

NEXCOM International Co., Ltd.

IoT Automation Solutions Business Group

Dual Radio Dual Band

IEEE 802.11 a/n+b/g/n Industrial Mesh AP

IWF 300/IWF 310 Series

User Manual

NEXCOM International Co., Ltd.

Version 1.2

Published July 2018

www.nexcom.com

CONTENTS

Preface	1
Copyright	1
Disclaimer	1
Acknowledgements	1
Regulatory Compliance Statements	1
Declaration of Conformity	2
RoHS Compliance	5
Safety Information	5
Installation Recommendations	6
Safety Precautions	6
Technical Support and Assistance	7
Conventions Used in this Manual	8
 Chapter 1: Product Overview	 9
1.1 Introduction	9
1.2 Installation	10
1.2.1 IWF 300/IWF 310 Front Panel	10
1.2.2 IWF 300/IWF 310 Rear Panel	11
1.2.3 IWF 300 Dimension	12
1.2.4 IWF 310 Dimension	13
1.2.5 IWF 300 Wall Mount Dimension	14
1.2.6 IWF 310 Wall Mount Dimension	14
1.3 Package Contents	15
 Chapter 2: System Configuration	 16
2.1 Quickly access IWF 300/IWF 310 with web browser	16
2.2 Status	19
2.2.1 Status	19
2.2.2 Overview	19
2.2.2.1 System	20
2.2.2.2 Memory	21
2.2.2.3 Network	21

2.2.2.4	DHCP Leases.....	22
2.2.2.5	DHCPv6 Leases	22
2.2.2.6	Wireless.....	23
2.2.2.7	Associated Stations.....	23
2.2.3	Firewall	24
2.2.4	Routes.....	25
2.2.4.1	ARP	25
2.2.4.2	Active IPv4-Routes	25
2.2.4.3	Active IPv6-Routes	26
2.2.4.4	IPv6 Neighbors.....	26
2.2.5	System Log.....	27
2.2.6	Kernel Log.....	28
2.2.7	Processes.....	29
2.2.8	Real-time Graphic.....	29
2.2.8.1	Load	30
2.2.8.2	Traffic	31
2.2.8.3	Wireless.....	32
2.2.8.4	Connections	33
2.3	System.....	34
2.3.1	System	35
2.3.1.1	General Settings	35
2.3.1.2	Logging	37
2.3.1.3	Language and Style	37
2.3.2	Administration	38
2.3.2.1	Router Password.....	38
2.3.2.2	SSH Access	38
2.3.3	Software	39
2.3.4	Startup.....	40
2.3.5	LED Configuration.....	40
2.3.6	Backup/Flash Firmware	41
2.3.6.1	Upgrade Firmware	41
2.3.6.2	Backup Configuration.....	43
2.3.6.3	Reset to default	44
2.3.6.4	Configuration	44
2.3.7	Reboot.....	45
2.4	Network	46
2.4.1	Interfaces	46

2.4.1.1	Change Default IP Address.....	46
2.4.1.2	Interfaces Overview	47
2.4.1.3	WAN(LAN) Interface Overview	48
2.4.1.4	DHCP Server	51
2.4.2	WiFi	52
2.4.2.1	Wireless Overview.....	52
2.4.2.2	Associated Stations.....	53
2.4.2.3	Wireless configuration	54
2.4.3	Switch.....	59
2.4.4	DHCP and DNS.....	61
2.4.4.1	General Settings	63
2.4.4.2	Resolve and Hosts Files	64
2.4.4.3	TFTP Settings	64
2.4.4.4	Advanced Settings.....	64
2.4.5	Hostnames.....	65
2.4.6	Static Routes	66
2.4.7	Firewall	68
2.4.7.1	General Settings	69
2.4.7.2	Port Forwards	70
2.4.7.3	Traffic Rules	70
2.4.7.4	Custom Rules	72
2.4.8	Diagnostics.....	72
Chapter 3:	Product Specification.....	74
IWF 300.....		74
Main Features		74
Specifications		74
IWF 310.....		78
Main Features		78
Specifications		78
Chapter 4:	Appendix.....	82
4.1	Setting Example	82
4.1.1	How to configure 5G mesh?	82
4.1.2	How to configure 2.4G AP?	83
4.1.3	How to run firmware upgrade?	84
4.1.4	How to restore to default settings?.....	85

PREFACE

This manual is for WLAN service providers or network administrators to set up a network environment using the IWF series product line. It contains step-by-step procedures and graphic examples to guide MIS staff 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

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

Regulatory Compliance Statements

This section provides the FCC compliance statement for Class B devices and describes how to keep the system CE compliant.

Declaration of Conformity

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

IMPORTANT NOTE:**Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA.

Operation of this device is restricted to indoor use only.

This device is intended only for OEM integrators under the following conditions:

The antenna must be installed such that 20 cm is maintained between the antenna and users.

The transmitter module may not be co-located with any other transmitter or antenna.

For all products market in US, OEM has to limit the operation channels in CH1 to CH11 for 2.4G band by supplied firmware programming tool. OEM shall not supply any tool or info to the end-user regarding to Regulatory Domain change.

As long as 3 conditions above are met, further transmitter test will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed.

IMPORTANT NOTE

In the event that these conditions can not be met (for example certain laptop configurations or co-location with another transmitter), then the FCC authorization is no longer considered valid and the FCC ID cannot be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate FCC authorization.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20 cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: YHI-EWF3210K".

Manual Information to the End User

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module in the user's manual of the end product which integrates this module. The end user manual shall include all required regulatory information/warning as shown in this manual.

CE

The product(s) described in this manual complies with all applicable European Union (CE) directives if it has a CE marking. For computer systems to remain CE compliant, only CE-compliant parts may be used. Maintaining CE compliance also requires proper cable and cabling techniques.

RoHS Compliance



NEXCOM RoHS Environmental Policy and Status Update

NEXCOM is a global citizen for building the digital infrastructure. We are committed to providing green products and services, which are compliant with European Union RoHS (Restriction on Use of Hazardous Substance in Electronic Equipment) directive 2011/65/EU, to be your trusted green partner and to protect our environment. RoHS restricts the use of Lead (Pb) < 0.1% or 1,000ppm, Mercury (Hg) < 0.1% or 1,000ppm, Cadmium (Cd) < 0.01% or 100ppm, Hexavalent Chromium (Cr6+) < 0.1% or 1,000ppm, Polybrominated biphenyls (PBB) < 0.1% or 1,000ppm, and Polybrominateddiphenyl Ethers (PBDE) < 0.1% or 1,000ppm. In order to meet the RoHS compliant directives, NEXCOM has established an engineering and manufacturing task force to implement the introduction of green products. The task force will ensure that we follow the standard NEXCOM development procedure and that all the new RoHS components and new manufacturing processes maintain the highest industry quality levels for which NEXCOM are renowned.

The model selection criteria will be based on market demand. Vendors and suppliers will ensure that all designed components will be RoHS compliant.

How to recognize NEXCOM RoHS Products?

For existing products where there are non-RoHS and RoHS versions, the suffix “(LF)” will be added to the compliant product name. All new product models launched after January 2013 will be RoHS compliant. They will use the usual NEXCOM naming convention.

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. CAUTION: DANGER OF EXPLOSION IF BATTERY IS INCORRECTLY REPLACED. REPLACE ONLY WITH THE SAME OR EQUIVALENT TYPE RECOMMENDED BY THE MANUFACTURER. DISCARD USED BATTERIES ACCORDING TO THE MANUFACTURER'S INSTRUCTIONS.

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 clean with a dry cloth.

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.

CHAPTER 1: PRODUCT OVERVIEW

1.1 Introduction

IWF 300/IWF 310 is QCA9344-based industrial-grade AP/Router/ EZ MESH AP designed with IEEE 802.11 b/g/n 2x2 MIMO and IEEE 802.11an 2x2 MIMO technology.

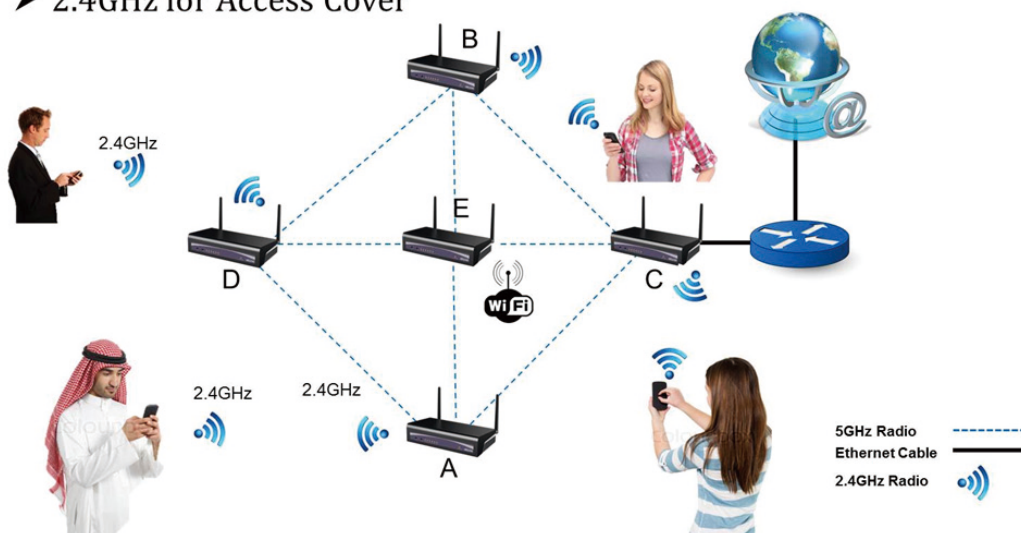
IWF 300/IWF 310 can deliver data rate up to 300mbps/ each radio. In addition, the Radio power can be up to 27dBm for wide range coverage and service. IWF 300 also functions as EZ MESH network Wi-Fi access with cost-effective option.

Key Features:

- ✓ Seamless Wi-Fi coverage for 320 * 320m middle scale facility.
- ✓ Reliable 5GHz Mesh Backbone plus 2.4GHz Access Point.
- ✓ High performance data/video transmitting after 4+ hops.
- ✓ Best path selection for Self-Forming/Self-Healing.
- ✓ Design for Industrial grade environment (-40~80).
- ✓ IWF 310 high RF power for 5GHz & 2.4GHz

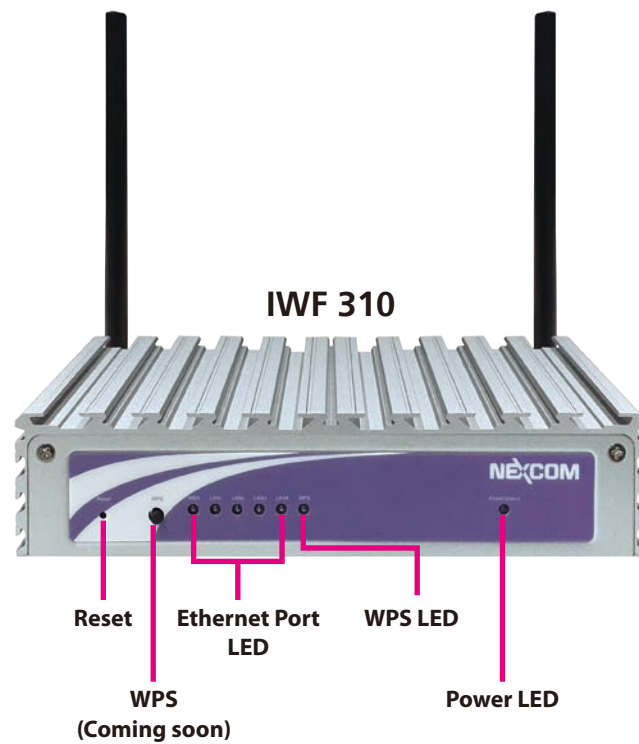
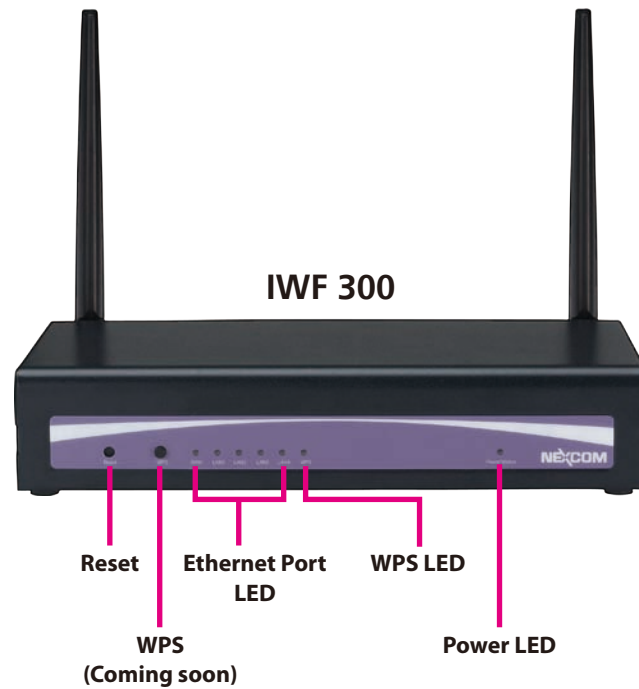
IWF 300/IWF 310 Mesh Application Scenarios

- 5GHz for Mesh Backbone
- 2.4GHz for Access Cover

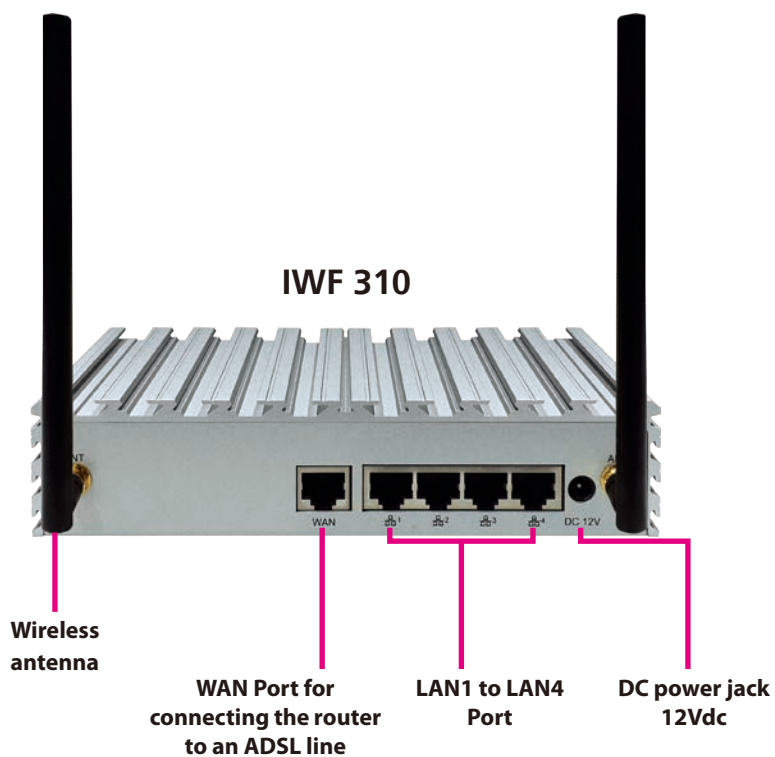
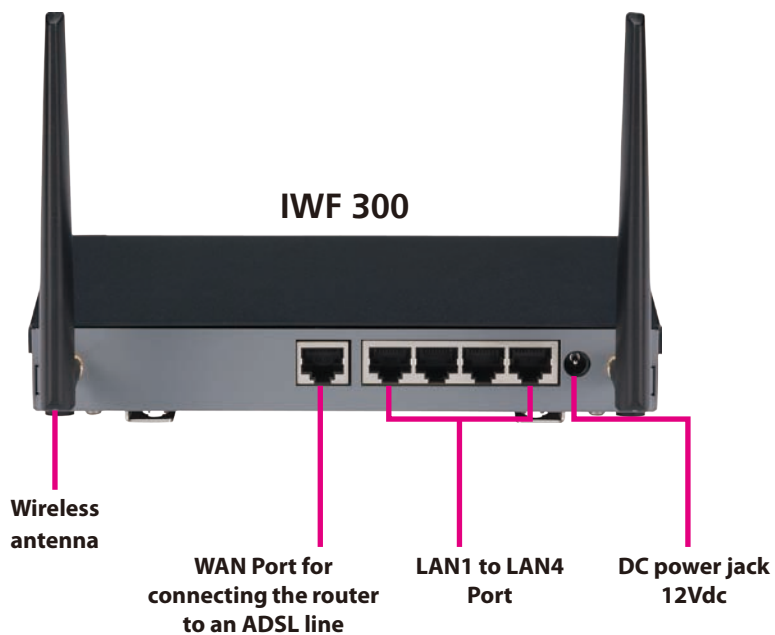


