Compliance Institute.
JSON	JavaScript Object Notation
LAN	Local Area Network
Link	A momentary or persistent interconnecting path between two or more devices for the purpose of transmitting and receiving messaging.
MCS	Monitoring Control System
Network Address	The 128-bit address of a device in the network.
Packet Error Rate	The ratio, in percent, of the number of lost packets (DPDU's) to the total number of packets sent by the selected device to its parent.
Process value	The quantity being controlled or the measurement value.
Provision	To update settings on an entity in order to prepare it for working in the network.
Revision	The device software revision related to vendor/model.
Router	A device that has data routing capability.

Term	Description
Security Manager	An entity in the ISA100.11a network that assigns the security keys that are required for communication between devices.
SM	System Manager
Superframe	A collection of timeslots with a common repetition period and possibly other common attributes.
System Manager	An entity in the ISA100.11a network that supervises the various operational aspects of a network other than security.
TR	Transceiver – the BBR radio
User Application Process	From ISA100.11a standard: An active process within the highest portion of the application layer that is the user of OSI (Open Systems Interconnection) services.
UTC	Coordinated Universal Time – A universal timekeeping standard that is based on the Greenwich Mean Time (GMT). Local time is calculated in UTC and offset by the local time zone.
FD	Field Device

2 Product Overview

2.1 About the NIO200WMR



NEXCOM's NIO200WMR is a unique anti-explosive (CID2 & ATEX certified) Wi-Fi routers which support Mesh, AP and Client modes. This is dedicated design for heavy industrial HazLoc environment. With the Wi-Fi Mesh technology, NIO200WMR provides most reliable wireless connectivity with intelligent multi-path mechanism. It establishes robust access and backbone infrastructure. To meet the requirement of critical environment, NIO200WMR equips with wide temperature (-40 ~75 °C), IP67 protection, highest standard level-4 EMC immunity, CID2 and ATEX anti-explosive capability.

For security consideration, NIO200WMR gives user versatile selection of different encryption (pre-shared key and Enterprise) black list and white list protection mechanism. Together with nCare, I4.0 network manager, NIO200WMR can be easily managed. Thus, effectively reduce the cost for network maintenance and management effort.

2.2 Package Contents

Each NIO200WMR package contains the following items:

- One NIO200WMR unit
- Two simple wall mounting kit
- Three liquid-tight cable gland or conduit based on the ATEX or CID2 model.
(used only for DC power input and Ethernet port)
- Two-pin DC power connector for 12~48 VDC power input
- Grounding screws
- Four outdoor antennas for evaluation purpose (when deployed in field site, the antenna may be changed to meet the application requirement)

3 Getting Started

3.1 Installation background

The web-based administration is the preferred method to administer/configure the NIO200WMR. It requires a web browser and the IP of the NIO200WMR. The NIO200WMR is suggested to connect 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.

3.2 Hardware installation Guide

Hardware connection of NIO200 includes the power, Ethernet interfaces and RF connectors. The installation of NIO200 should be carefully done with standard waterproof connectors accessories in the package (CID2: conduit connector, ATEX: cable gland connector).

Note: the mounting of NIO200 should always let water proof connectors down to bottom position. The following picture illustrates the proper mounting direction of NIO200 in the field.



3.2.1 Water proof connector installation

A. Installation of conduit connector for CID2 model



To install conduit in NIO200 enclosure, please follow the steps below:



- Put conduit through cap nut and gland packing.
- Position the ferrule at the end of the conduit. (Just have the bottom of ferrule cover the conduit, over-tighten may enlarge conduit diameter and loosen
- Pass DC power cable or Ethernet cable through conduit



- Connect connector into
- Insert the conduit with
- Push gland packing and

NIO200 enclosure, tighten locknut with body.

ferrule into connector of NIO200 enclosure.

cap nut forwards to NIO200 conduit connector and tighten the cap nut

To install the conduit, user should implement with Flexible Metal Conduit, Liquid-tight which meets UL360 standard. Here is the requirement of the diameter and size information for the selection of Metal Conduit that mate with NIO200 conduit connectors.

Nominal size (inch)	Inner diameter min. (mm)	Inner diameter max. (mm)	Outside diameter min. (mm)	Outside diameter max. (mm)	Min bending radius (mm)	Packing length (m)
3/8"	12.29	12.80	17.50	18.00	50.50	30
1/2"	15.80	16.31	20.80	21.30	82.50	30
3/4"	20.83	21.34	26.20	26.70	108.00	30
1"	26.44	27.08	32.80	33.40	165.00	20
1-1/4"	35.05	35.81	41.40	42.20	203.00	20
1-1/2"	40.01	40.64	47.40	48.30	228.50	20

B. Installation of cable gland connector for ATEX model



To install cable gland with power / Ethernet cable on NIO200 enclosure, please follow the steps below:

Power connector installation



1. De-assembly the cable gland connector.



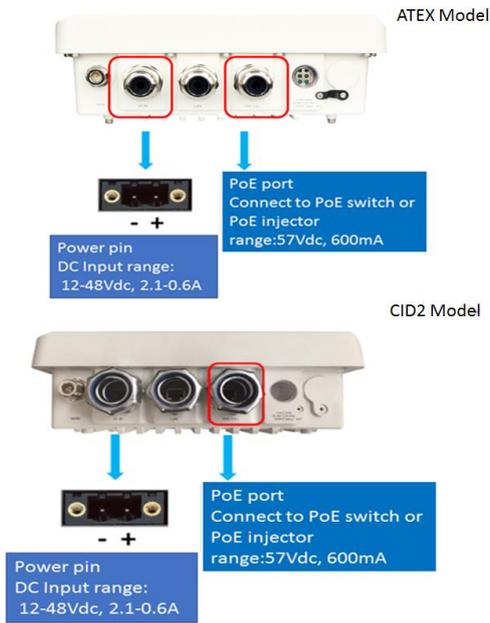
1. Pass power and Ethernet cable through cable gland as the illustration at the left.



2. Connect cable gland to NIO200 unit:

- Screw up the tips of power cable to green power connector.
- Fit the power cable to the left screw hole and tightly fasten cable gland to enclosure of NIO200 unit.
- Fit the Ethernet cable into the LAN or WAN hole on the enclosure. Tightly fasten cable gland to enclosure of NIO200 unit.

3.2.2 Power installation



- 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 the Ethernet cable into PoE port.
- If the power connects correctly, then the “Power LED” will light accordingly

3.2.3 Antenna installation



Wi-Fi antenna connector for Wi-Fi Mesh connection (WLAN 1 & WLAN 2)



IWSN antenna connector (for connecting to ISA100 or WirelessHART), not used in NIO200WMR.

3.2.4 Earth grounding



1. Be sure to ground the 0.75mm² ground screw with an appropriate grounding wire (Earth, Green/Yellow wire 18AWG, not included) by attaching it to a good earth ground connection.
2. There must be a disconnect device in front of “NIO200 series” to keep the worker or field side maintainer be cautious and aware to close the general power supply before they start to do maintenance.
3. The disconnect device hereby means a 20A circuit-breaker. Power installation must be performed with qualified electrician and followed with National Electrical Code, ANSI/NFPA 70 and Canadian Electrical Code, Part I, CSA C22.1.

3.2.5 Mounting of NIO200 Series

Mounting method in NIO200 is default with simple wall mounting kit. If the installation is with pole mounting method, then user should purchase pole mounting kit for the installation. Here is the guide for both simple wall mounting method and pole mounting method:

A.Simple wall mounting method:

1. Screw the simple wall mounting kit to the bottom of NIO200 enclosure.

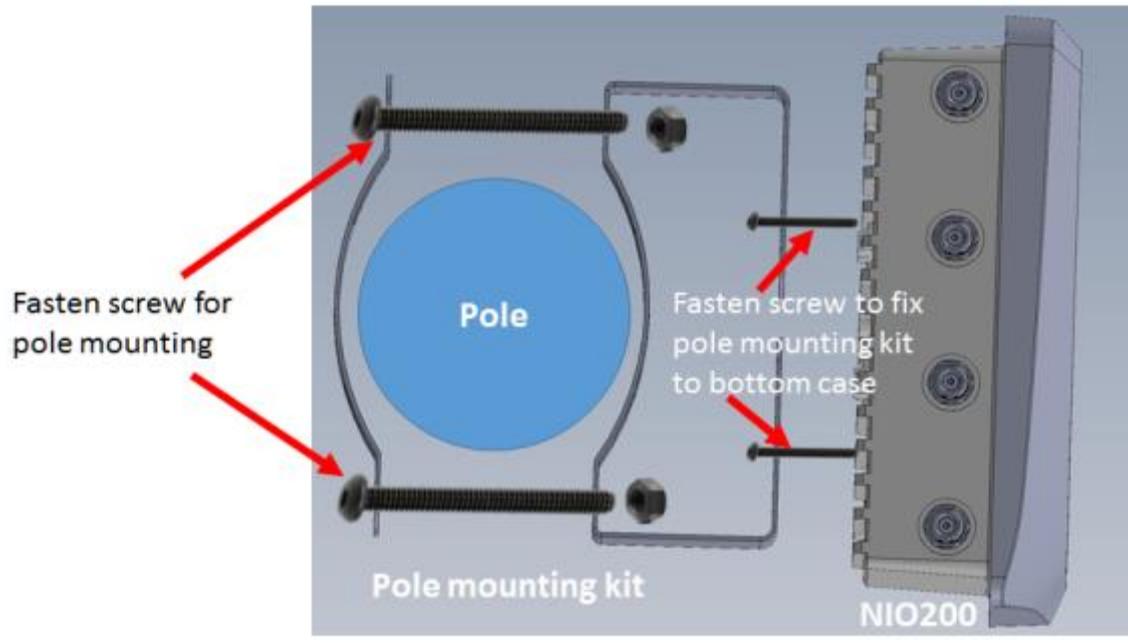


2. Be sure to fasten the mounting kit with horizontal position as below:



3. Hang on NIO200 to the wall with water proof connector at the bottom direction.

B.Pole mounting method:



4 System configuration

4.1 Login

To access the NIO200WMR 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:

NEXCOM NIO200-15

Authorization Required

Please enter your username and password.

Username:

Password:

Powered by LuCI / NIO200-WMR(US) / v1.0.98

Default login information is:

Login: root

Password: admin

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

NEXCOM NIO200-15 Status - System - Network - Logout AUTO-RENEWAL ON

Status

System

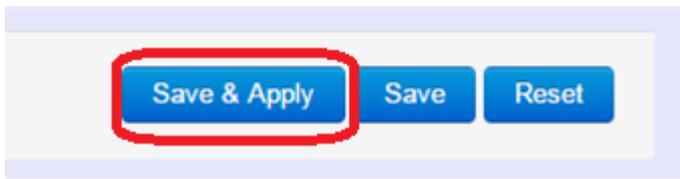
Hostname	NIO200-15
Model	NIO200-WMR
Firmware Version	NIO200-WMR(US)-v1.0.98 / LuCI (git-16.020.59380-63d70da)
Kernel Version	3.14.27
Local Time	Mon Jul 16 14:40:22 2018
Uptime	23d 4h 25m 53s
Load Average	0.03, 0.07, 0.12

Memory

Total Available	<input type="text" value="25860 kB / 775424 kB (3%)"/>
Free	<input type="text" value="25860 kB / 775424 kB (3%)"/>
Buffered	<input type="text" value="0 kB / 775424 kB (0%)"/>

Saving Changes

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



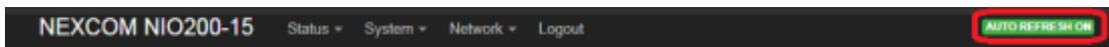
Unsaved Changes



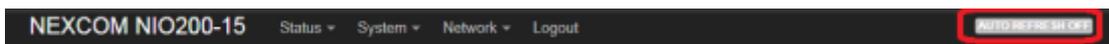
"UNSAVED CHANGES" provides the help to see the parameters which were not saved & applied,

Click "Save & Apply" button to save the parameters.

Auto Refresh

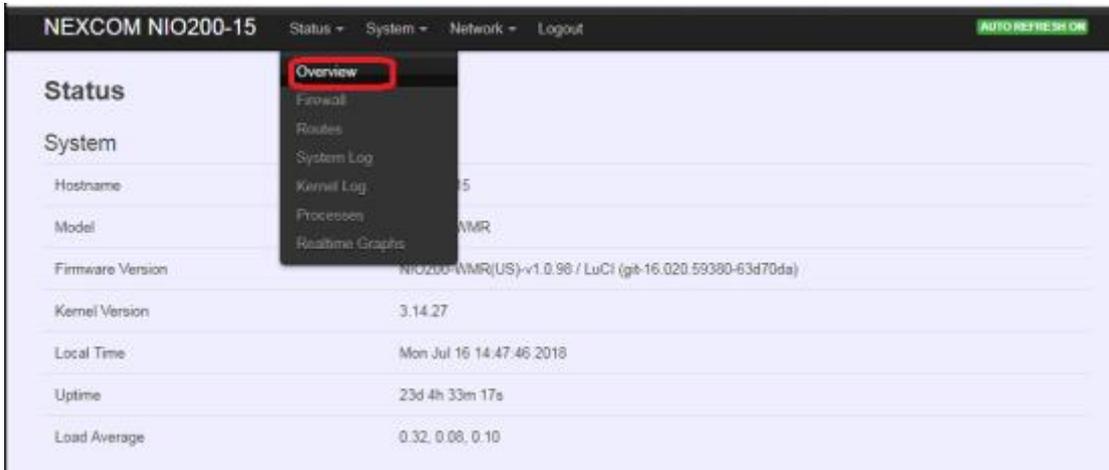


Toggle "AUTO REFRESH" button to turn on/off WebUI refresh function automatically



4.2 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:



4.2.1 Overview

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

4.2.1.1 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.

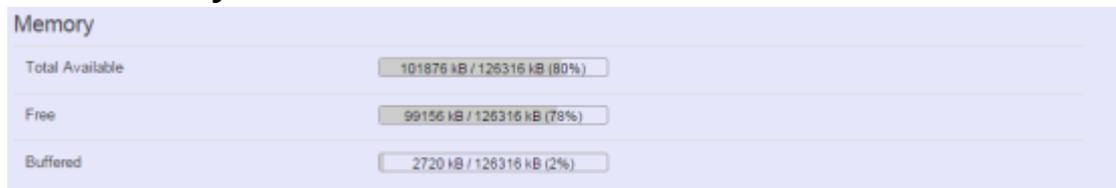
Load Average: CPU average loading in recent time frame.

For example,



CPU average loading:
94% in the past 1 minute.
43% in the past 5 minutes
24% in the past 15 minutes.

4.2.1.2 Memory

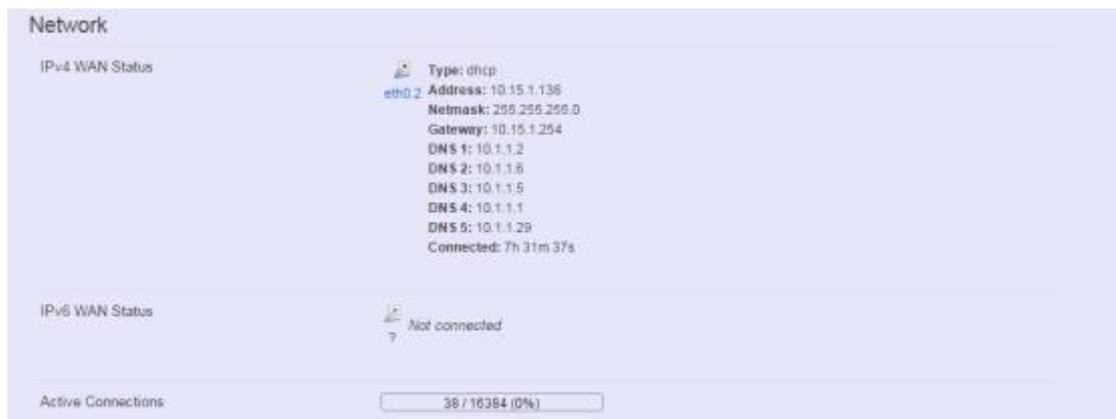


Total Available: Displays the available memory in percentage.

Free: Displays free memory of NIO200.

Buffered: Displays buffer memory used in the system.

4.2.1.3 Network



IPv4 WAN Status: Displays current connecting IPv4 information.

IPv6 WAN Status: Displays current connecting IPv6 information.

Active Connections: Displays current active connections.

4.2.1.4 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

4.2.1.5 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	000100011b2c6cb9206a8e9612c0	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.

4.2.1.6 Wireless

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

4.2.1.7 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 NIO200WMR, including device's MAC address, signal level, noise, connecting data rate.

4.2.2 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.

NEXCOM NIO200-15 Status - System - Network - Logout

Firewall Status

Overview
Firewall
Routes
System Log
Kernel Log
Processes
Realtime Graphs

Reset Counters Restart Firewall

Table: Filter

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

Pkts.	Traffic	Target	Prot.	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	-

4.2.3 Routes

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

4.2.3.1 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.

4.2.3.2 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.

4.2.3.3 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	:::/8		256	local
(eth0)	:::/8		256	local
wan	:::/8		256	local
lan	:::/8		256	local
lan	:::/8		256	local

Displays active IPv6 routing table of WAN and LAN port.

4.2.3.4 IPv6 Neighbors

IPv6 Neighbours

IPv6 Address	MAC Address	Interface
fdfc:68c3:19eb:0:1f4:f243:8e92:e881	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:e5df:2aba:f91:5221	80:19:34:c9:04:00	lan
fdfc:68c3:19eb::3b0	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:21cf:7bb5:a2c9:e438	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:b815:35d6:d8b7:dff8	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:691a:9a70:b879:924d	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:468:1e7:d4fe:8c9a	9c:2a:70:1b:4c:9d	lan
fdfc:68c3:19eb:0:f118:d10c:ab71:1676	80:19:34:c9:04:00	lan
fdfc:68c3:19eb:0:7c3a:bc4c:52a3:da5a	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:6046:1236:d6c8:82c:1	00:0d:f0:ac:c8:63	lan
fdfc:68c3:19eb:0:c654:4dff:fedc:fea5	c4:54:44:da:fa:a5	lan
fdfc:68c3:19eb:0:a151:5f16:e22f:f07c	c4:54:44:da:fa:a5	lan
fdfc:68c3:19eb:0:61ad:92b6:99e2:bf9b	80:19:34:c9:04:00	lan

Display connected device with IPv6 information.

4.2.4 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 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 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
```

4.2.5 Kernel Log

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