1.2 Installation

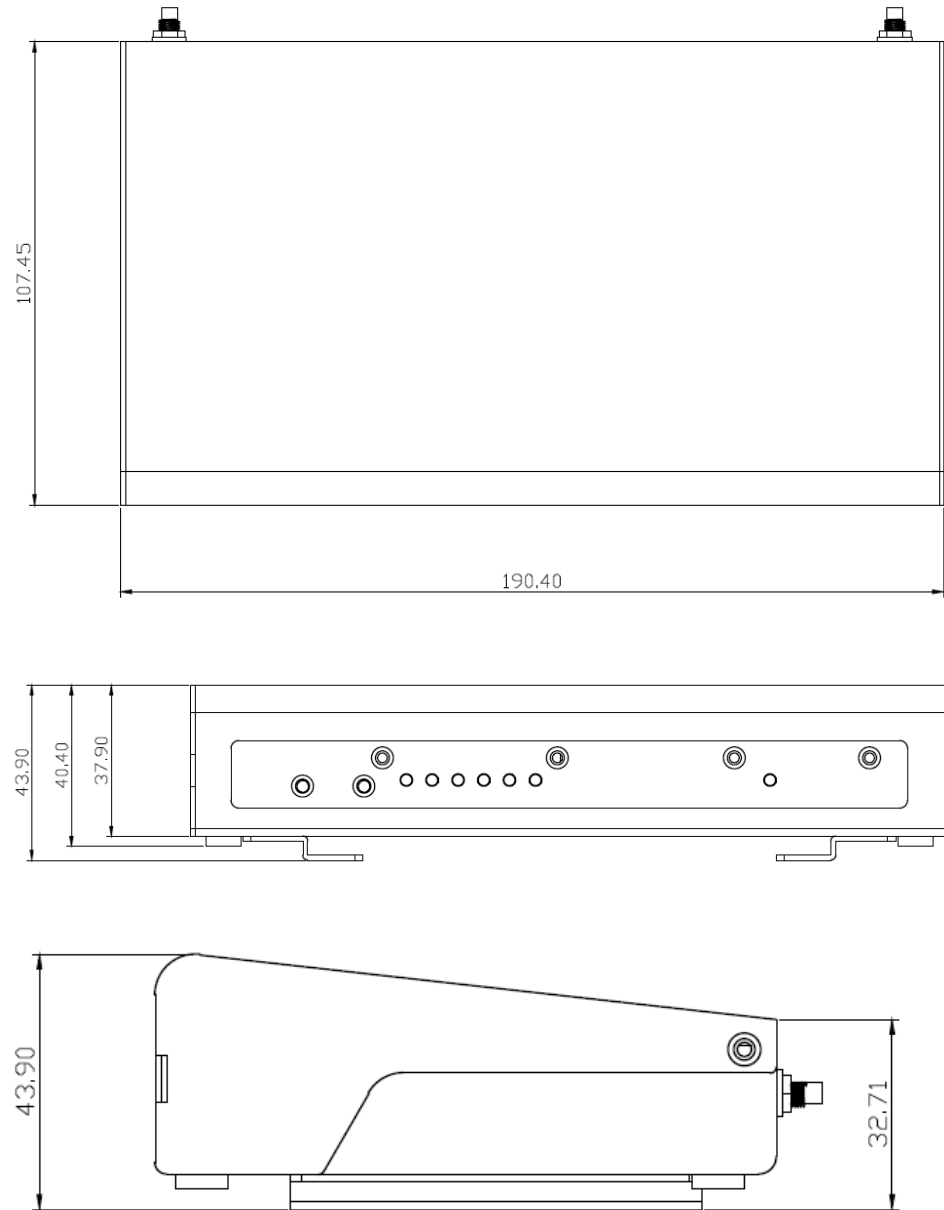
1.2.1 IWF 300/IWF 310 Front Panel



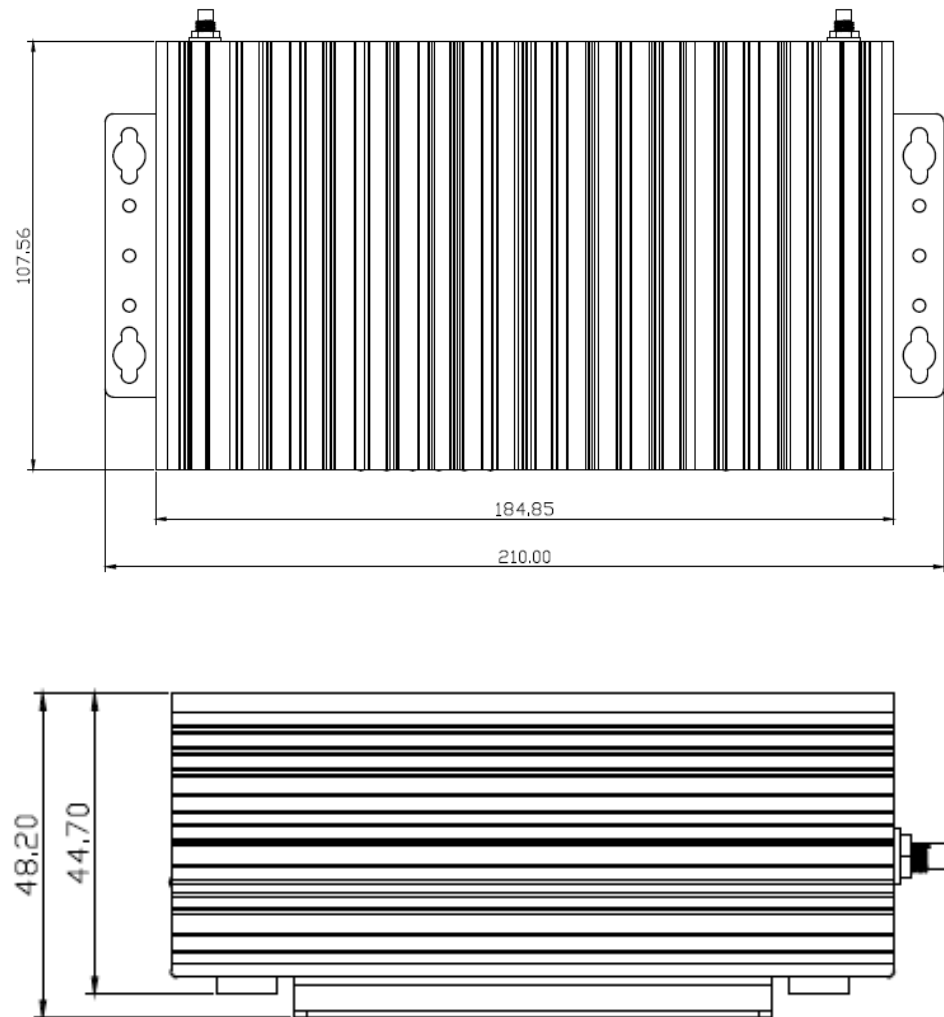
1.2.2 IWF 300/IWF 310 Rear Panel



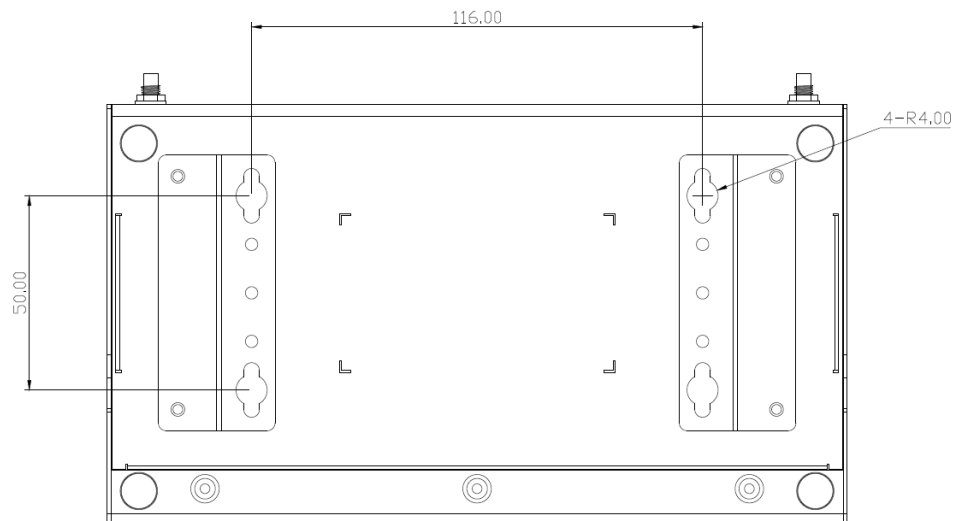
1.2.3 IWF 300 Dimension



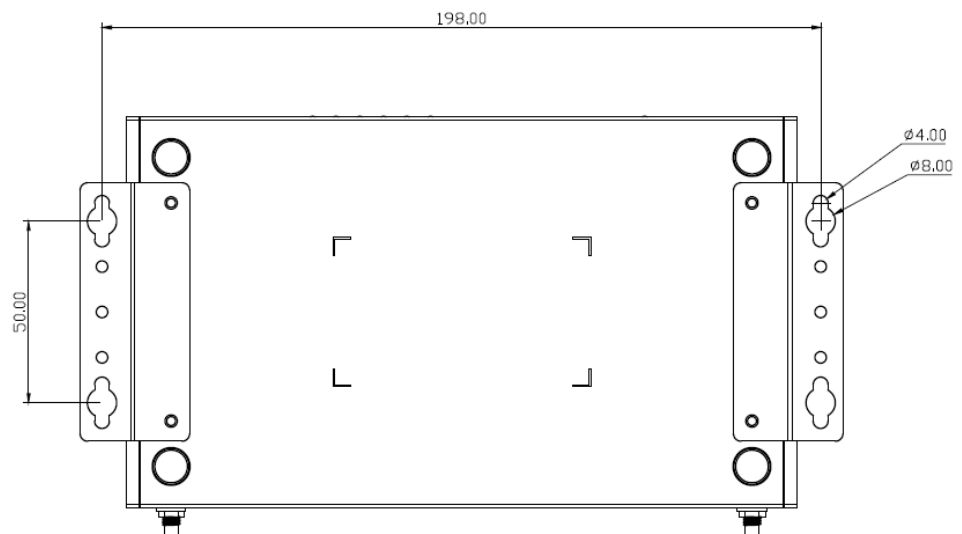
1.2.4 IWF 310 Dimension



1.2.5 IWF 300 Wall Mount Dimension



1.2.6 IWF 310 Wall Mount Dimension



1.3 Package Contents

IWF 300/IWF 310 unit x 1	
Dual band antenna x 2	
Wall-mount kit x 1	
AC-DC power adaptor x 1	

CHAPTER 2: SYSTEM CONFIGURATION

2.1 Quickly access IWF 300/IWF 310 with web browser

Login

To access the IWF 300/ IWF 310 device, you can open a browser to access the Web GUI via default IP address **192.168.1.1**

The default administrator login settings are:

Login: **root**

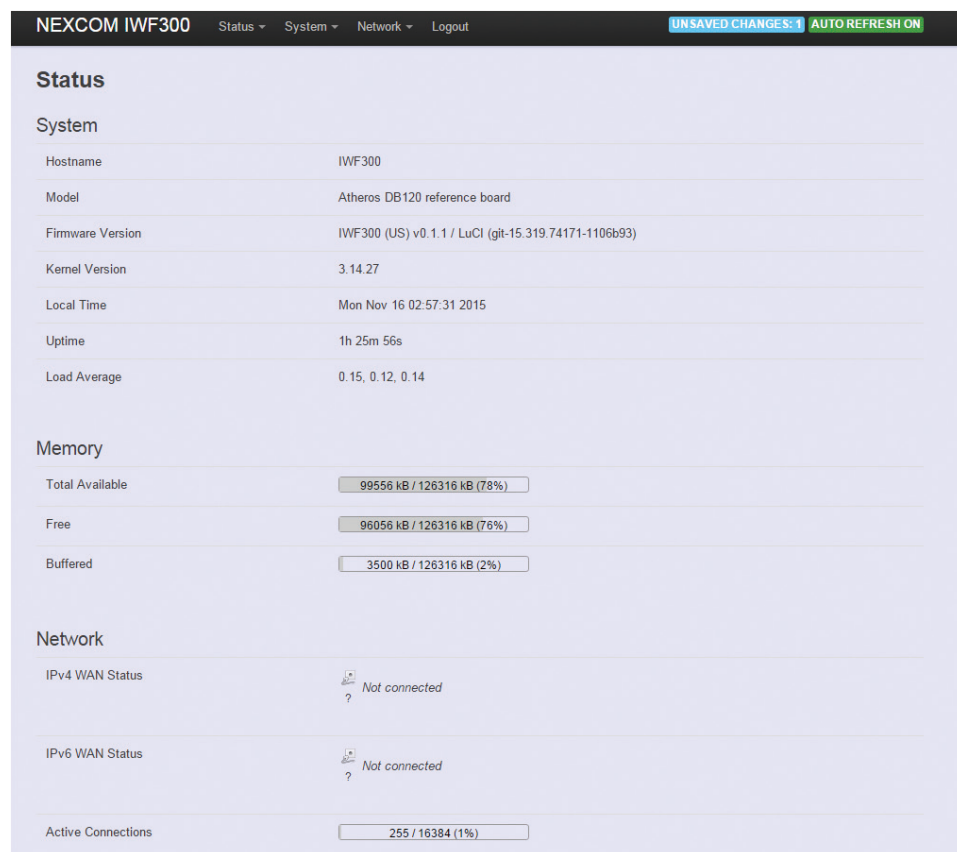
Password: **admin**

The first page you would see the login page like below screenshot:



The screenshot shows the NEXCOM IWF300 web interface. At the top, there is a black header with the text "NEXCOM IWF300". Below this, the main content area has a light blue background. The title "Authorization Required" is displayed in bold, followed by the instruction "Please enter your username and password." There are two input fields: "Username" with the value "root" and "Password" with masked characters "*****". Below the input fields, there are two buttons: "Login" (highlighted with a red box) and "Reset". At the bottom, a footer line reads "Powered by LuCI (git-15.319.74171-1106b93) / IWF300 (US) v0.1.1".



After successful administrator login you will see the “Status” page of the device Web management interface with current information of System, Memory, Network, DHCP, Wireless, and Associated Stations. The device is now ready for configuration.



The screenshot shows the NEXCOM IWF300 Status page. At the top, there is a navigation bar with links for Status, System, Network, and Logout. A status bar indicates 'UNSAVED CHANGES: 1' and 'AUTO REFRESH ON'. The main content area is titled 'Status' and contains three sections: System, Memory, and Network.