```
NEXCOM NIO200 Status - System - Network - Logout

Kernel Log
[ 0.000000] Using P1020 RDB machine description
[ 0.000000] Memory CAM mapping: 256/256/256 Mb, residual: 256Mb
[ 0.000000] Linux version 3.14.27 (ronsu@ronsu-vm) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r582) ) #20 SMP Thu Oct 25 12:17:26 CST 2018
[ 0.000000] Found legacy serial port 0 for /soc@ffe00000/serial@4500
[ 0.000000] mem=ffe04500, taddr=ffe04500, irq=0, clk=399999996, speed=0
[ 0.000000] Found legacy serial port 1 for /soc@ffe00000/serial@4600
[ 0.000000] mem=ffe04600, taddr=ffe04600, irq=0, clk=399999996, speed=0
[ 0.000000] CPU maps initialized for 1 thread per core
[ 0.000000] (thread shift is 0)
[ 0.000000] boot/console [udbg0] enabled
[ 0.000000] MPC85xx RDB board from Freescale Semiconductor
[ 0.000000] Top of RAM: 0x30000000, Total RAM: 0x30000000
[ 0.000000] Memory hole size: 0MB
[ 0.000000] Zone ranges:
[ 0.000000] DMA [mem 0x00000000-0x2ffffff]
[ 0.000000] Normal empty
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000] node 0: [mem 0x00000000-0x2ffffff]
[ 0.000000] node 0: [mem 0x00000000-0x2ffffff]
```

4.2.6 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%	Hang Up	Terminate	Kill	
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill	
3	root	[kssoftirqd/0]	0%	0%	Hang Up	Terminate	Kill	
5	root	[kworker/0.0H]	0%	0%	Hang Up	Terminate	Kill	
7	root	[rcu_sched]	0%	0%	Hang Up	Terminate	Kill	
8	root	[rcu_bh]	0%	0%	Hang Up	Terminate	Kill	
9	root	[migration/0]	0%	0%	Hang Up	Terminate	Kill	
10	root	[migration/1]	0%	0%	Hang Up	Terminate	Kill	

4.2.7 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”**.



4.2.7.1 Load



Display real-time CPU average loading percentage.
i.e.

<u>1 Minute Load:</u>	0.08	Average:	0.08	Peak:	0.33
<u>5 Minute Load:</u>	0.33	Average:	0.33	Peak:	0.39
<u>15 Minute Load:</u>	0.34	Average:	0.34	Peak:	0.36

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

4.2.7.2 Traffic

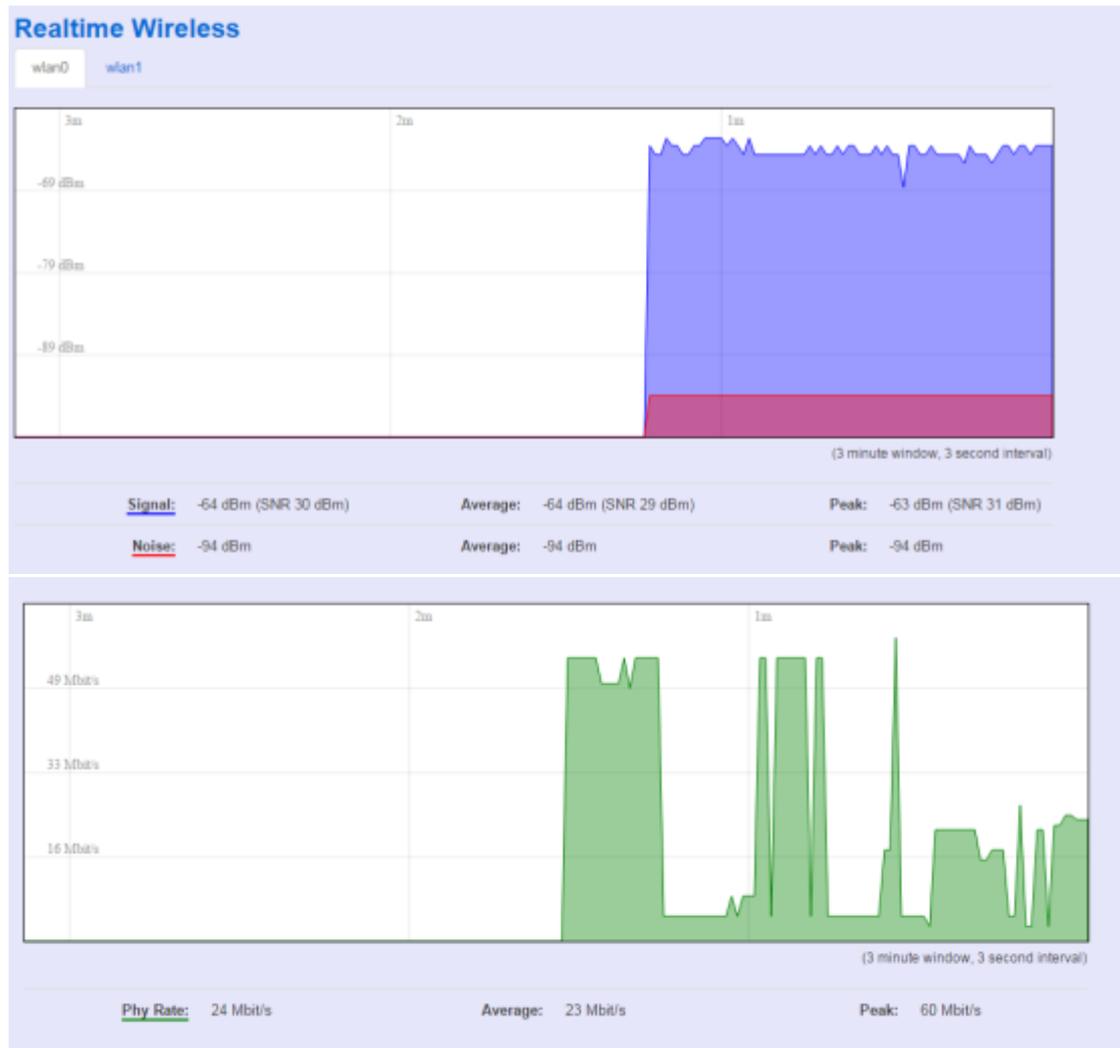


Display NIO200 real-time traffic loading of Ethernet, WLAN and internal bridge interfaces.

Inbound: Incoming data throughput of the observed interface.

Outbound: Outgoing data throughput of the observed interface.

4.2.7.3 Wireless



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

wlan0: Radio0 information.

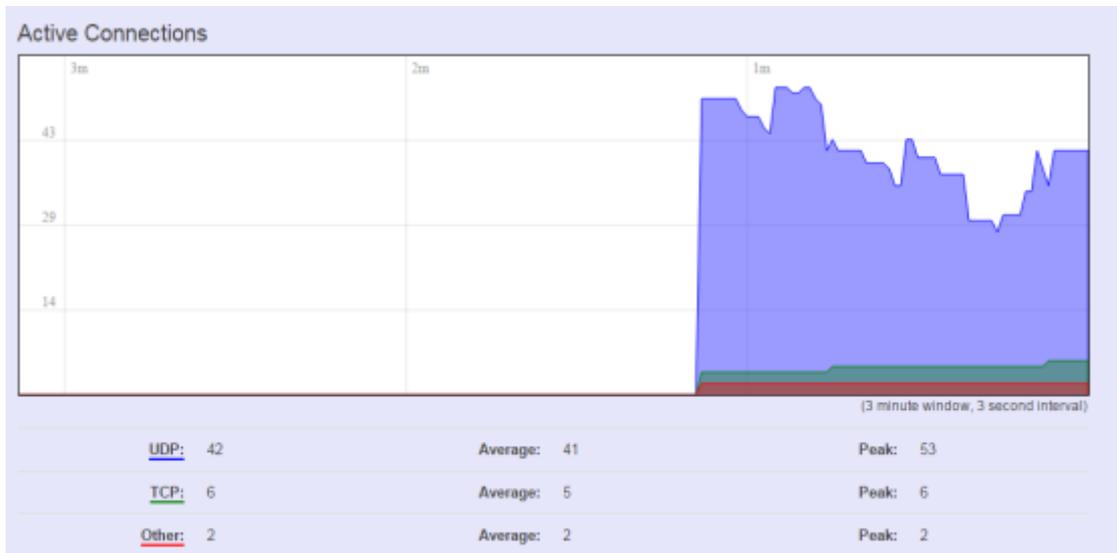
wlan1: Radio1 information.

Note:

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

4.2.7.4 Connections

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



Network	Protocol	Source	Destination	Transfer
IPV4	ICMP	IM03-AndrewWang1.lan:0	IWF300.lan:0	602.29 KB (10279 Pkts.)
IPV4	UNKNOWN	0.0.0.0:0	all-systems.mcast.net:0	92.06 KB (2946 Pkts.)
IPV4	UDP	IM03-AndrewWang1.lan:17500	192.168.1.255:17500	57.96 KB (345 Pkts.)
IPV4	TCP	IM03-AndrewWang1.lan:57367	40.113.115.191:443	53.97 KB (573 Pkts.)