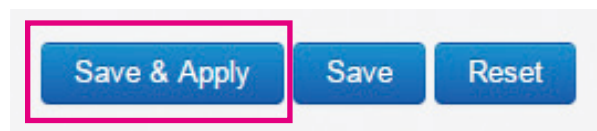
System	
Hostname	IWF300
Model	Atheros DB120 reference board
Firmware Version	IWF300 (US) v0.1.1 / LuCI (git-15.319.74171-1106b93)
Kernel Version	3.14.27
Local Time	Mon Nov 16 02:57:31 2015
Uptime	1h 25m 56s
Load Average	0.15, 0.12, 0.14

Memory	
Total Available	99556 kB / 126316 kB (78%)
Free	96056 kB / 126316 kB (76%)
Buffered	3500 kB / 126316 kB (2%)

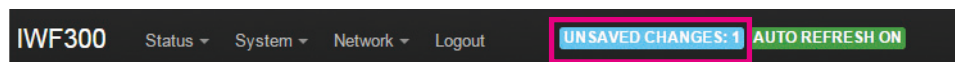
Network	
IPv4 WAN Status	 Not connected
IPv6 WAN Status	 Not connected
Active Connections	255 / 16384 (1%)

Saving Changes

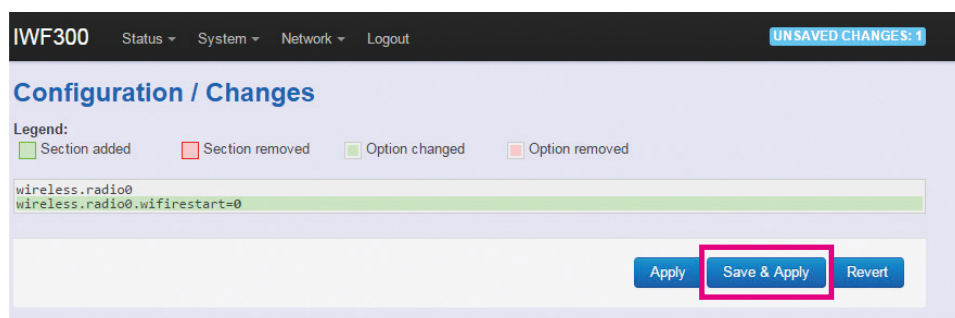
Save & apply the configuration in WebUI after you do the changes at the bottom of WebUI.



Unsaved Changes

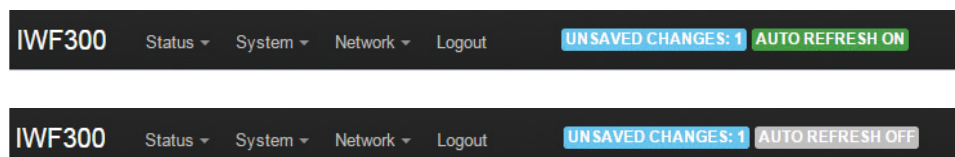


“UNSAVED CHANGES” provides the help to see the parameters which were not saved & applied.



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

Auto Refresh



Click the “AUTO REFRESH” button; to turn on/off WebUI refresh function automatically.

2.2 Status

2.2.1 Status

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



2.2.2 Overview

To see the overall status of IWF 300 and IWF 310, click “Overview” to displays the current settings of the IWF 300/IWF 310's ports and some system information.

2.2.2.1 System

System	
Hostname	IWF300
Model	Atheros DB120 reference board
Firmware Version	OpenWrt (US) v0.1.0 / LuCI (git-15.216.69575-bb7ea3e)
Kernel Version	3.14.27
Local Time	Mon Jan 4 08:35:02 2016
Uptime	4d 4h 56m 40s
Load Average	0.04, 0.09, 0.13

Hostname:	Displays IWF 300/IWF 310 name
Model:	Displays IWF 300/IWF 310 HW basic information
Firmware Version:	Displays IWF 300
Kernel Version:	Displays IWF 300/IWF 310 current Kernel version.
Local Time:	Displays IWF 300/IWF 310 current date and time.
Uptime:	Displays how long IWF 300 /IWF 310 has been operating since last boot-up.uptime.
Load Average:	CPU average loading. For example:

Load Average	0.94, 0.43, 0.24
--------------	------------------

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

2.2.2.2 Memory



Memory	
Total Available	101876 kB / 126316 kB (80%)
Free	99156 kB / 126316 kB (78%)
Buffered	2720 kB / 126316 kB (2%)

Total Available: Displays IWF 300/IWF 310 available current memory.

Free: Displays IWF 300/IWF 310 current free memory.

Buffered: Displays IWF 300/IWF 310 memory using for buffering.

2.2.2.3 Network

Network	
IPv4 WAN Status	 Type: dhcp Address: 10.15.1.138 Netmask: 255.255.255.0 Gateway: 10.15.1.254 DNS 1: 10.1.1.2 DNS 2: 10.1.1.6 DNS 3: 10.1.1.5 DNS 4: 10.1.1.1 DNS 5: 10.1.1.29 Connected: 7h 31m 37s
IPv6 WAN Status	 Not connected
Active Connections	38 / 16384 (0%)

IPv4 WAN Status: Displays current connecting IPv4 information.

IPv6 WAN Status: Displays current connecting IPv6 information.

Active Connections: Displays current active connections.

2.2.2.4 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 IWF 300/IWF 310 including IPv4, MAC address and leasing time

2.2.2.5 DHCPv6 Leases


Hostname	IPv6-Address	DUID	Leasetime remaining
River-Ubuntu	fdcf:68c3:19eb::10b/128	0004767fcd07324b68cbab02958b2991f645	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 IWF 300/IWF 310 including IPv6, DUID and leasing time.

2.2.2.6 Wireless


Wireless

Generic 802.11abgn Wireless Controller (radio0)


61%

SSID: IWF300_11N_2G_PM
Mode: Master
Channel: 7 (2.442 GHz)
Bitrate: 92.5 Mbit/s
BSSID: 00:10:F3:30:8A:22
Encryption: WPA PSK (TKIP, CCMP)

Generic 802.11abgn Wireless Controller (radio1)


0%

SSID: IWF300_11A_5G_PM
Mode: Master
Channel: 44 (5.220 GHz)
Bitrate: ? Mbit/s
BSSID: 00:0E:8E:67:64:F5
Encryption: WPA PSK (TKIP, CCMP)





This displays wireless information about IWF 300/IWF 310 for radio 0 & 1.

Radio0 default setting is Access Point.

Radio1 default setting is Mesh Access.

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.

2.2.2.7 Associated Stations

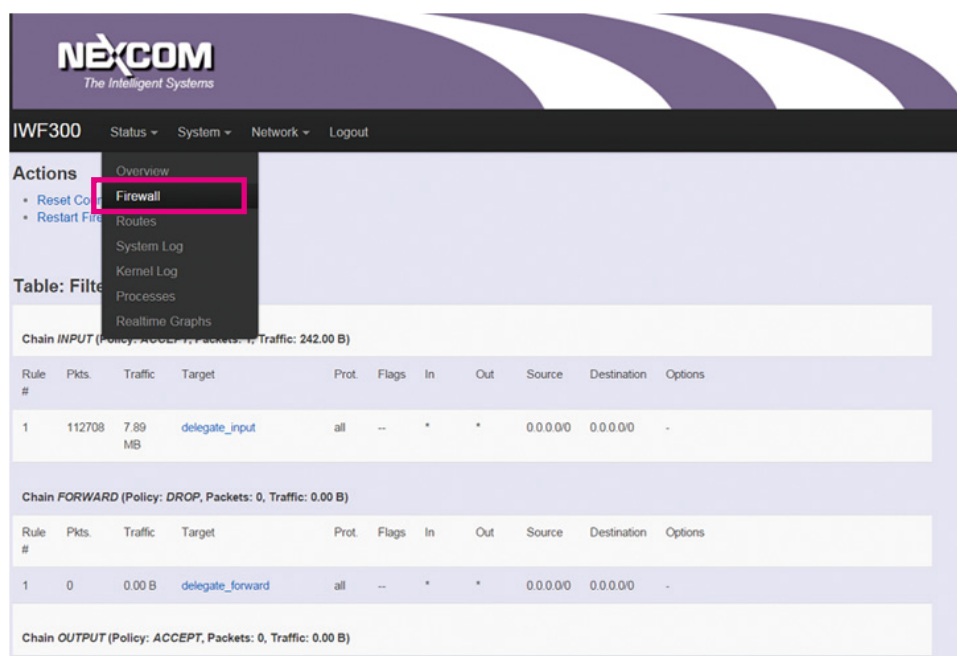
Associated Stations						
MAC-Address	Network	Signal	Noise	RX Rate	TX Rate	
 94:A1:A2:87:6F:08	Master "IWF300_11N_2G_PM"	-54 dBm	-95 dBm	54.0 Mbit/s, MCS 0, 20MHz	54.0 Mbit/s, MCS 0, 20MHz	
 80:19:34:C9:04:00	Master "IWF300_11N_2G_PM"	-61 dBm	-95 dBm	180.0 Mbit/s, MCS 12, 40MHz	150.0 Mbit/s, MCS 7, 40MHz	
 08:3E:8E:67:64:03	Master "IWF300_11N_2G_PM"	-70 dBm	-95 dBm	121.5 Mbit/s, MCS 6, 40MHz	108.0 Mbit/s, MCS 11, 40MHz	
 00:0D:F0:AC:C8:63	Master "IWF300_11N_2G_PM"	-73 dBm	-95 dBm	1.0 Mbit/s, MCS 0, 20MHz	26.0 Mbit/s, MCS 3, 20MHz	

Displays current associated device information (Personal Computers or electronic devices) with IWF 300/IWF 310, including device's MAC address, signal level, noise, connecting data rate.

2.2.3 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.

The settings in Firewall are suggested to keep it as factory default.



Chain INPUT (Policy: ACCEPT, Packets: 17, Traffic: 242.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	112708	7.89 MB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain OUTPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

2.2.4 Routes

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

2.2.4.1 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 ARP table in IWF 300/IWF 310, including IPv4 address, MAC address and connecting interface.

2.2.4.2 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.

2.2.4.3 Active IPv6-Routes

Network	Target	Source	Metric	Table
lan	fdfe:68c3:19eb:0:e5df:2aba:f91:5221		0	main
lan	fdfe:68c3:19eb::/64		1024	main
wan	ff02::1		0	local
wan	ff02::2		0	local
wan	ff02::c		0	local
wan	ff02::1:2		0	local
wan	ff02::1:3		0	local
wan	ff02::1:ff50:9e09		0	local
lan	ff00::/8		256	local
(eth0)	ff00::/8		256	local
wan	ff00::/8		256	local
lan	ff00::/8		256	local
lan	ff00::/8		256	local

Displays active IPv6 routing table of WAN and LAN port.

2.2.4.4 IPv6 Neighbors

IPv6-Address	MAC-Address	Interface
fdfe:68c3:19eb:0:1f4:f243:8e92:e881	80:19:34:c9:04:00	lan
fdfe:68c3:19eb:0:e5df:2aba:f91:5221	80:19:34:c9:04:00	lan
fdfe:68c3:19eb::3b0	00:0d:f0:ac:c8:63	lan
fdfe:68c3:19eb:0:21cf:78b5:a2c9:e438	00:0d:f0:ac:c8:63	lan
fdfe:68c3:19eb:0:b815:35d6:d6b7:df68	00:0d:f0:ac:c8:63	lan
fdfe:68c3:19eb:0:691a:9a70:b879:924d	80:19:34:c9:04:00	lan
fdfe:68c3:19eb:0:468:1e7:d4fe:8c9a	9c:2a:70:1b:4c:9d	lan
fdfe:68c3:19eb:0:f118:d10c:ab71:1676	80:19:34:c9:04:00	lan
fdfe:68c3:19eb:0:7c3e:bc4c:52e3:de5a	00:0d:f0:ac:c8:63	lan
fdfe:68c3:19eb:0:6046:1236:d6c8:82c1	00:0d:f0:ac:c8:63	lan
fdfe:68c3:19eb:0:c654:44ff:fede:fea5	c4:54:44:de:fe:a5	lan
fdfe:68c3:19eb:0:e151:5f16:e22f:fc7c	c4:54:44:de:fe:a5	lan
fdfe:68c3:19eb:0:61ad:92b6:99e2:bf9b	80:19:34:c9:04:00	lan

Display connected device with IPv6 information.

2.2.5 System Log

IWF300
UNSAVED CHANGES: 1

Status ▾
System ▾
Network ▾
Logout

System Log

```

Mon Jan 4 08:59:27 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 08:59:27 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:00:12 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:00:12 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:00:37 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:00:37 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:01:03 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:01:03 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:01:28 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:01:28 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:02:13 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:02:13 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:02:38 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:02:38 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:02:38 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:04 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:04 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:29 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:29 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:49 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:49 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:03:49 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:04:14 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:04:14 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:04:21 2016 daemon.info hostapd: wlan0: STA 00:0d:f0:ac:c8:63 IEEE 802.11: disassociated
Mon Jan 4 09:04:39 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:04:39 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:04 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:04 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:29 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:29 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:50 2016 daemon.info dnsmasq-dhcp[1252]: DHCPINFORM(br-lan) 192.168.1.219 08:3e:8e:67:64:03
Mon Jan 4 09:05:50 2016 daemon.info dnsmasq-dhcp[1252]: DHCPACK(br-lan) 192.168.1.219 08:3e:8e:67:64:03 IM03-AndrewWang1
Mon Jan 4 09:05:55 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:05:55 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:06:15 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:06:15 2016 daemon.warn dnsmasq[1252]: possible DNS-rebind attack detected: ex01.nexcom.com.tw
Mon Jan 4 09:06:25 2016 daemon.info hostapd: wlan0: STA 00:0d:f0:ac:c8:63 IEEE 802.11: authenticated
Mon Jan 4 09:06:25 2016 daemon.info hostapd: wlan0: STA 00:0d:f0:ac:c8:63 IEEE 802.11: associated (aid 3)
Mon Jan 4 09:06:25 2016 daemon.info hostapd: wlan0: STA 00:0d:f0:ac:c8:63 WPA: pairwise key handshake completed (WPA)
Mon Jan 4 09:06:25 2016 daemon.info hostapd: wlan0: STA 00:0d:f0:ac:c8:63 WPA: group key handshake completed (WPA)

```

Displays the record of system activities. The administrator can monitor the system status by checking this log.