IPV4	TCP	IM03-AndrewWang1.lan:62255	IWF300.lan:80	19.43 KB (217 Pkts.)
IPV4	UDP	10.15.1.254:67	255.255.255.255:68	6.91 KB (21 Pkts.)
IPV4	TCP	IM03-AndrewWang1.lan:57369	fl-hn-f125.1e100.net:5222	4.25 KB (55 Pkts.)
IPV4	TCP	IM03-AndrewWang1.lan:57366	91.190.218.53:12350	2.68 KB (48 Pkts.)
IPV4	UDP	IM03-AndrewWang1.lan:68	255.255.255.255:67	328.00 B (1 Pkts.)
IPV4	UDP	IWF300.lan:67	IM03-AndrewWang1.lan:68	328.00 B (1 Pkts.)
IPV4	UDP	IM03-AndrewWang1.lan:137	192.168.1.255:137	234.00 B (3 Pkts.)
IPV4	UDP	10.15.1.138:61033	10.1.1.2:53	118.00 B (1 Pkts.)
IPV4	UDP	10.15.1.138:43389	10.1.1.2:53	118.00 B (1 Pkts.)
IPV4	UDP	10.15.1.138:52009	10.1.1.2:53	118.00 B (1 Pkts.)

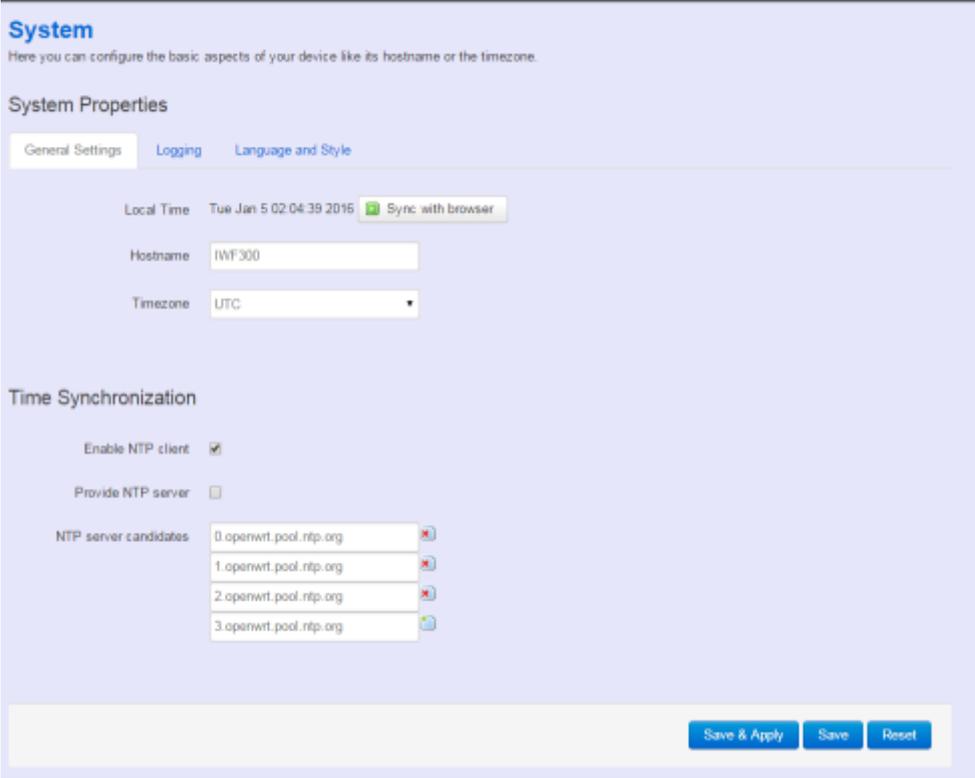
4.3 System

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.

4.3.1 System

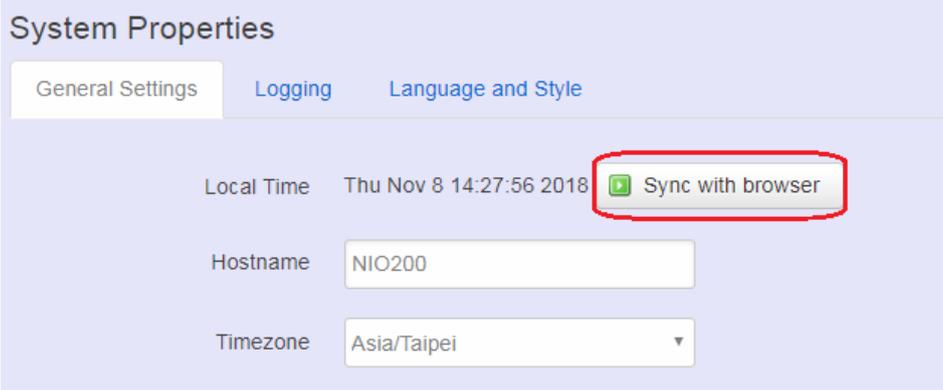
4.3.1.1 General Settings

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



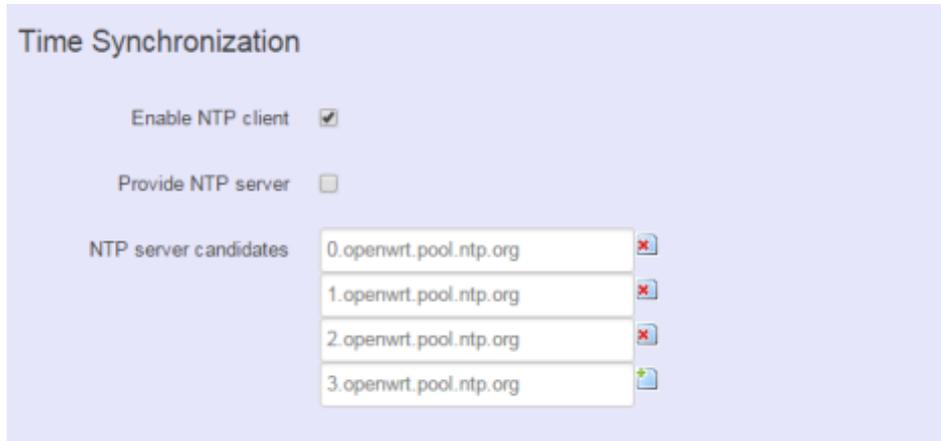
The screenshot shows the 'System' configuration page for NIO200. The page title is 'System' and it includes a subtitle: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Below this is the 'System Properties' section with three tabs: 'General Settings' (selected), 'Logging', and 'Language and Style'. Under 'General Settings', there are three rows of configuration: 'Local Time' showing 'Tue Jan 5 02:04:39 2016' with a 'Sync with browser' button; 'Hostname' with a text input field containing 'HWF300'; and 'Timezone' with a dropdown menu set to 'UTC'. Below these is the 'Time Synchronization' section with 'Enable NTP client' checked and 'Provide NTP server' unchecked. A list of 'NTP server candidates' contains four entries, all set to '0.openwrt.pool.ntp.org'. At the bottom right, there are three buttons: 'Save & Apply', 'Save', and 'Reset'.

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



This is a close-up screenshot of the 'System Properties' configuration page. It shows the 'General Settings' tab selected. The 'Local Time' row displays 'Thu Nov 8 14:27:56 2018' and the 'Sync with browser' button is highlighted with a red rectangle. The 'Hostname' row has a text input field containing 'NIO200'. The 'Timezone' row has a dropdown menu set to '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

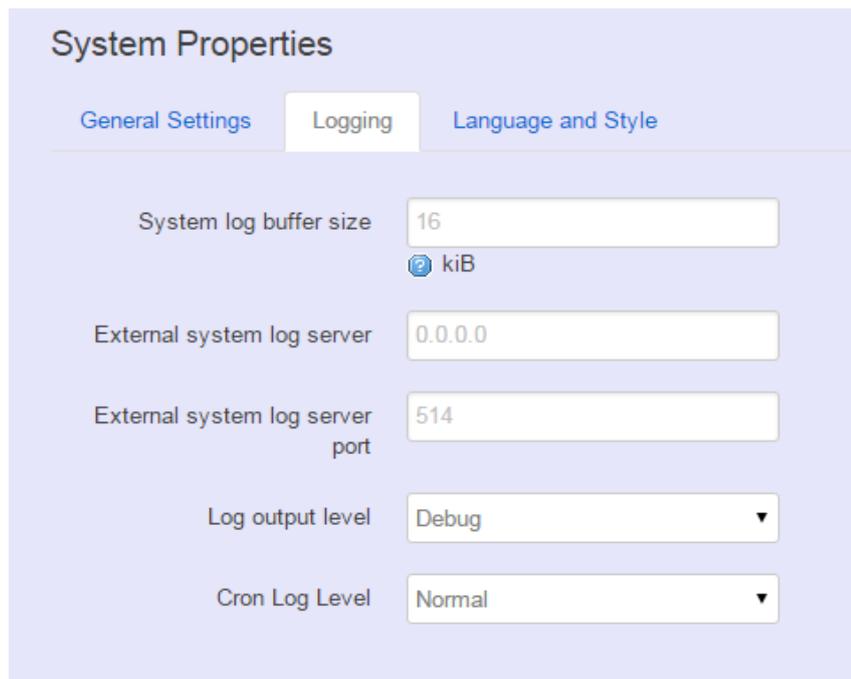
Provide NTP server

NTP server candidates

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

4.3.1.2 Logging

This section provides the setting of log configuration.



System Properties

General Settings **Logging** Language and Style

System log buffer size: 16
kiB

External system log server: 0.0.0.0

External system log server port: 514

Log output level: Debug

Cron Log Level: Normal

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

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

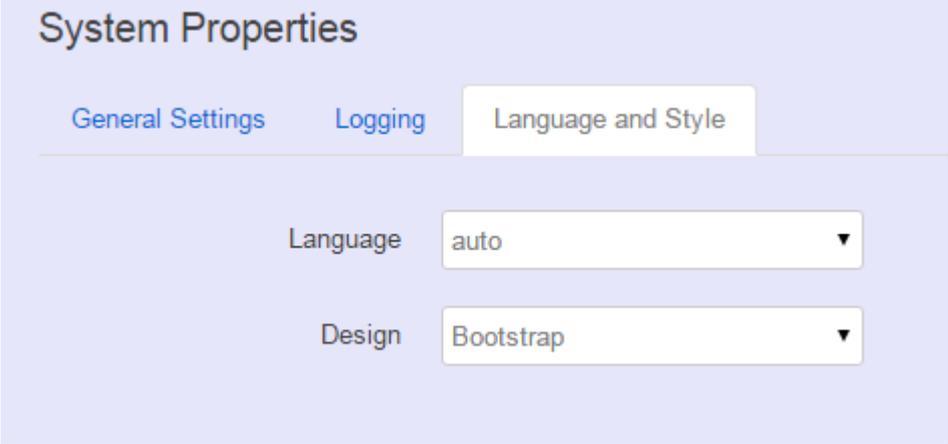
External system log server port: The port number of external log server.

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.

4.3.1.3 Language and Style

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



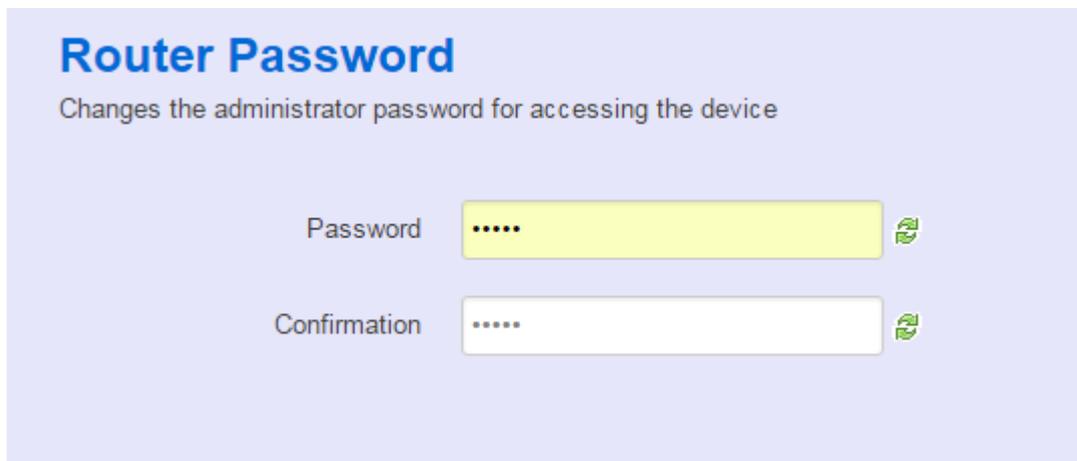
The image shows a screenshot of the 'System Properties' dialog box, specifically the 'Language and Style' tab. The dialog has a light blue background and a title bar. At the top, there are three tabs: 'General Settings', 'Logging', and 'Language and Style'. The 'Language and Style' tab is selected and highlighted. Below the tabs, there are two settings:

- Language:** A dropdown menu with 'auto' selected.
- Design:** A dropdown menu with 'Bootstrap' selected.

4.3.2 Administration

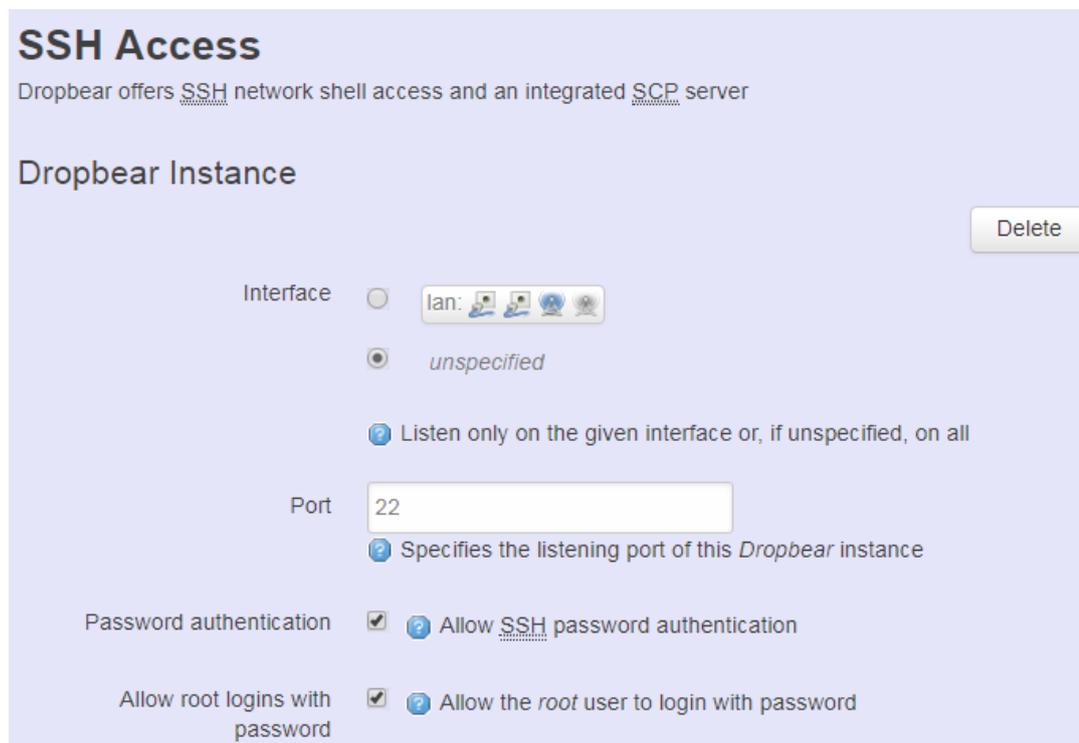
4.3.2.1 Router Password

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



4.3.2.2 SSH Access

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



Interface: Select the interface.

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

Password authentication: Enable/Disable SSH password authentication.

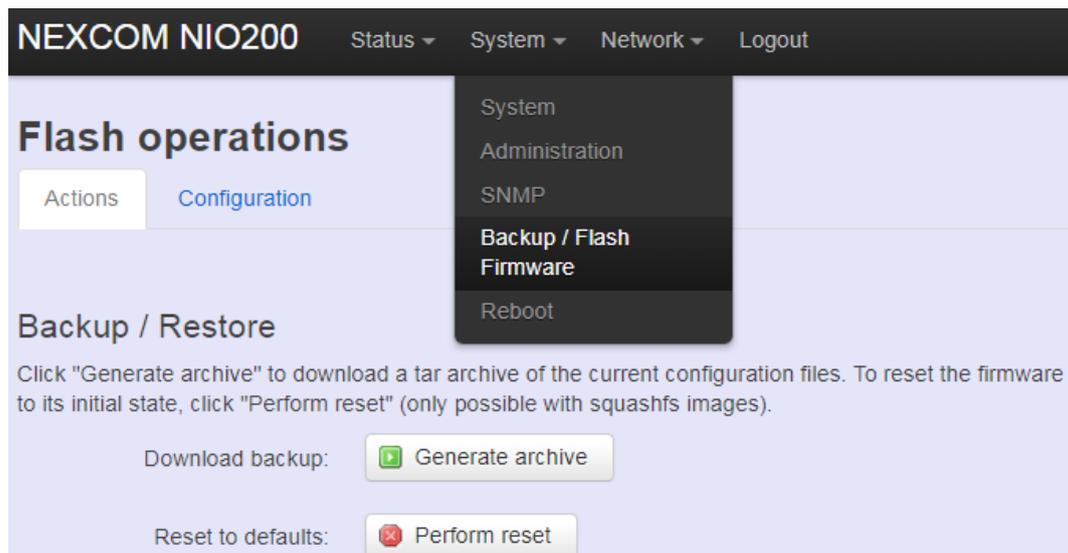
Allow root logins with password: Enable/Disable the *root* user to login with password.

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



4.3.3 Backup/Flash Firmware

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

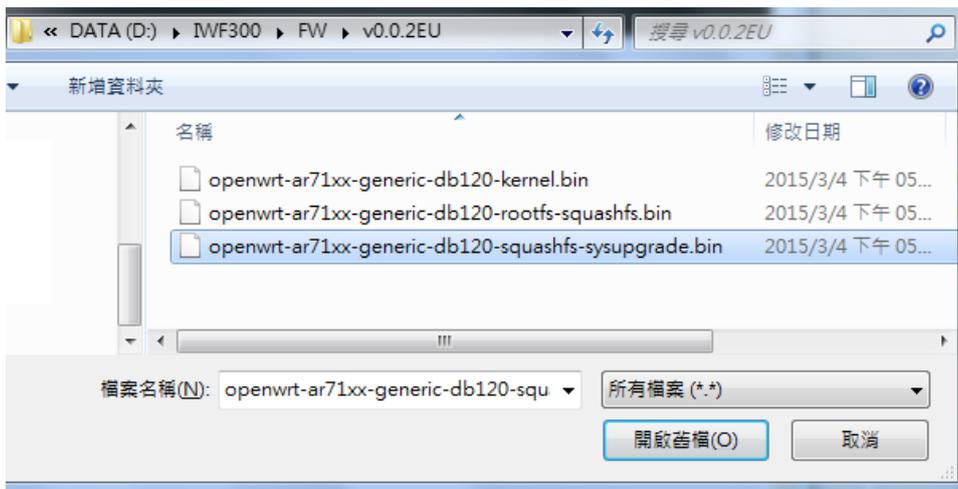


4.3.3.1 Upgrade Firmware

- 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:

System - Flashing...

The system is flashing now.

DO NOT POWER OFF THE DEVICE!

Wait a few minutes before you try to reconnect. It might be necessary to renew the address of your computer to reach the device again, depending on your settings.



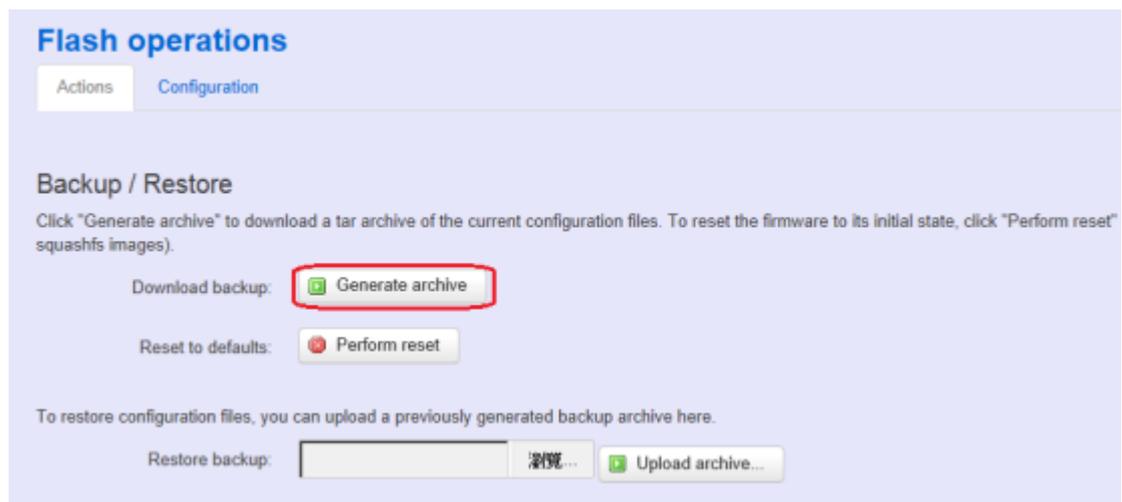
Waiting for changes to be applied...

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

4.3.3.2 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.

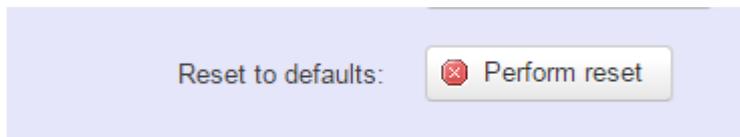
To restore previous configuration, user need to browse the backup file and then press “Upload archive...” button as below:



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.

4.3.3.3 Reset to default

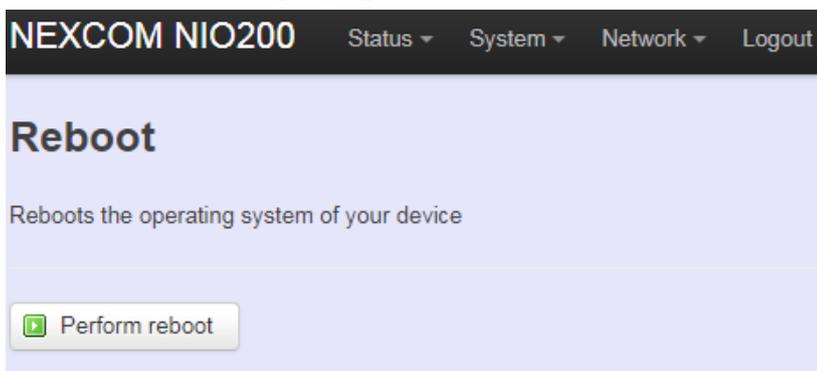
To reset NIO200 to factory default configuration, user will need to press “Perform reset” button as below.



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.

4.3.4 Reboot

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



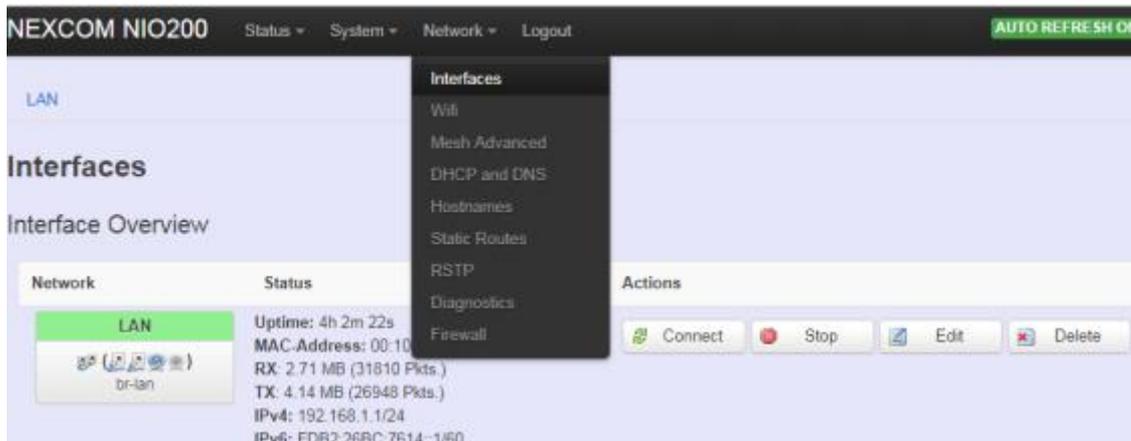


4.4 Network

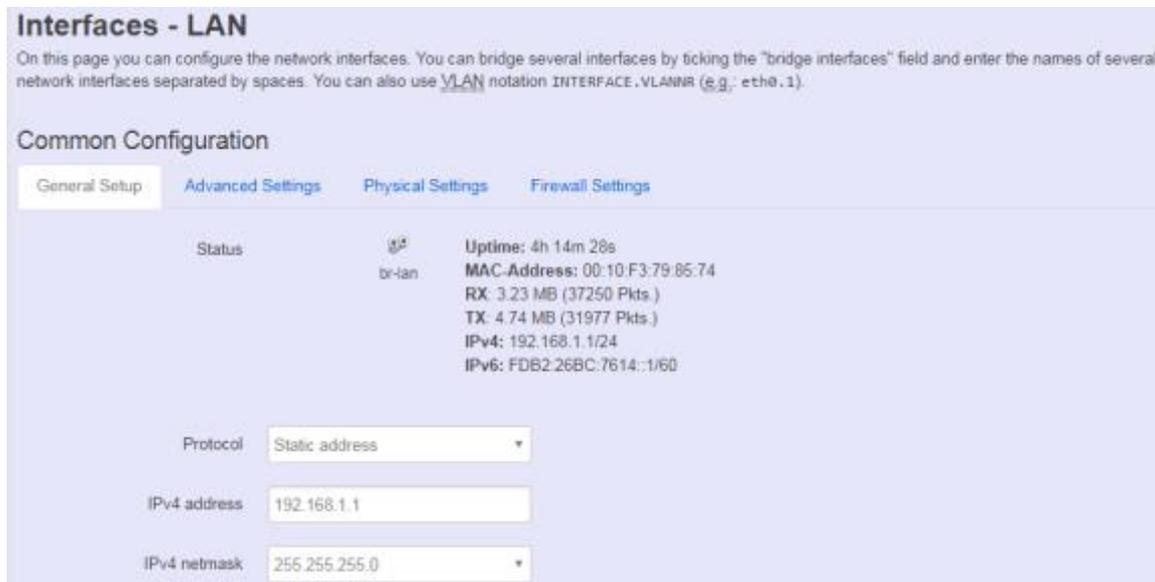
4.4.1 Interfaces

4.4.1.1 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

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.





LAN

Interfaces - LAN

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. You can also use VLAN notation INTERFACE.VLANID (e.g., eth0.1).