2.2.6 Kernel Log

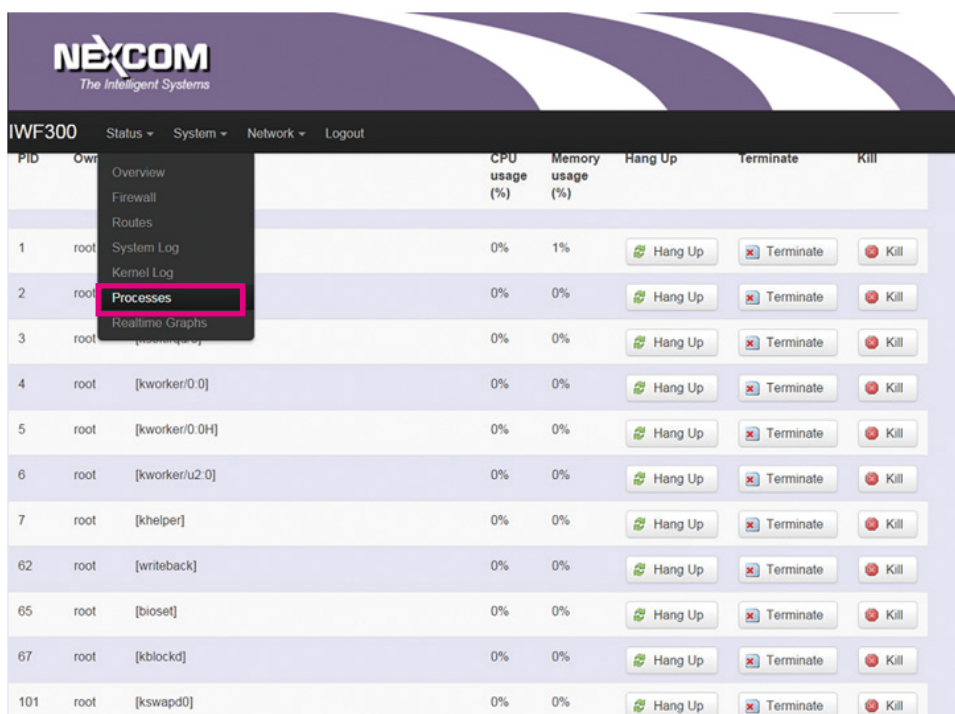
Kernel Log

```
[ 0.000000] Linux version 3.14.27 (kevin@debian603) (gcc version 4.8.3 (OpenWrt/Linaro GCC 4.8-2014.04 r371) ) #1 Wed Aug 5 12:20:03 CST 2015
[ 0.000000] MyLoader: syp=a56da565, boardp=a565a56d, parts=b565a565
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU0 revision is: 0001974c (MIPS 74Kc)
[ 0.000000] SoC: Atheros AR9344 rev 2
[ 0.000000] Determined physical RAM map:
[ 0.000000]   memory: 08000000 @ 00000000 (usable)
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] Zone ranges:
[ 0.000000]   Normal [mem 0x00000000-0x07ffffff]
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000]   node 0: [mem 0x00000000-0x07ffffff]
[ 0.000000] On node 0 totalpages: 32768
[ 0.000000] free_area_init_node: node 0, pgdat 80336420, node_mem_map 81000000
[ 0.000000]   Normal zone: 256 pages used for memmap
[ 0.000000]   Normal zone: 0 pages reserved
[ 0.000000]   Normal zone: 32768 pages, LIFO batch:7
[ 0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
[ 0.000000] Primary data cache 32kB, 4-way, VIPT, cache aliases, linesize 32 bytes
[ 0.000000] pcpu-alloc: s0 r0 d32768 u32768 alloc=1*32768
[ 0.000000] pcpu-alloc: [0] 0
[ 0.000000] Built 1 zonelists in Zone order, mobility grouping on. Total pages: 32512
[ 0.000000] Kernel command line: board=DB120 console=ttyS0,115200 mtdparts=spi0.0:256k(u-boot),64k(u-boot-env),14528k(rootfs),1408k(kernel),64k(nvr
[ 0.000000] PID hash table entries: 512 (order: -1, 2048 bytes)
[ 0.000000] Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
[ 0.000000] Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
[ 0.000000] Writing ErrCtl register=00000000
[ 0.000000] Readback ErrCtl register=00000000
[ 0.000000] Memory: 126116K/131072K available (2370K kernel code, 122K rwdata, 500K rodata, 200K init, 187K bss, 4956K reserved)
[ 0.000000] SLUB: HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[ 0.000000] NR_IRQS:51
[ 0.000000] Clocks: CPU:560.000MHz, DDR:450.000MHz, AHB:225.000MHz, Ref:40.000MHz
[ 0.000000] Calibrating delay loop... 278.93 BogoMIPS (lpj=1394688)
[ 0.070000] pid_max: default: 32768 minimum: 301
[ 0.070000] Mount-cache hash table entries: 1024 (order: 0, 4096 bytes)
[ 0.080000] Mountpoint-cache hash table entries: 1024 (order: 0, 4096 bytes)
[ 0.080000] NET: Registered protocol family 16
[ 0.090000] MIPS: machine is Atheros DB120 reference board
[ 0.100000] registering PCI controller with io_map_base unset
[ 0.110000] -----(ath79_setup_ar934x_eth_cfg) AR934X_GMAC_REG_ETH_CFG=0x28041
[ 0.550000] bio: create slab <bio-0> at 0
```

Displays the record of kernel activities. The administrator can monitor the system status by checking this log.

2.2.7 Processes

This Webpage is designed for detailed troubleshooting/status monitoring by professional personnel in the field. Any improper terminating or killing individual process tasks may cause device malfunction. **The settings are suggested to keep it as factory default.**

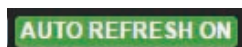


PID	Owner	Process Name	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	[kernel]	0%	1%	Hang Up	Terminate	Kill
2	root	[init]	0%	0%	Hang Up	Terminate	Kill
3	root	[systemd]	0%	0%	Hang Up	Terminate	Kill
4	root	[kworker/0:0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/0:0H]	0%	0%	Hang Up	Terminate	Kill
6	root	[kworker/u2:0]	0%	0%	Hang Up	Terminate	Kill
7	root	[khelper]	0%	0%	Hang Up	Terminate	Kill
62	root	[writeback]	0%	0%	Hang Up	Terminate	Kill
65	root	[bioset]	0%	0%	Hang Up	Terminate	Kill
67	root	[kblockd]	0%	0%	Hang Up	Terminate	Kill
101	root	[kswapd0]	0%	0%	Hang Up	Terminate	Kill

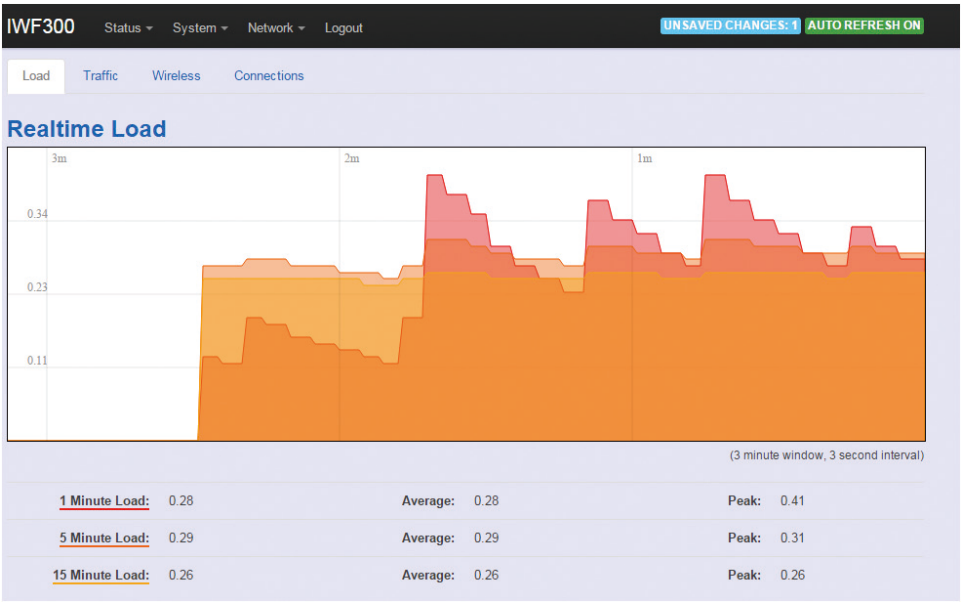
2.2.8 Real-time Graphic

This section provides utilities to monitor IWF 300/IWF 310 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"**.



2.2.8.1 Load

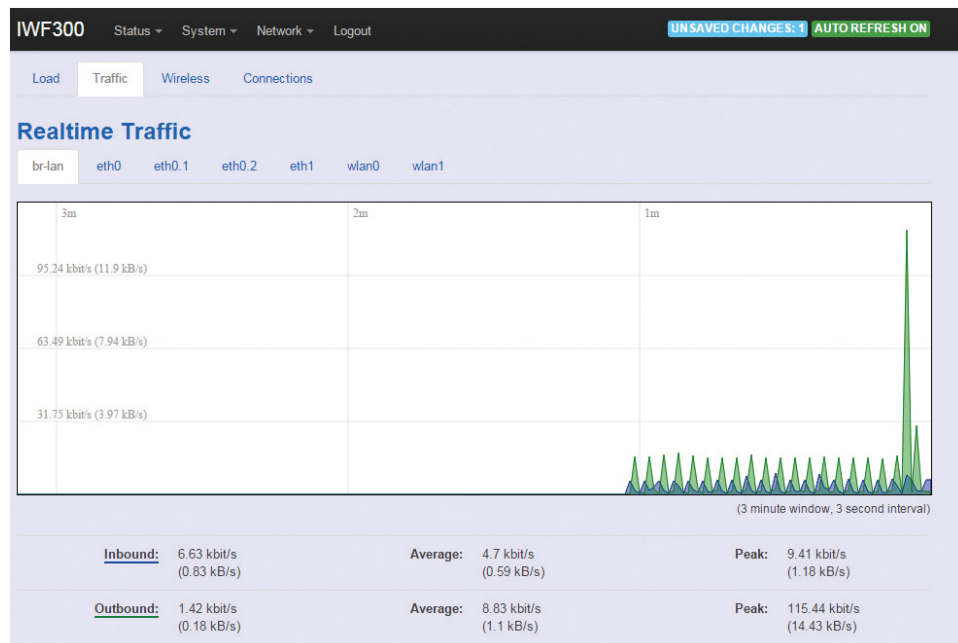


Display real-time CPU average loading percentage.
For example:

1 Minute Load	0.08	Average	0.08	Peak	0.33
5 Minute Load	0.33	Average	0.33	Peak	0.39
15 Minute Load	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%

2.2.8.2 Traffic

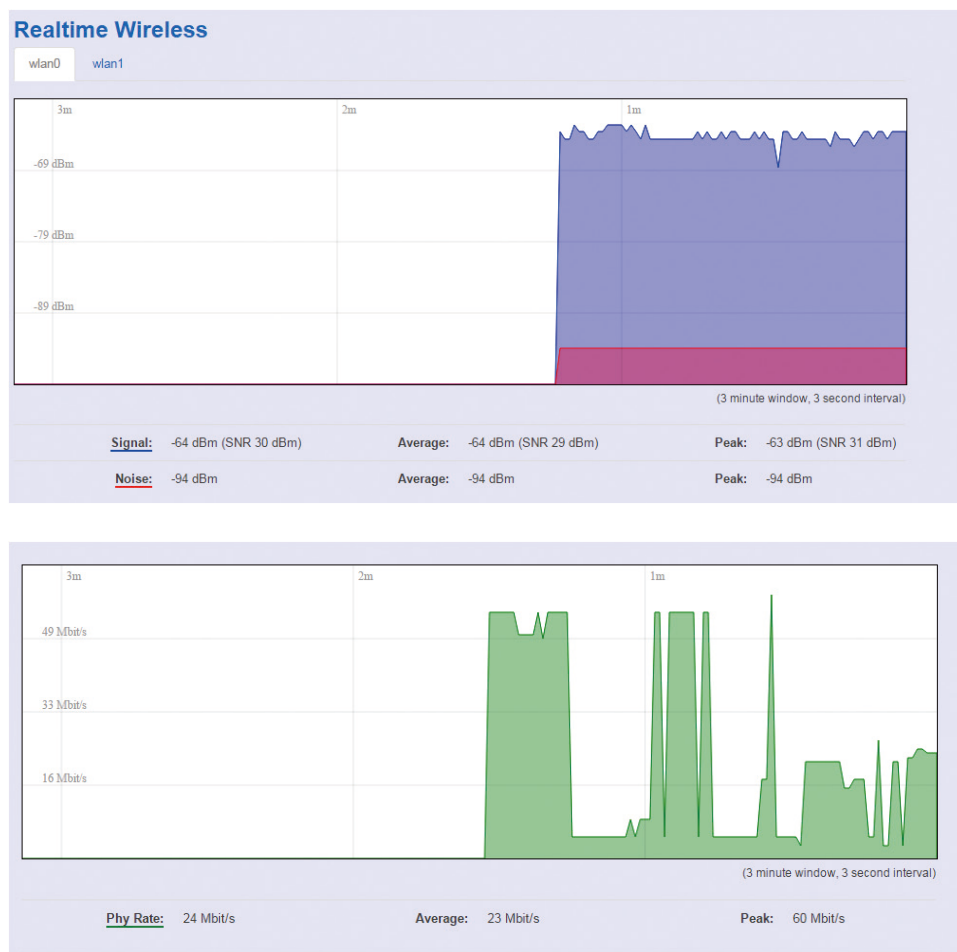


Display IWF 300/IWF 310 Ethernet real-time traffic loading.

Inbound: Incoming data packet size.

Outbound: Outgoing data packet size

2.2.8.3 Wireless

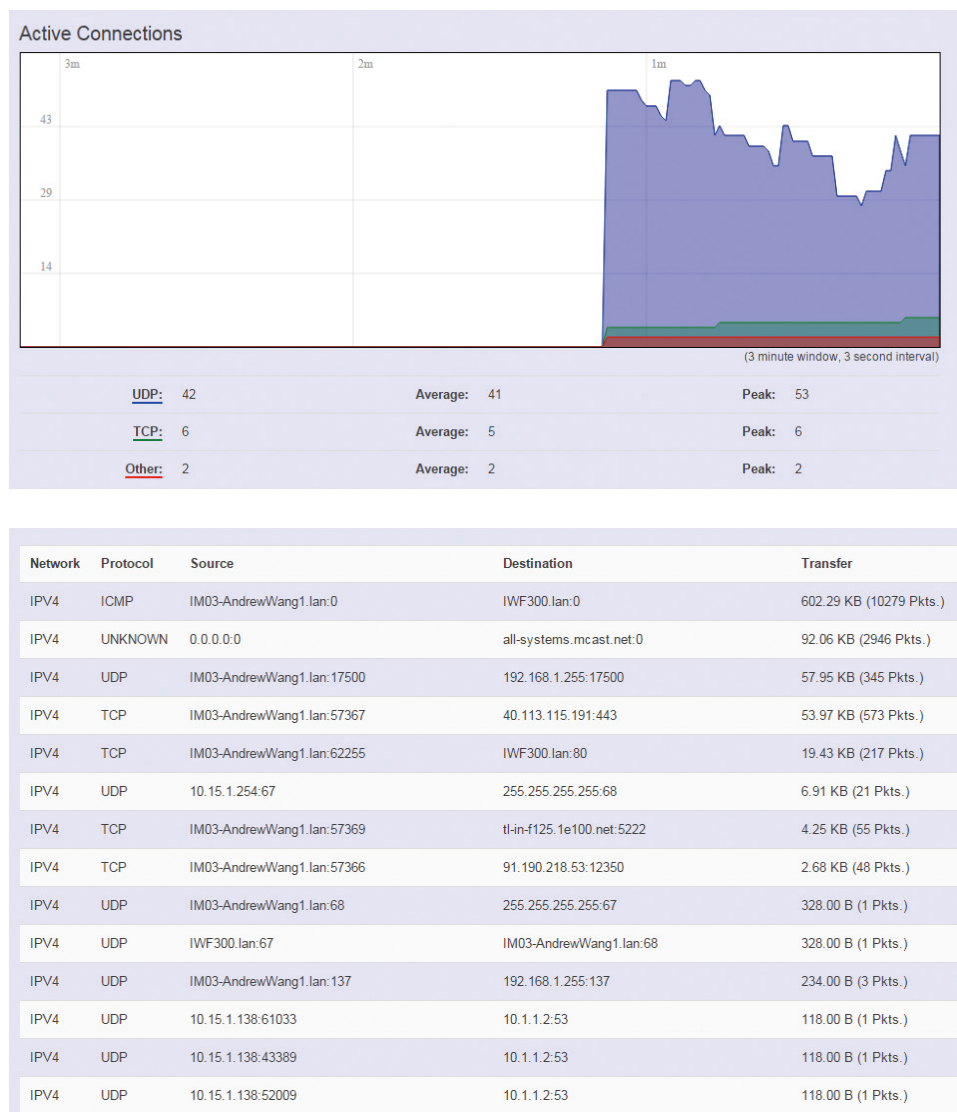


Display Wireless real-time signal quality including signal level, noise and data rate.

wlan0: Radio0 (2.4GHz Access Point) information.

wlan1: Radio1 (5GHz Mesh Access) information.

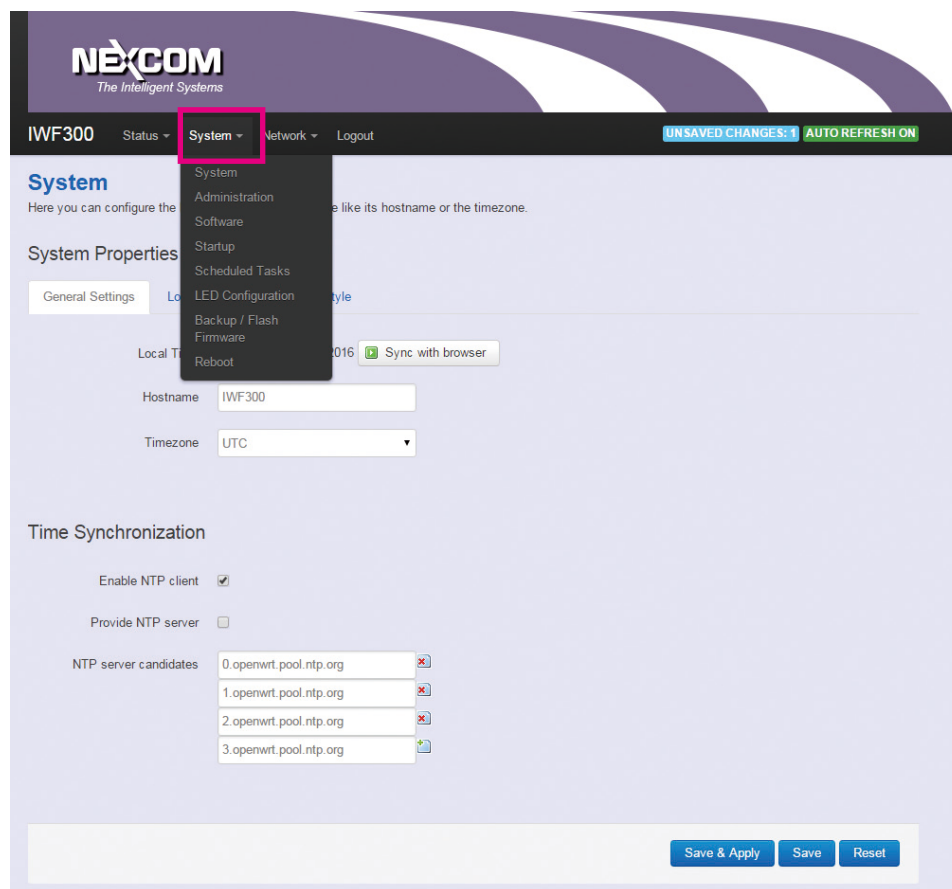
2.2.8.4 Connections



Displays IWF 300/IWF 310 real-time active connection information.

2.3 System

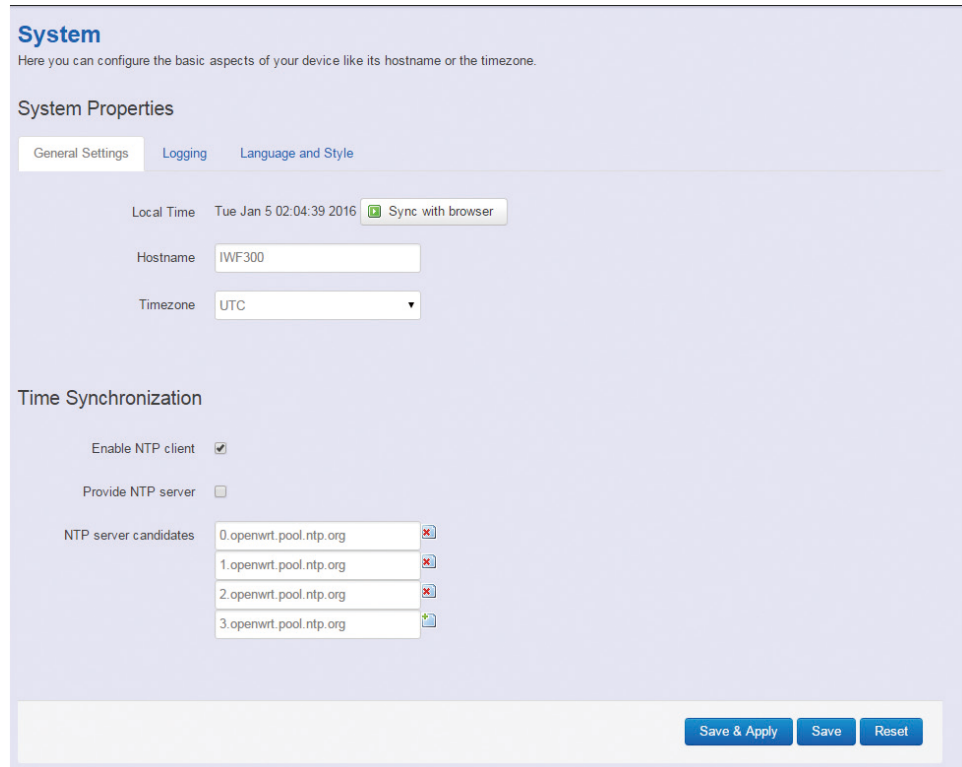
To setup detail configuration about IWF 300/IWF 310 system, click the “System” under the menu bar, then select the item of System, Administration, Software, Start up, Scheduled Tasks, LED configuration, Backup/Flash Firmware and Reboot from the pull-down list like the below screen:



2.3.1 System

2.3.1.1 General Settings

This section provide general settings of IWF 300/IWF 310 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 2016 [Sync with browser](#)

Hostname:

Timezone:

Time Synchronization

Enable NTP client: ☒

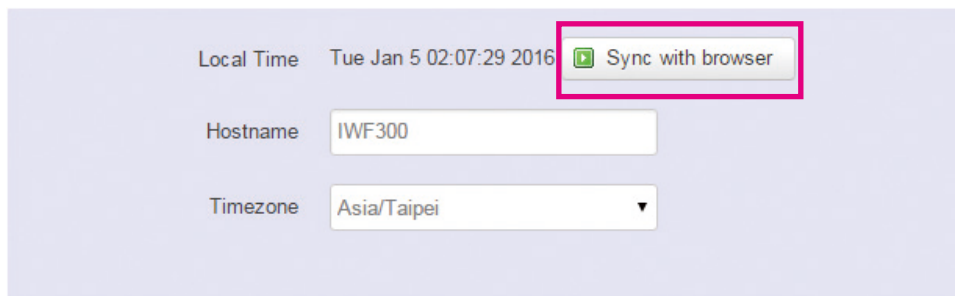
Provide NTP server: ☐

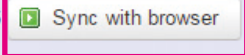
NTP server candidates:

- 0. [✖](#)
- 1. [✖](#)
- 2. [✖](#)
- 3. [✚](#)

[Save & Apply](#) [Save](#) [Reset](#)

Click “Sync with browser” and let IWF 300/IWF 310 sync time with your current computer, then select your country from the Timezone pull-down list.



Local Time Tue Jan 5 02:07:29 2016 

Hostname IWF300

Timezone Asia/Taipei ▼

Enter the address of an SNTP server to receive time updates.




Time Synchronization

Enable NTP client ☒

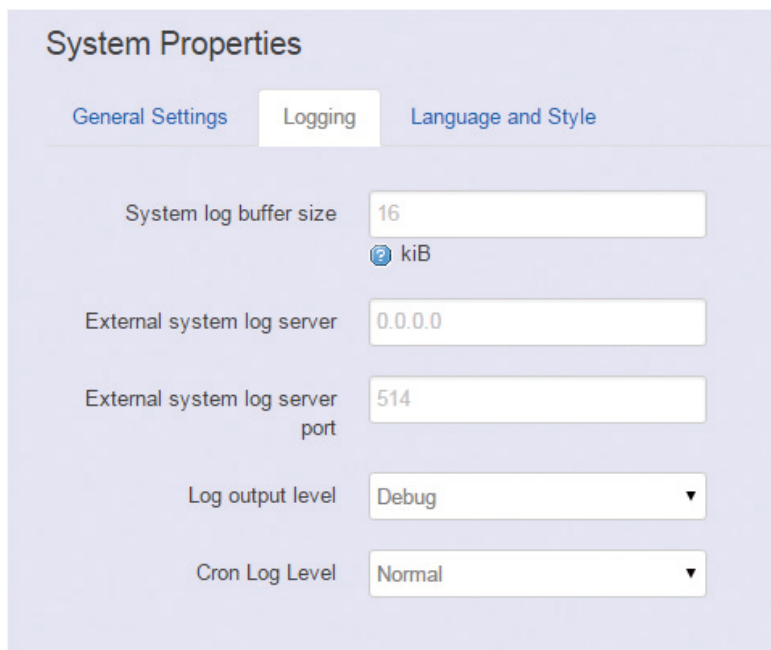
Provide NTP server ☐

NTP server candidates

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

2.3.1.2 Logging

This section provides settings for 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.

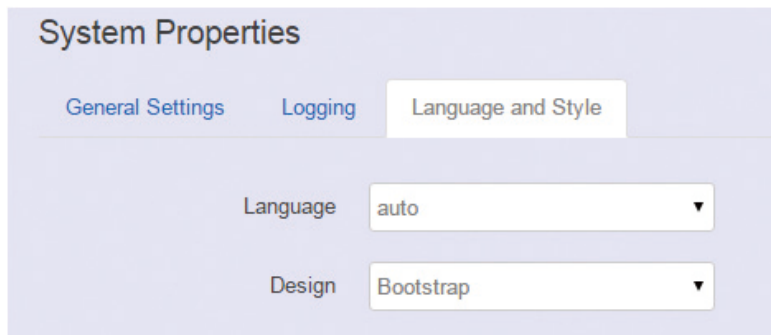
External system log server port: The port number of external log server.

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.

2.3.1.3 Language and Style

This section provides settings for language and WebUI style. IWF 300/IWF 310 only provides English as default and NEXCOM style of WebUI.



System Properties

General Settings | Logging | **Language and Style**

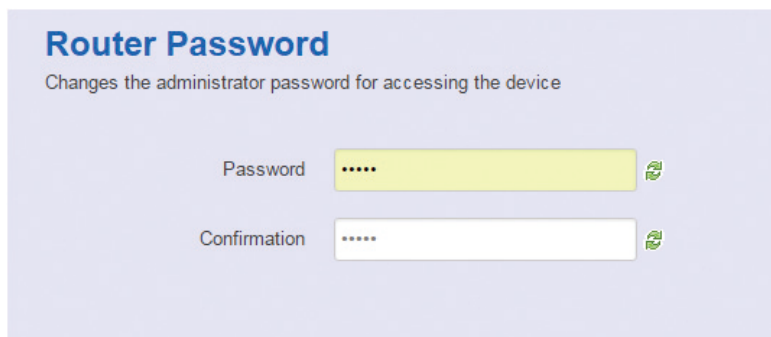
Language: auto ▼

Design: Bootstrap ▼

2.3.2 Administration

2.3.2.1 Router Password

To change the default password, enter the new password and confirm it.



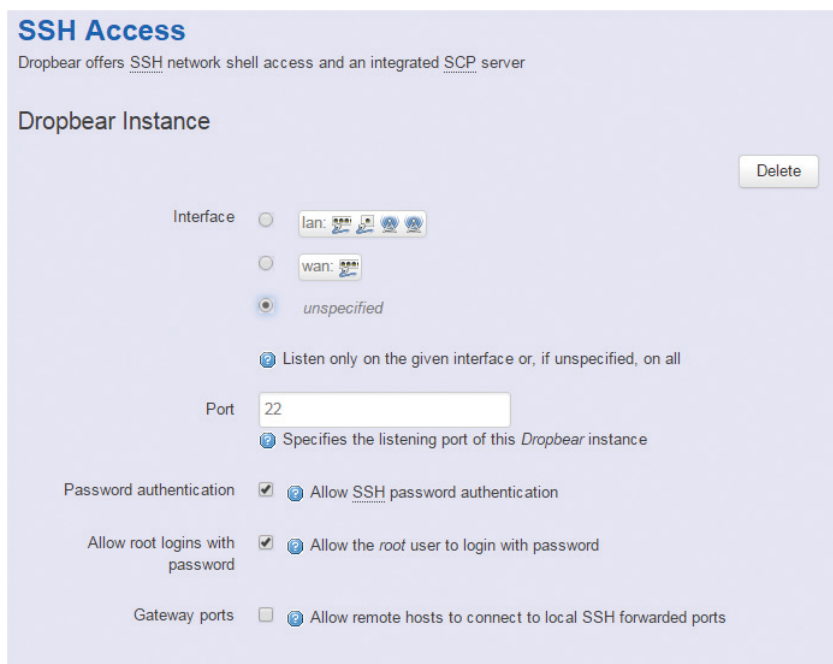
Router Password
Changes the administrator password for accessing the device

Password

Confirmation

2.3.2.2 SSH Access

Secure Shell (SSH). Enable your IWF 300/IWF 310 to be accessed via SSH-based application.



SSH Access
Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance Delete

Interface ☐ lan: ☐ wan: ☒ 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

Gateway ports ☐ ☐ Allow remote hosts to connect to local SSH forwarded ports

Interface: Select the interface.

Port: Enter the port number.

Password authentication: Enable/Disable SSH password authentication.

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

Gateway ports: Enable/Disable remote hosts to connect to local SSH forwarded ports.

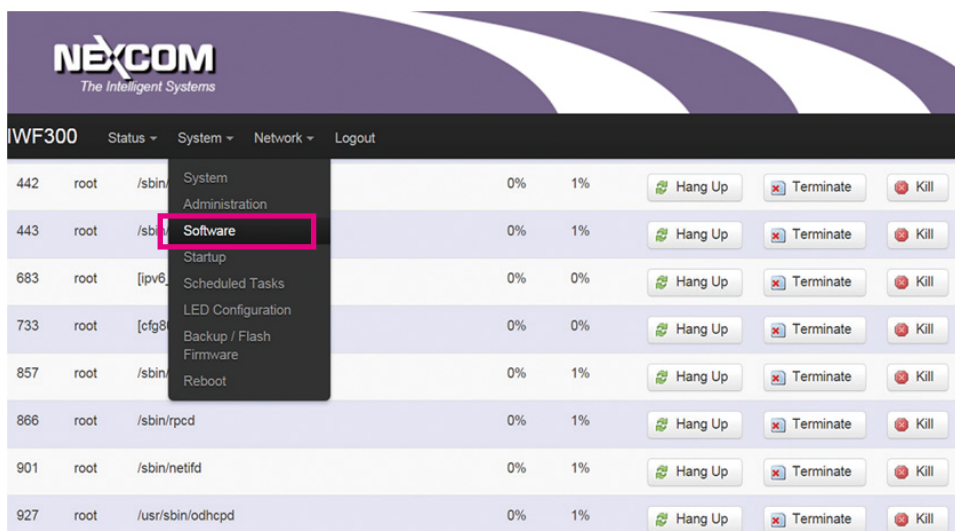
To paste public SSH-Keys (one per line) for SSH public-key authentication.

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

2.3.3 Software

This Webpage is designed for detailed troubleshooting/ status monitoring by professional personnel in the field. Any improper terminating or killing individual process tasks may cause device malfunction. **The settings are suggested to keep it as factory default. Notice that none of the software item can be killed; otherwise, the software may not be recovered.**

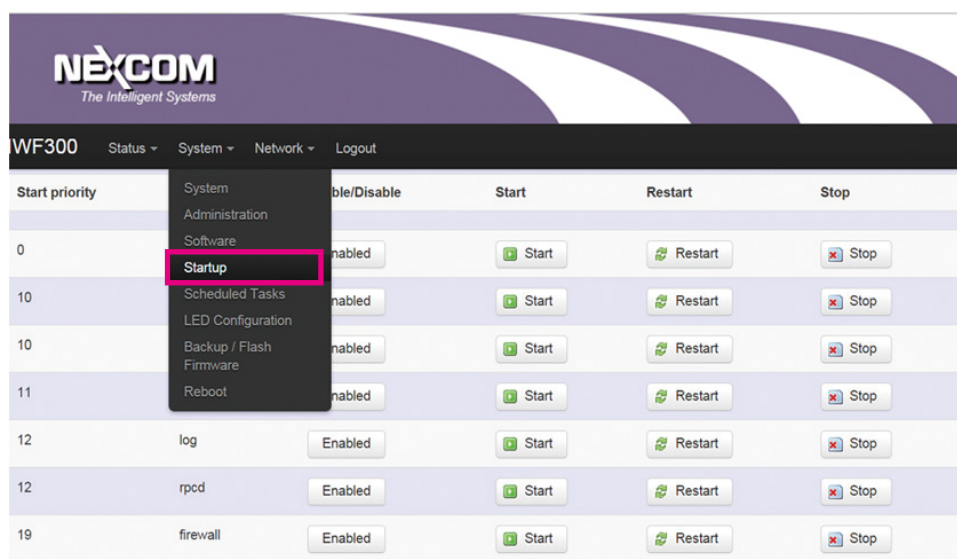


The screenshot shows the NEXCOM IWF300 web interface. The top navigation bar includes 'Status', 'System', 'Network', and 'Logout'. A dropdown menu is open under the 'System' tab, with 'Software' highlighted. The main content area displays a table of system processes with columns for PID, User, Path, CPU, and Memory usage, along with 'Hang Up', 'Terminate', and 'Kill' buttons for each process.