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

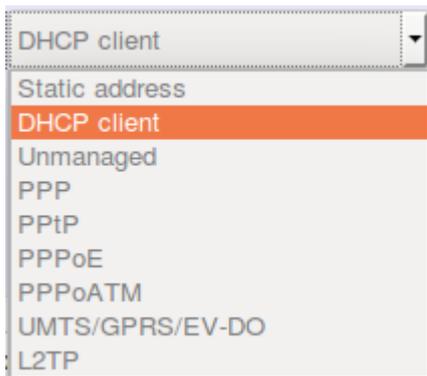
Status: br-lan Uptime: 2d 11h 12m 20s
 MAC-Address: 00:10:F3:52:AD:8B
 RX: 80.07 MB (735059 Pkts.)
 TX: 131.34 MB (893894 Pkts.)
 IPv4: 192.168.1.11/24
 IPv6: FDB2:26BC:7614::1/60

Protocol: Static address

IPv4 address: 192.168.1.11

<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 NIO200WMR

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 NIO200WMR

PPPoE

For cable modem or ADSL user, link NIO200WMR 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"/> ? Required for certain ISPs, e.g. Charter with DOCSIS 3
Use default gateway	<input checked="" type="checkbox"/> ? If unchecked, no default route is configured
Use DNS servers advertised by peer	<input checked="" type="checkbox"/> ? 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"/>	? 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"/>	





General Setup Advanced Settings **Physical Settings** Firewall Settings

Bridge interfaces ⓘ creates a bridge over specified interface(s)

Enable STP ⓘ Enables the Spanning Tree Protocol on this bridge

Interface

- ⓘ Ethernet Switch: "eth0"
- ⓘ VLAN Interface: "eth0.1" (lan)
- ⓘ VLAN Interface: "eth0.2" (wan)
- ⓘ Ethernet Adapter: "eth1" (lan)
- ⓘ VLAN Interface: "eth1.1"
- ⓘ Wireless Network: Master "IWF300_11N_2G_PM" (lan)
- ⓘ Wireless Network: Mesh "IWF300_11A_5G_PM" (lan)
- ⓘ Custom Interface:

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>

DHCP Server

General Setup Advanced Settings IPv6 Settings

Ignore interface ⓘ Disable DHCP for this interface.

Start
 ⓘ Lowest leased address as offset from the network address.

Limit
 ⓘ Maximum number of leased addresses.

Leasetime
 ⓘ Expiry time of leased addresses, minimum is 2 minutes (2m).





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 three 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.





4.4.2 Wi-Fi

4.4.2.1 Wireless Overview

The screenshot displays the 'Wireless Overview' section. At the top, there are three tabs: 'radio0: Mesh "Test"', 'radio0: Mesh "backbone"', and 'radio1: Mesh "MESH_CAN4"'. The main content is divided into two sections: 'Generic MAC80211 802.11an (radio0)' and 'Generic MAC80211 802.11an (radio1)'. Each radio interface section lists SSIDs with their respective modes, MAC addresses, and encryption settings. Action buttons like 'Scan', 'Add', 'Disable', 'Enable', 'Edit', and 'Remove' are provided for each SSID. Below this, the 'Associated Stations' section features a table with the following data:

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 networks:

- NEXCOM_2_4G**: Channel: 1 | Mode: Master | BSSID: 00:10:F3:32:7C:6F | Encryption: WPA2 - 802.1X (92% signal)
- O2O4**: Channel: 1 | Mode: Master | BSSID: 84:C9:B2:68:4D:B2 | Encryption: WPA2 - PSK (62% signal)
- 168**: Channel: 1 | Mode: Master | BSSID: B4:B3:62:C2:A0:7D | Encryption: WPA2 - PSK (75% signal)
- NEXCOM_2_4G**: Channel: 1 | Mode: Master | BSSID: 00:10:F3:32:7B:7F | Encryption: WPA2 - 802.1X (48% signal)

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

The screenshot shows the configuration for a radio interface. It lists the following SSIDs:

- IWF300_11N_2G_PM**: Mode: Master | BSSID: 00:10:F3:30:8A:22 | Encryption: WPA PSK (TKIP, CCMP) (78% signal)
- OpenWrt**: Mode: Master | BSSID: 02:10:F3:30:8A:22 | Encryption: None (0% signal)

The 'OpenWrt' entry is highlighted with a red box, indicating it is the newly added virtual AP.

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.

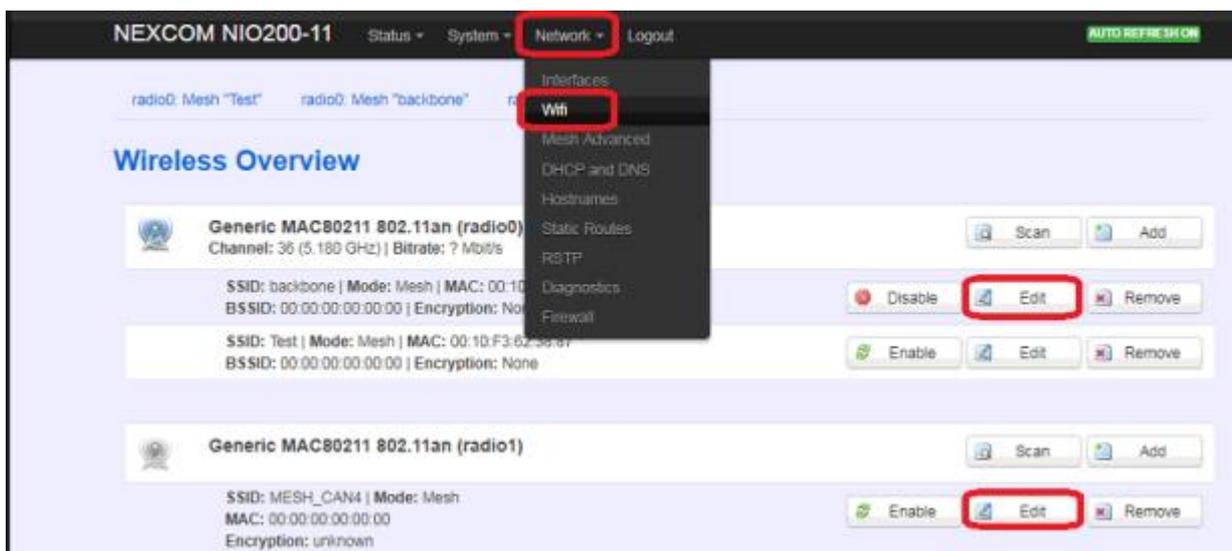
4.4.2.2 Associated Stations

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

4.4.2.3 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

Disable

Operating frequency

Mode

Channel

Width

N

auto

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 ISO/IEC 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 shows the NEXCOM NIO200-11 web interface. At the top, there is a navigation bar with 'Status', 'System', 'Network', and 'Logout' links, and an 'AUTO REFRESH ON' button. Below the navigation bar, there are four input fields: 'Distance Optimization', 'Fragmentation Threshold', 'RTS/CTS Threshold', and 'Transmitter/Receiver Antenna' (with radio buttons for '1Tx1R' and '2Tx2R'). The 'Interface Configuration' section is expanded, showing two tabs: 'General Setup' and 'Wireless Security'. The 'General Setup' tab is active, displaying 'ESSID/Mesh ID' as 'backbone', 'Mode' as 'Mesh_802.11s', and 'Network' selection options (checkboxes for 'lan' and 'create'). A note at the bottom of the 'Interface Configuration' section reads: '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>

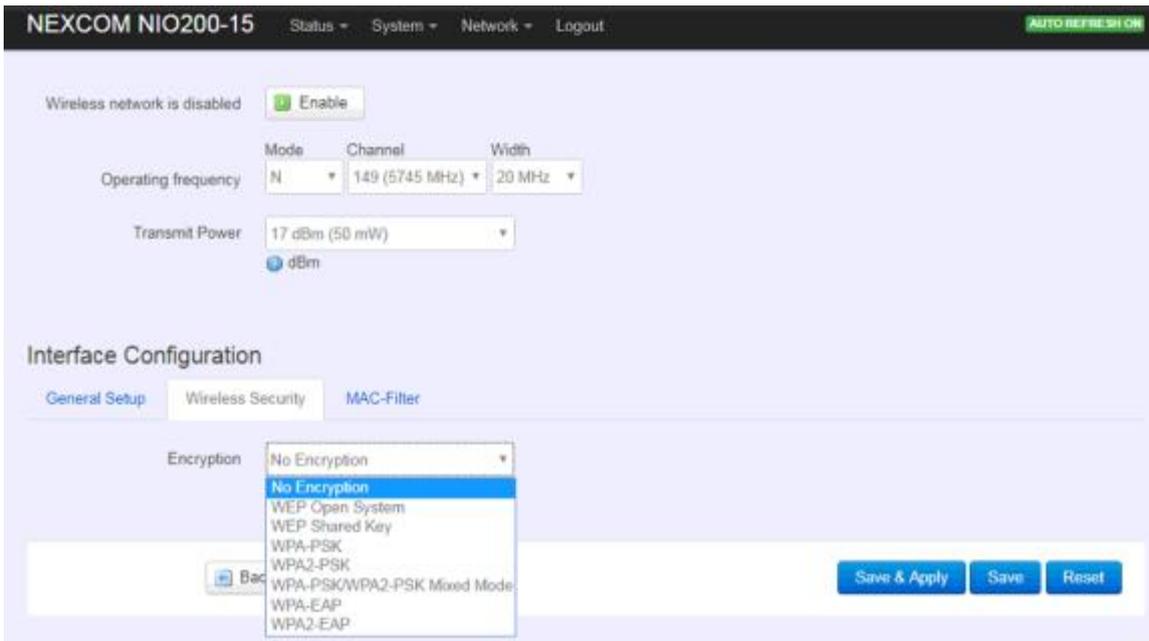
ESSID: Edit the SSID or Mesh ID.

Mode: Select operation mode

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

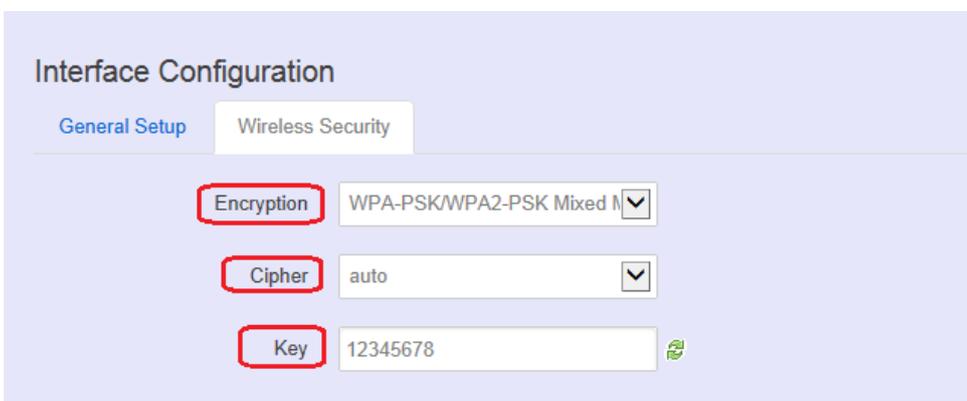
<Wireless Security>





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

Cipher

Key 

The cycle icon will display the characters you just input.

<MAC filter>

Interface Configuration

General Setup Wireless Security **MAC-Filter**

MAC-Address Filter

MAC-List

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

4.4.3 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.

4.4.3.1 Mesh Advanced

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	327 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

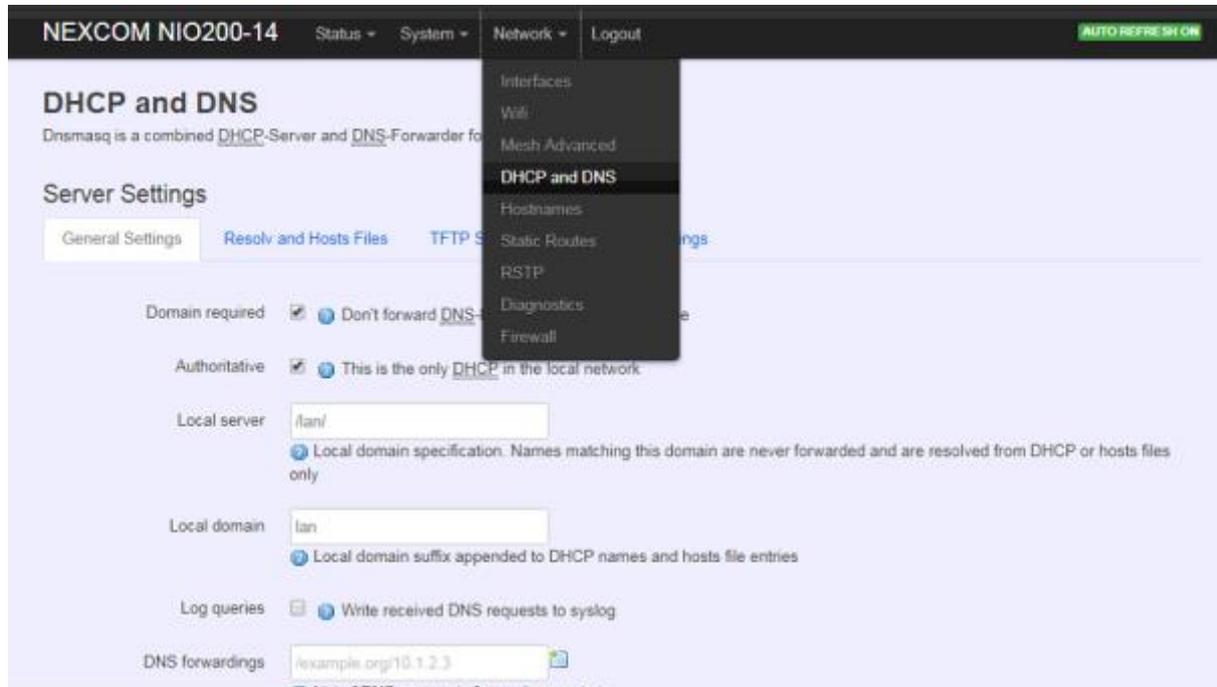
Dest addr	Next hop	iface
00:10:F3:62:38:87	00:10:F3:62:38:87	wlan0
00:10:F3:62:38:81	00:10:F3:62:38:81	wlan0
00:10:F3:6E:E6:9C	00:10:F3:62:38:81	wlan0

- 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