PID	User	Path	CPU	Memory	Hang Up	Terminate	Kill
442	root	/sbin/System Administration	0%	1%	Hang Up	Terminate	Kill
443	root	/sbin/Software	0%	1%	Hang Up	Terminate	Kill
683	root	[ipv6] Startup	0%	0%	Hang Up	Terminate	Kill
733	root	[cfg8] LED Configuration	0%	0%	Hang Up	Terminate	Kill
857	root	/sbin/Backup / Flash Firmware	0%	1%	Hang Up	Terminate	Kill
866	root	/sbin/Reboot	0%	1%	Hang Up	Terminate	Kill
901	root	/sbin/rpcd	0%	1%	Hang Up	Terminate	Kill
927	root	/sbin/netifd	0%	1%	Hang Up	Terminate	Kill
927	root	/usr/sbin/odhcpd	0%	1%	Hang Up	Terminate	Kill

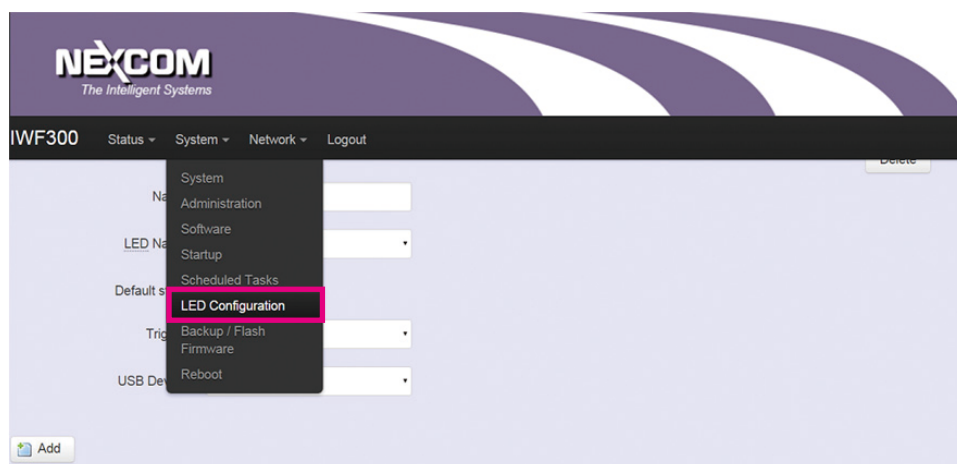
2.3.4 Startup

This Webpage is designed for manual configuration (Enable/Disable, Start, Reset and Stop) of individual init script. It provides comprehensive settings for troubleshooting/status monitoring by professional personnel in the field. **Any improper setting may cause device malfunction.**



2.3.5 LED Configuration

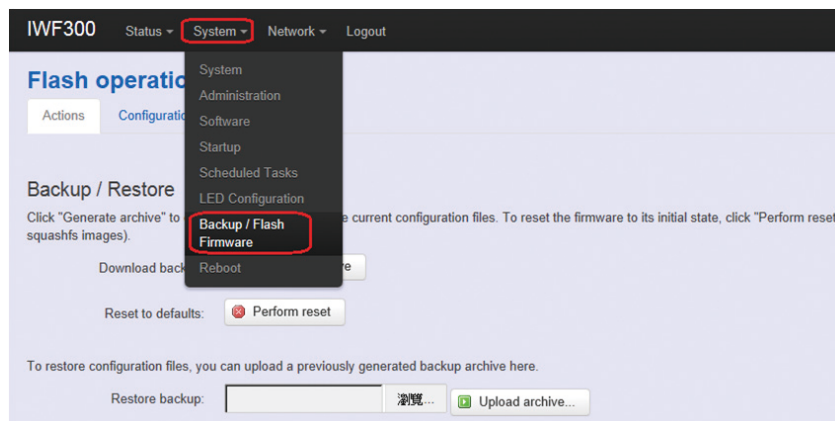
This Webpage is designed for manual configuration of LED definition (including PHY, Wi-Fi, Status and WPS). It provides comprehensive settings for troubleshooting/status monitoring by professional personnel in the field. **It is suggested to leave the settings as factory default.**



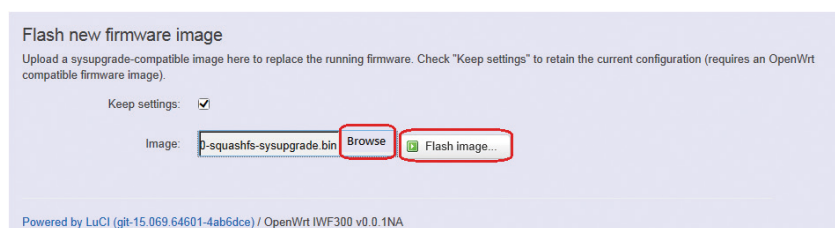
2.3.6 Backup/Flash Firmware

2.3.6.1 Upgrade Firmware

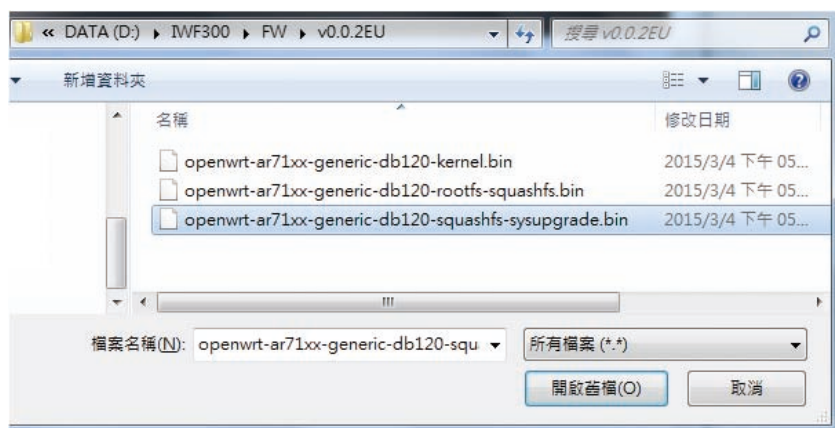
To upgrade a new firmware onto the device, please choose “System” from the menu bar, then select “Backup/Flash Firmware” like the below screen:



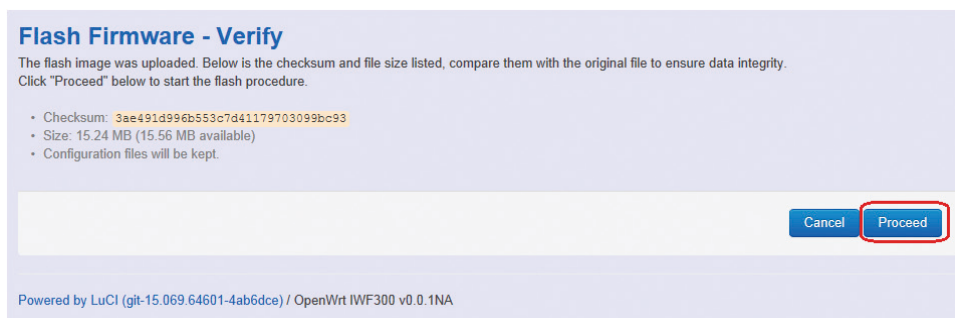
Please click “Browse” under the “Flash new firmware image” section:



Then select the correct firmware file in the file browser like:

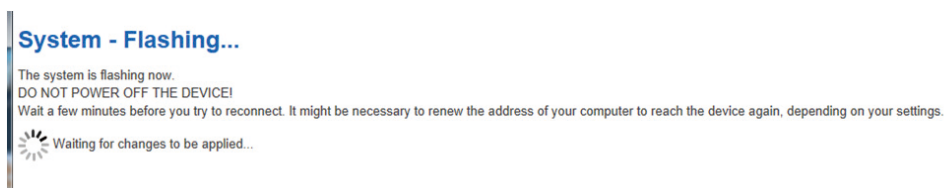


Then GUI will display the file checksum.



You can choose "Proceed" to start the upgrade process.

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



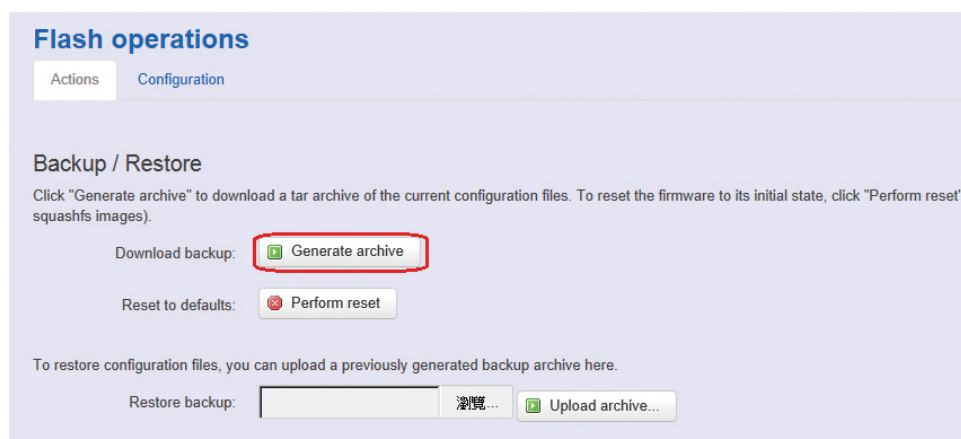
Note: The whole programming might take several minutes to complete the flash writing. **PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole progress.

If the firmware upgrad is successful, the GUI should switch to the Login page.

You can also check the version via the "Firmware Version" field under the Status page.

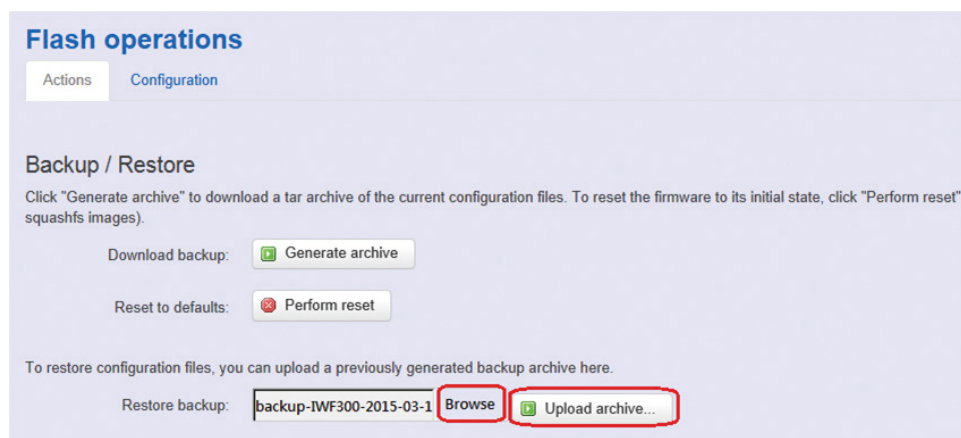
2.3.6.2 Backup Configuration

To backup you current configuration, please choose "System" from the menu bar, then select "Backup/Flash Firmware" and click the "Generate archive" button under the Backup / Restore section, like:



Then save it as a file in your PC.

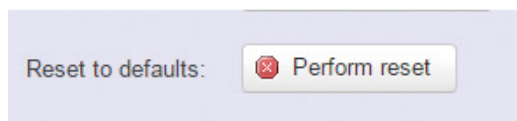
To restore the device to your previous configuration, please choose "System" from the menu bar, then select "Backup/Flash Firmware" and click "Browse" under the section to select your previous configuration file, then click the button "Upload archive...", like:



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

2.3.6.3 Reset to default

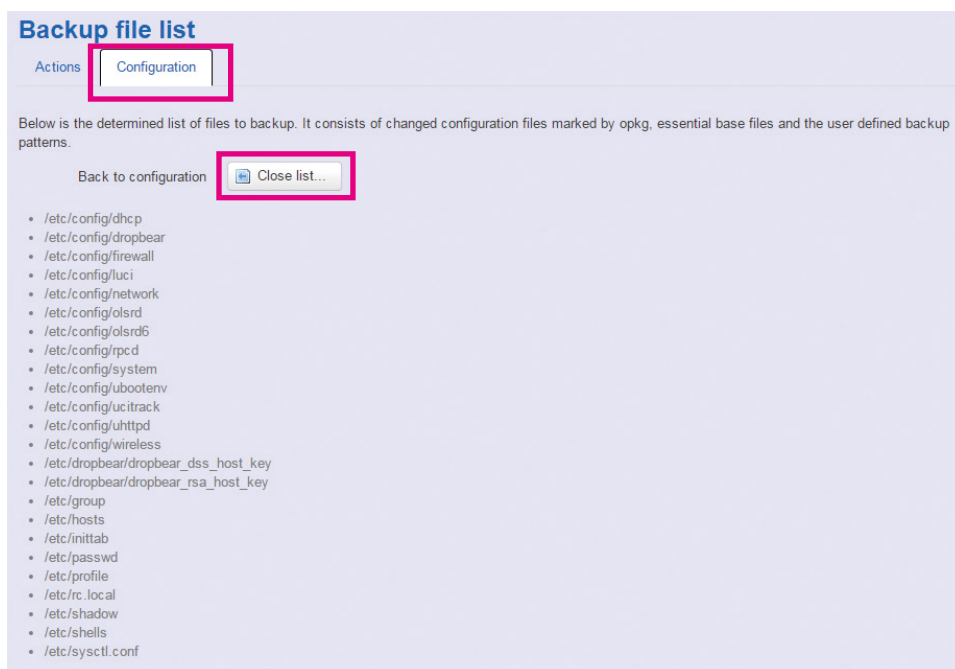
To reset your IWF 300/IWF 310 to default settings, please click "Perform reset".



Note: The whole programming might take several minutes to complete the process. **PLEASE DO NOT REBOOT OR POWER OFF THE DEVICE** before the whole progress.

2.3.6.4 Configuration

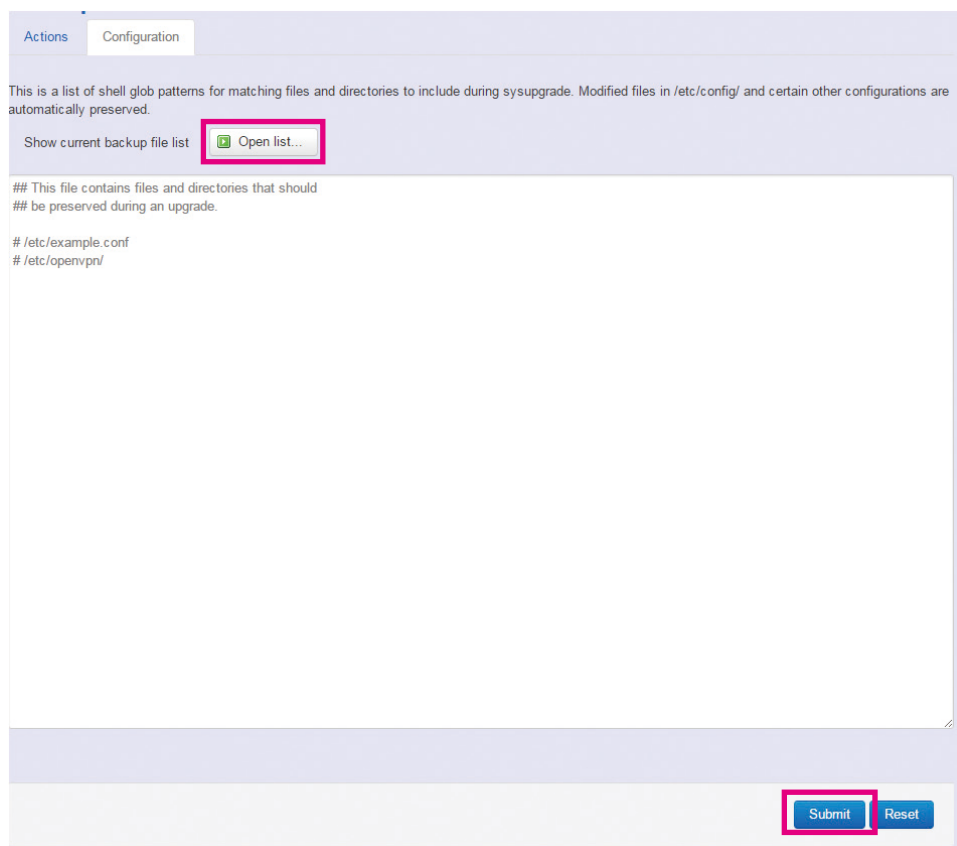
Click Configuration to see the configuration list. The files in "Close list" are the determined list of files to backup. It consists of changed configuration files marked by opkg, essential base files and the user defined backup patterns.