4.4.4 DHCP and DNS

A combined DHCP-Server and DNS-Forwarder for NAT firewall is provided in NIO200WMR. 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.



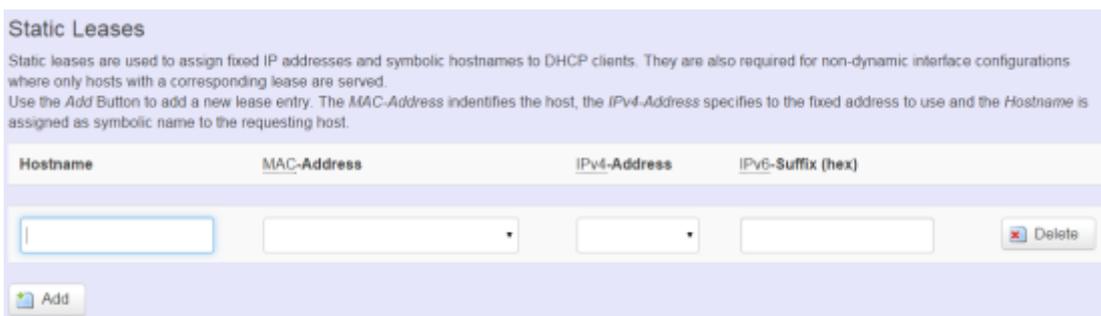


Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients by calculating MAC-Address. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.



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).

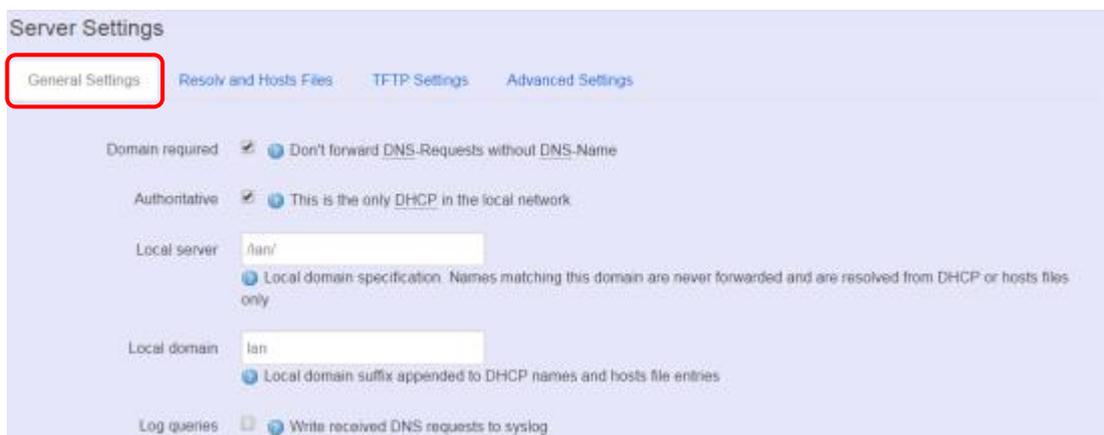


Delete: delete the followed entry.

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

There are 4 tabs to select more options for DHCP and DNS services in the NIO200WMMR.

4.4.4.1 General Settings





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.

4.4.4.2 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](#)

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

Ignore resolve file

Resolve file
[local DNS file](#)

Ignore `/etc/hosts`

Additional Hosts files

4.4.4.3 TFTP Settings

IWF300 [Status](#) [System](#) [Network](#) [Logout](#) [AUTO REFRESH ON](#)

Server Settings

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

Enable TFTP server

By default, TFTP server is not enabled.





4.4.4.4 Advanced Settings

NEXCOM NIO200-14 Status System Network Logout AUTO REFRESH ON

Server Settings

General Settings Resolv 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.

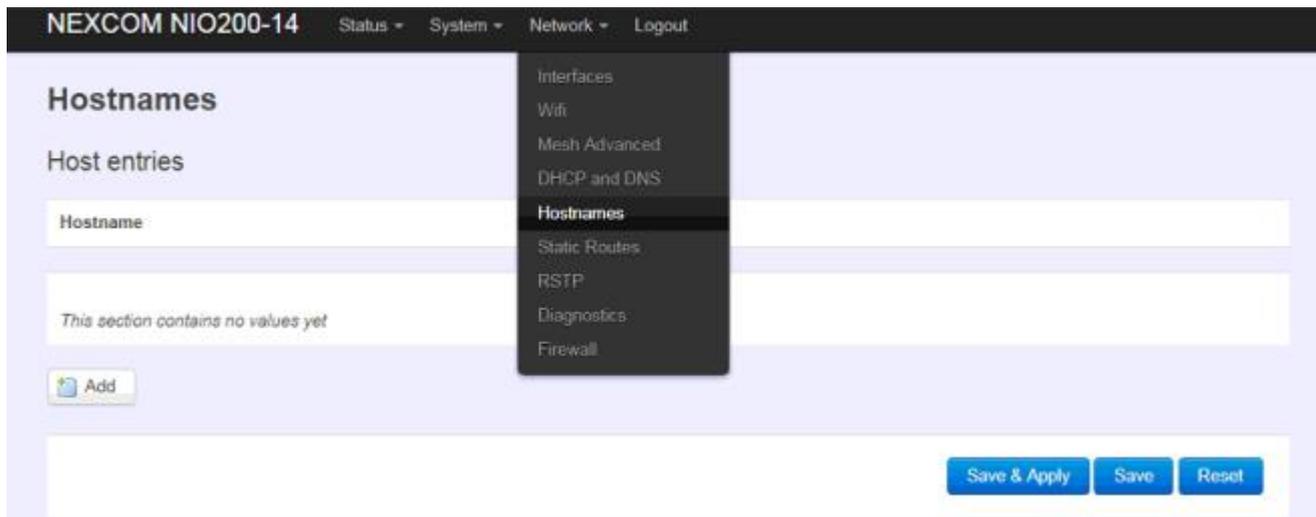
Max. concurrent queries: default value is 150





4.4.5 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.

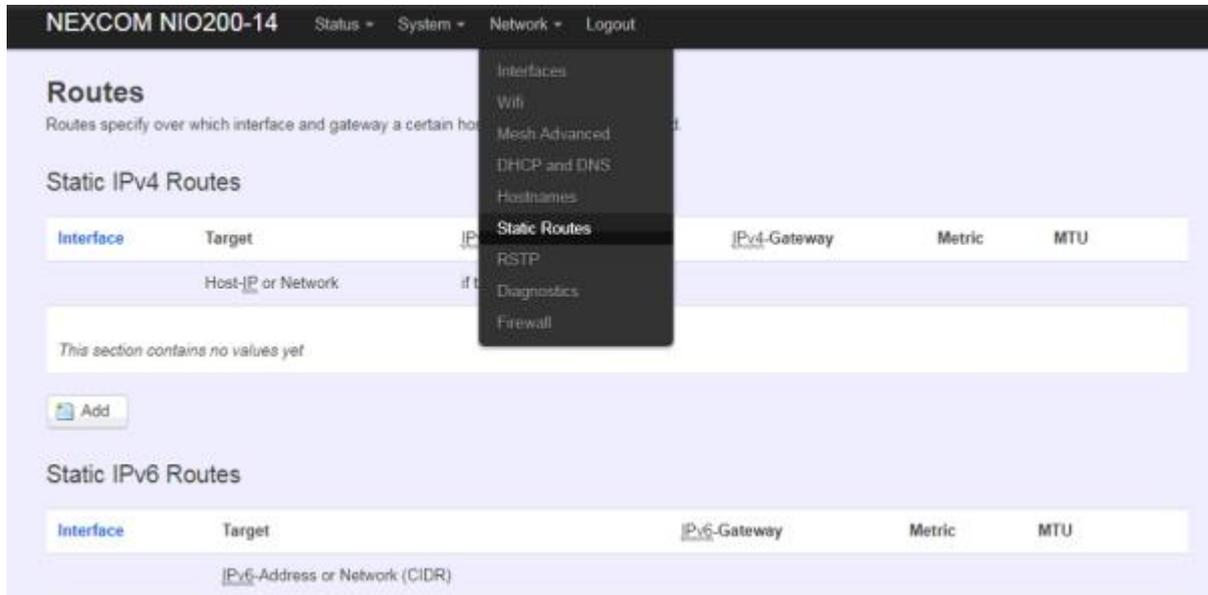




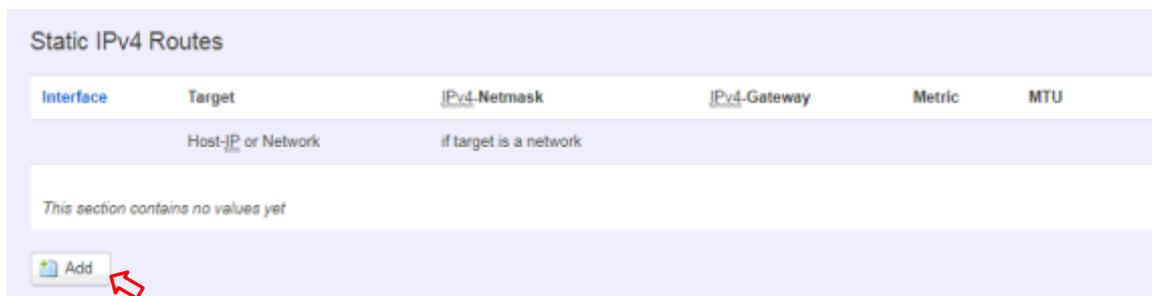
4.4.6 Static Routes

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.



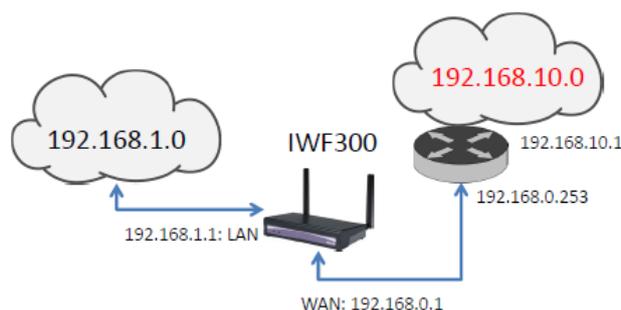
For IPv4 network, scroll down to “Static IPv4 Routes” screen as follows.



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; NIO200WMR 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	
wan	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	
lan			0	1500	Delete

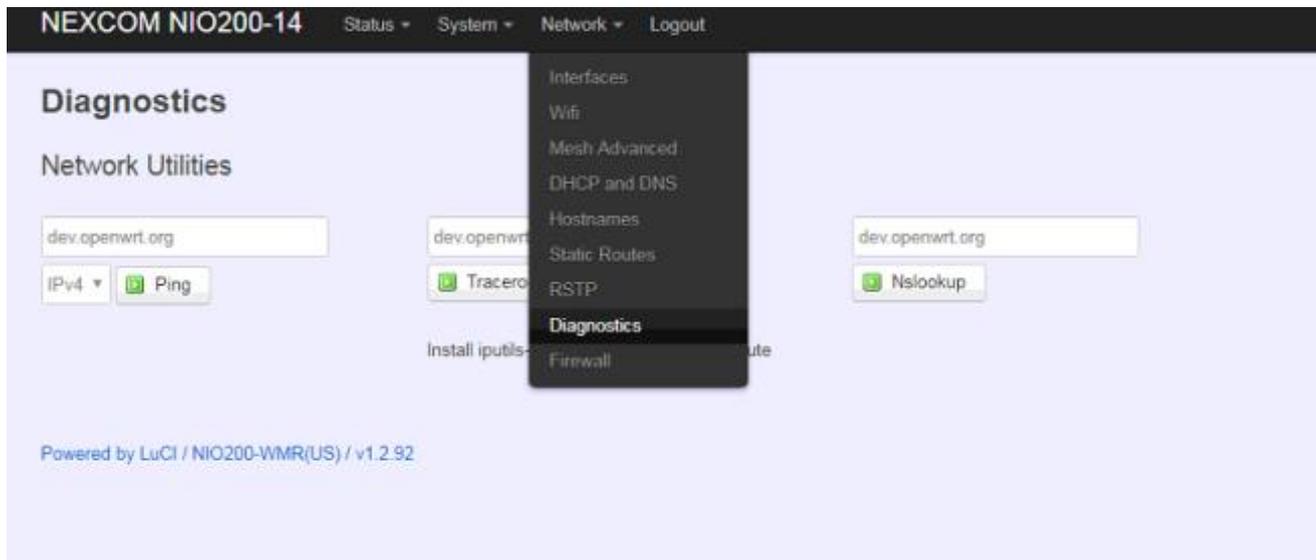
Add





4.4.7 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.

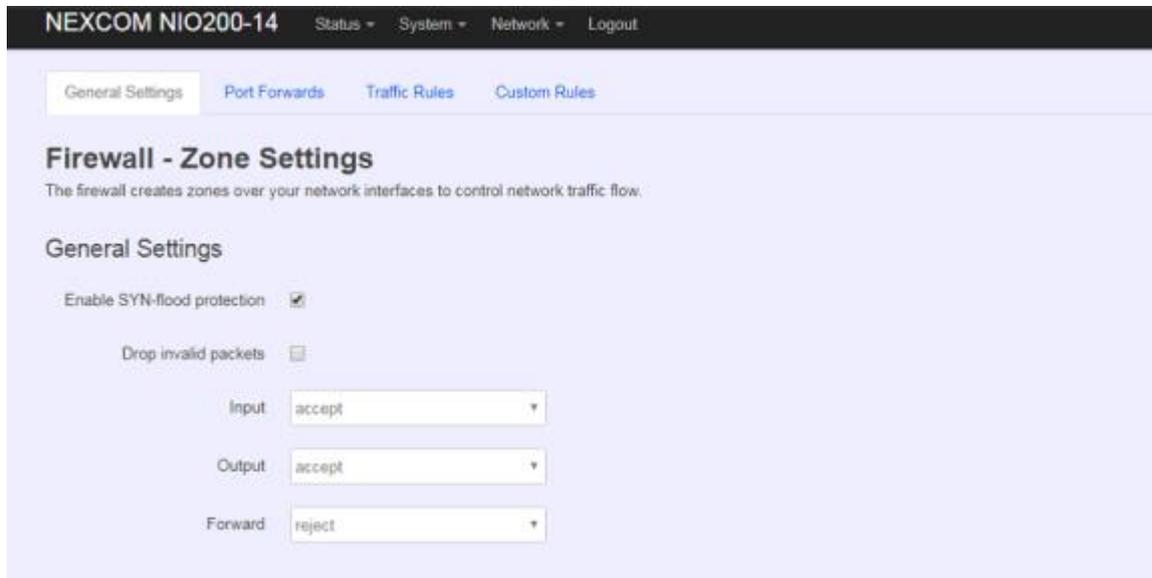
Nslookup: query the Domain Name System (DNS) to obtain domain name or IP address mapping.





4.4.8 Firewall

Click “Network” -> “Firewall” in the GUI menu, and navigate to page configuring firewall attributes in the NIO200WMR.

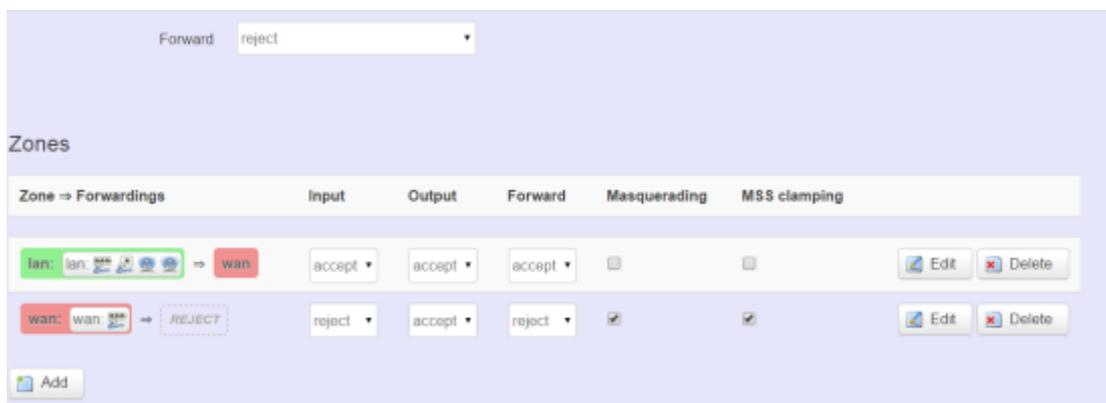


4.4.8.1 General Settings

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.

4.4.8.2 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.

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.

4.4.8.3 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”.





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.

4.4.8.4 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.
```