In “Open list”, a list of shell glob patterns for matching files and directories to include during system upgrade are shown.

Modified files in /etc/config/ and other certain configurations are automatically preserved.

Click the “Submit” button after finishing editing.



Actions Configuration

This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.

Show current backup file list

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
```

2.3.7 Reboot

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



NEXCOM IWF300 Status System Network Logout

Reboot

Reboots the operating system of your device

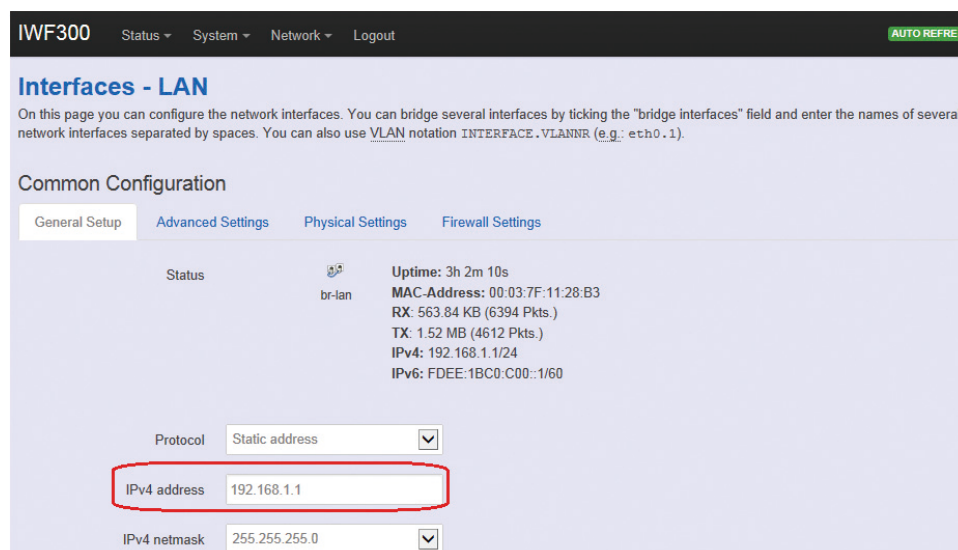
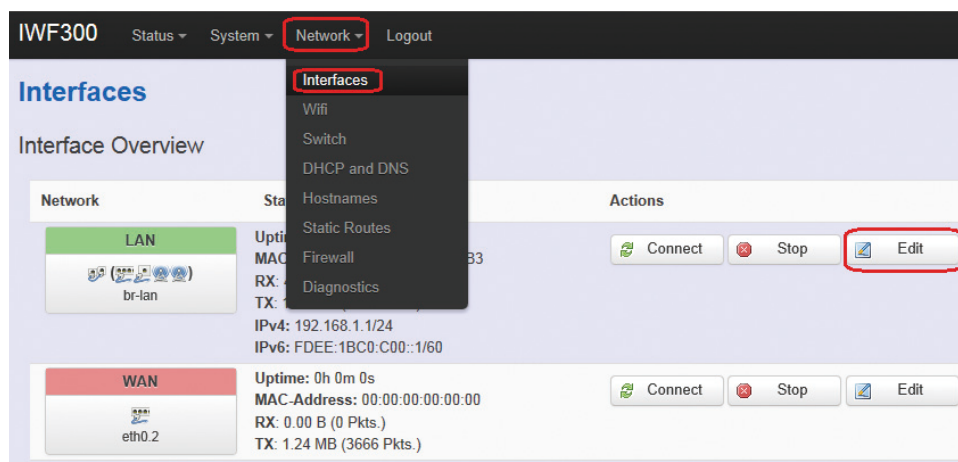
Powered by LuCI (git-15.319.74171-1106b93) / IWF300 (US) v0.1.1

2.4 Network

2.4.1 Interfaces

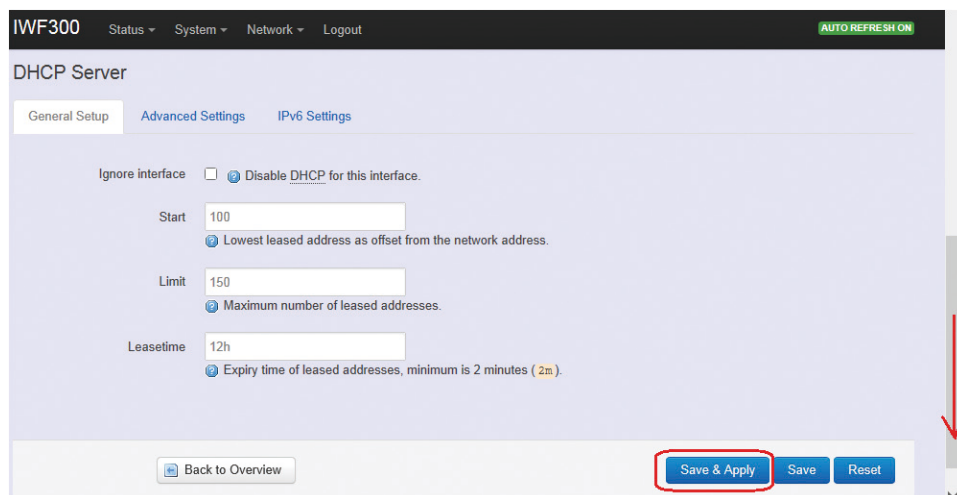
2.4.1.1 Change Default IP Address

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



Under the “IPv4 address” field, you can input the new IP address of this device, and then pull down the scroll bar to the bottom of the WebUI page and click “Save & Apply” to save this new IP address into flash and apply it immediately.

Note: After applying 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 the browser again if the GUI does not switch to new GUI page after 5 minutes.



IWF300 Status System Network Logout AUTO REFRESH ON

DHCP Server

General Setup **Advanced Settings** IPv6 Settings

Ignore interface ☐ [Disable DHCP for this interface.](#)

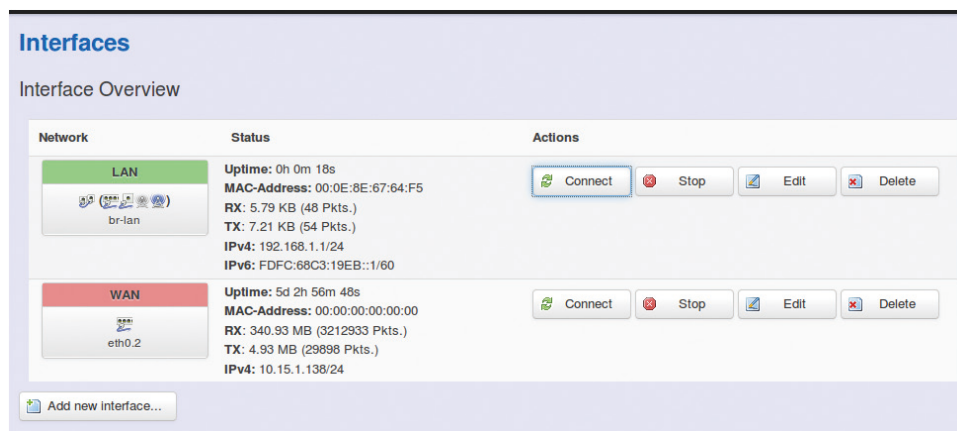
Start
[Lowest leased address as offset from the network address.](#)

Limit
[Maximum number of leased addresses.](#)

Leasetime
[Expiry time of leased addresses, minimum is 2 minutes \(2m\).](#)



[Back to Overview](#) **Save & Apply** Save Reset

2.4.1.2 Interfaces Overview



Interfaces

Interface Overview

Network	Status	Actions
LAN  br-lan	Uptime: 0h 0m 18s MAC-Address: 00:0E:8E:67:64:F5 RX: 5.79 KB (48 Pkts.) TX: 7.21 KB (54 Pkts.) IPv4: 192.168.1.1/24 IPv6: FDFC:68C3:19EB::1/60	Connect Stop Edit Delete
WAN  eth0.2	Uptime: 5d 2h 56m 48s MAC-Address: 00:00:00:00:00:00 RX: 340.93 MB (3212933 Pkts.) TX: 4.93 MB (29898 Pkts.) IPv4: 10.15.1.138/24	Connect Stop Edit Delete

[Add new interface...](#)

Connect: Link up this interface to the network, functions like "Save & Apply".

Stop: Disable the interface to link to the network.

Edit: Modify WAN port settings or LAN port group settings.

Delete: Delete this interface group.

2.4.1.3 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.

Interfaces - WAN

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.VLANNR (e.g.: eth0.1).

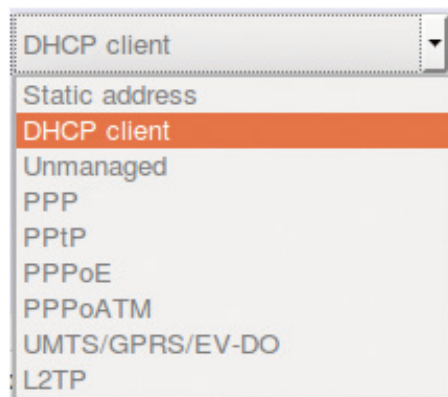
Common Configuration

General Setup
Advanced Settings
Physical Settings
Firewall Settings

Status	 eth0.2	Uptime: 5d 3h 8m 21s MAC-Address: 00:00:00:00:00:00 RX: 341.67 MB (3219751 Pkts.) TX: 4.93 MB (29901 Pkts.) IPv4: 10.15.1.138/24
Protocol	<input type="text" value="DHCP client"/>	
Hostname to send when requesting DHCP	<input type="text" value="IWF300"/>	

<General Setup>

You can change the protocol used to link the 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 IWF 300/IWF 310.

DHCP client

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

Unmanaged

This interface has no configuration interface or options.

PPP

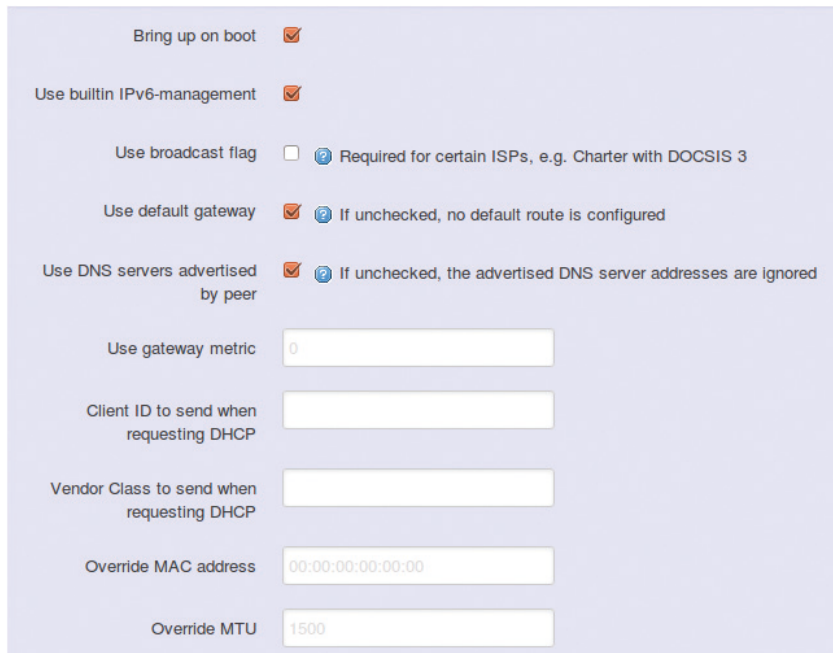
Used to provide point to point link for connecting IWF 300/IWF 310 to old serial modem.

PPPoE

Used for cable modem or ADSL users to link IWF 300/IWF 310 to your internet provider.

<Advanced Settings>

Advanced settings and configuration, it is advised that generic users leave the settings unchanged.



Bring up on boot ☒

Use builtin IPv6-management ☒

Use broadcast flag ☐ ? Required for certain ISPs, e.g. Charter with DOCSIS 3

Use default gateway ☒ ? If unchecked, no default route is configured

Use DNS servers advertised by peer ☒ ? If unchecked, the advertised DNS server addresses are ignored

Use gateway metric

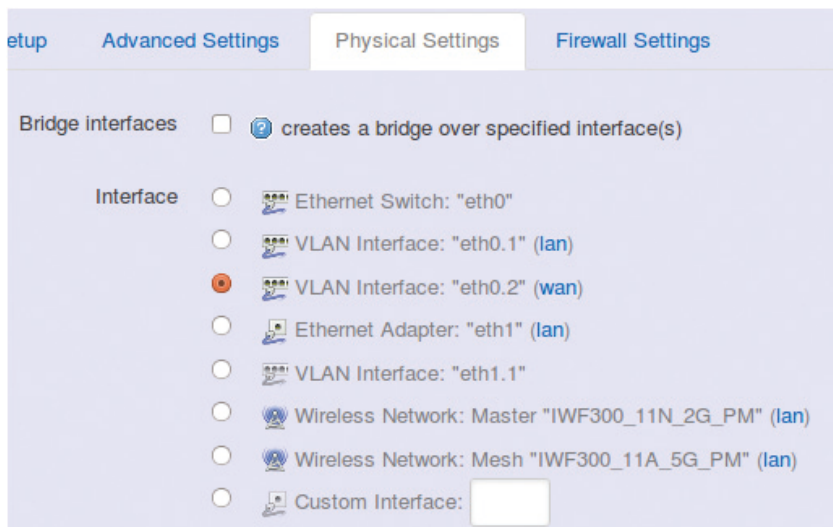
Client ID to send when requesting DHCP

Vendor Class to send when requesting DHCP

Override MAC address

Override MTU

<Physical Settings>

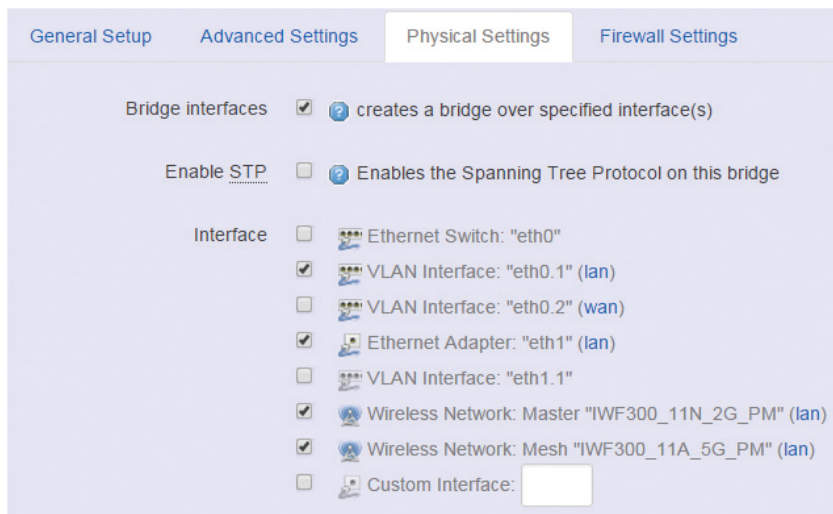


Setup Advanced Settings Physical Settings Firewall Settings

Bridge interfaces ☐ ? creates a bridge over specified interface(s)

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:



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

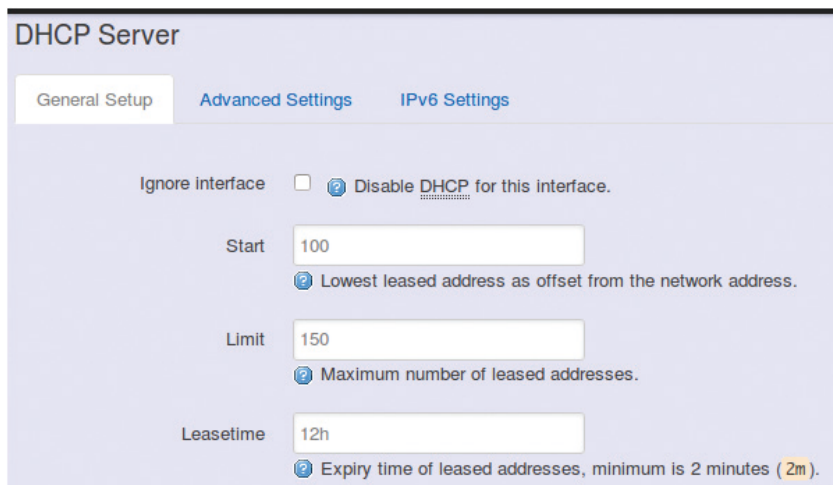
You can bridge an interface group for your WAN or LAN interface. Normally, only LAN interface needs to enable bridge interfaces. After enabling bridge interfaces, select the interfaces to bridge.

Interface

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

2.4.1.4 DHCP Server

<General Setup>



DHCP Server

General Setup Advanced Settings IPv6 Settings

Ignore interface ☐ ? Disable DHCP for this interface.

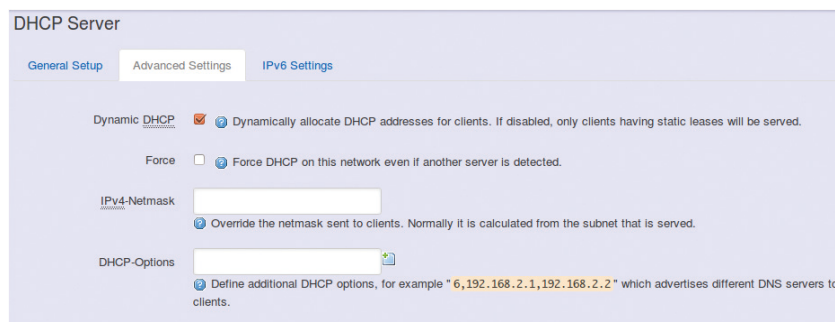
Start ? Lowest leased address as offset from the network address.

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 a static IP or another DHCP server for your network interfaces. Default is "enable DHCP".

<Advanced Settings>

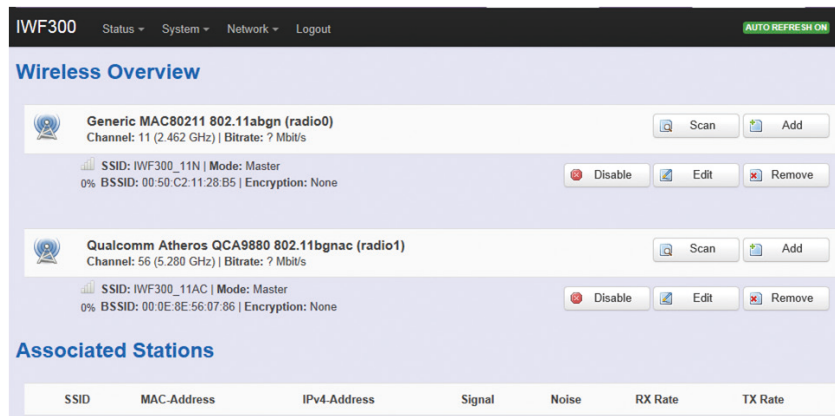


Dynamic DHCP: Dynamically allocate DHCP addresses for clients. If disabled, only clients with static leases will be served.

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

2.4.2 WiFi

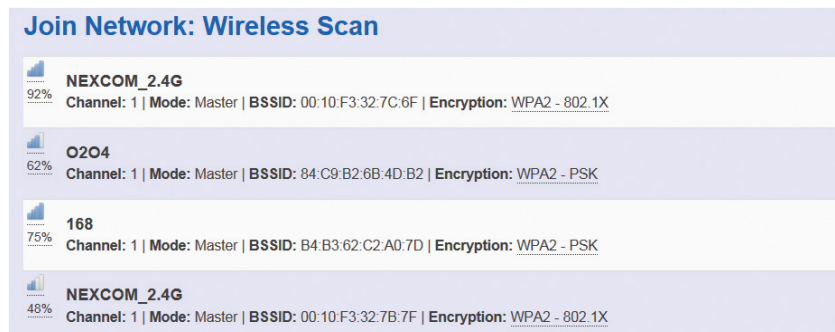
2.4.2.1 Wireless Overview



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

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

Scan: Scan any AP nearby the Radio, we can check how many APs are nearby this AP and avoid using the same channel.



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



Disable: Disable the radio interface.

Edit: Configure the radio interface.

Remove: Remove radio interface. Please note that the radio must be disabled first when you don't want to use the radio interface.

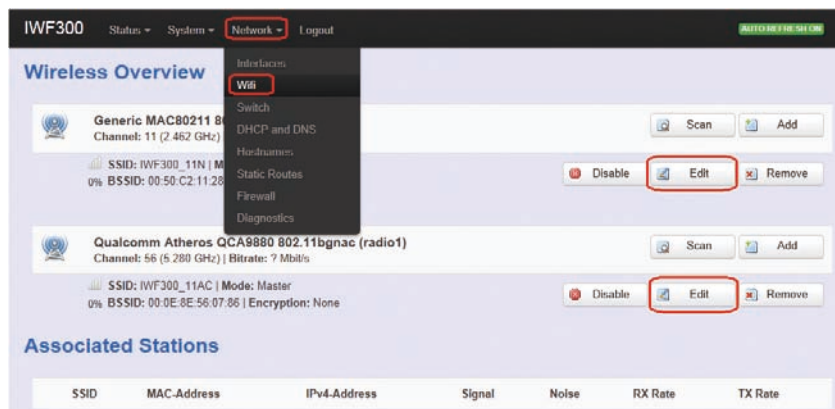
2.4.2.2 Associated Stations

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

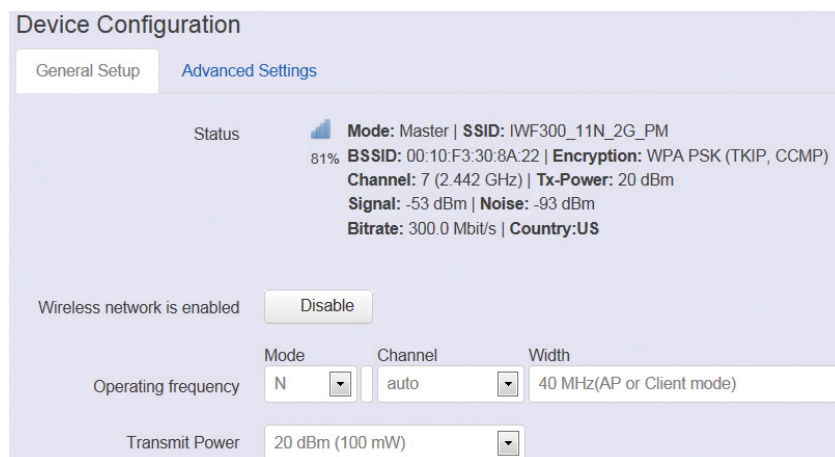
Associated Stations						
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
IWF300_11N_2G_PM	9C:2A:70:1B:4C:9D	192.168.1.215	-53 dBm	-93 dBm	162.0 Mbit/s, MCS 12, 40MHz	104.0 Mbit/s, MCS 13, 20MHz

2.4.2.3 Wireless configuration

Please select “network” -> “Wifi” and click Edit to configure Radio0 (802.11n) or Radio1 (802.11AC).



The **Device Configuration** section covers physical settings of the radio hardware such as channel, transmit power and so forth.

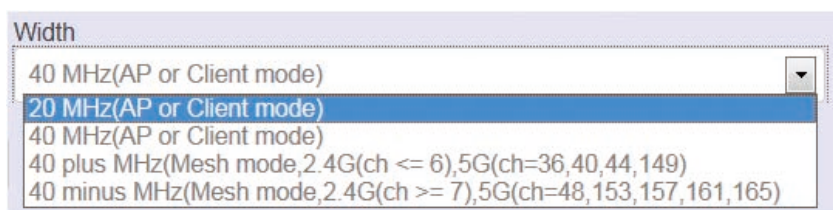


<General Setup>

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 the channel you will use.

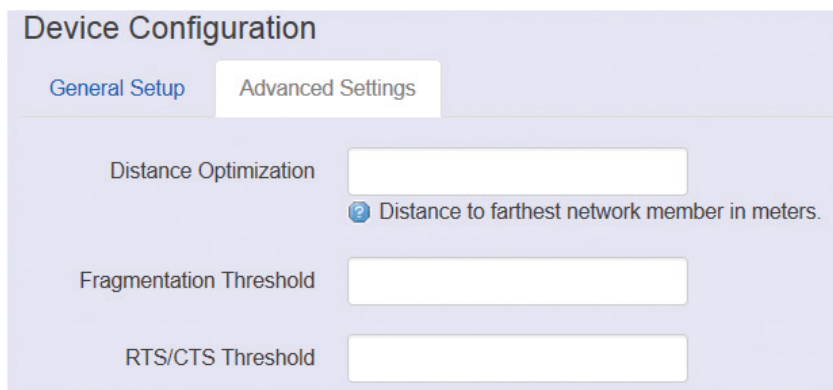


Width

- 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: Select the transmit power of a radio.

<Advanced Settings>



Device Configuration

General Setup Advanced Settings

Distance Optimization  Distance to farthest network member in meters.

Fragmentation Threshold

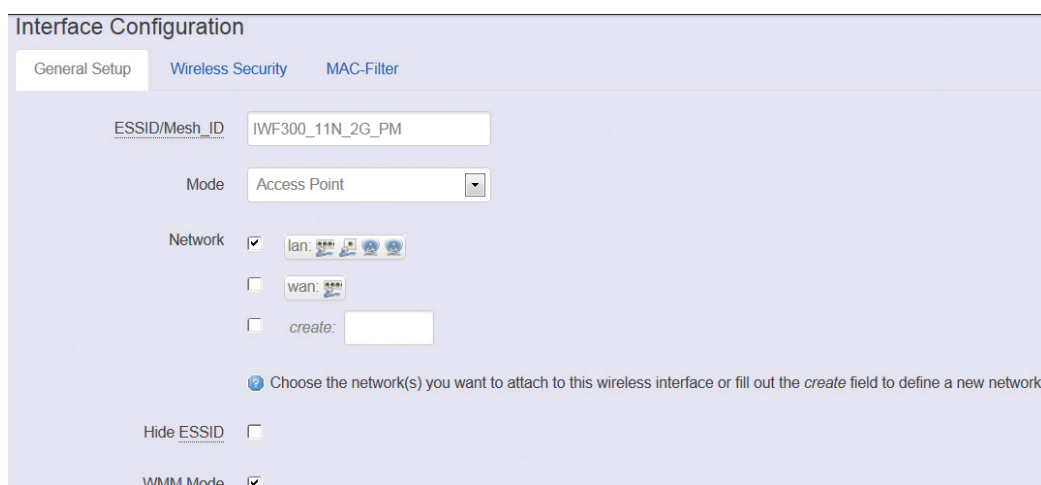
RTS/CTS Threshold

Distance Optimization: Specify the ACK timeout by entering the value manually. ACK timeout can be entered by defining the link distance. A value too short for the ACK timeout may cause transmission time out and no packets can be received. A value too long 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.

The **Interface Configuration** section covers SSID operation mode and encryption.



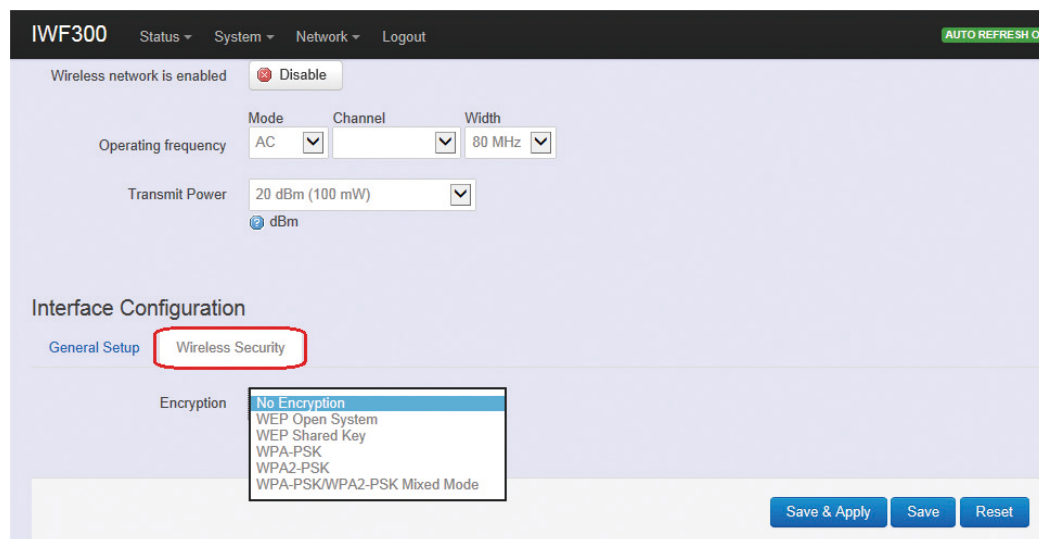
<General Setup>

ESSID: Edit the SSID. The default SSID for radio0 is IWF 300/ IWF 310_11N and default SSID for radio1 is IWF 300/IWF 310_11A_5G

Mode: Select the operation mode:

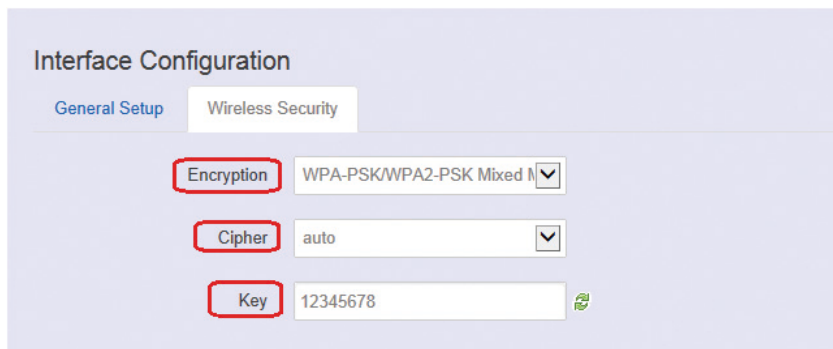
- AP
- Client Router
- 802.11s (Mesh mode)

<Wireless Security>



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

- 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.



Interface Configuration

General Setup Wireless Security

Encryption WPA-PSK/WPA2-PSK Mixed N

Cipher auto

Key 12345678

Cipher: It is recommended to select TKIP and CCMP (AES).

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



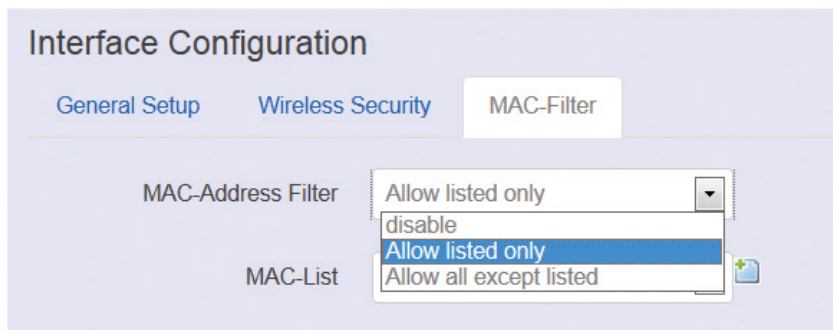
Encryption WPA-PSK/WPA2-PSK Mixed N

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

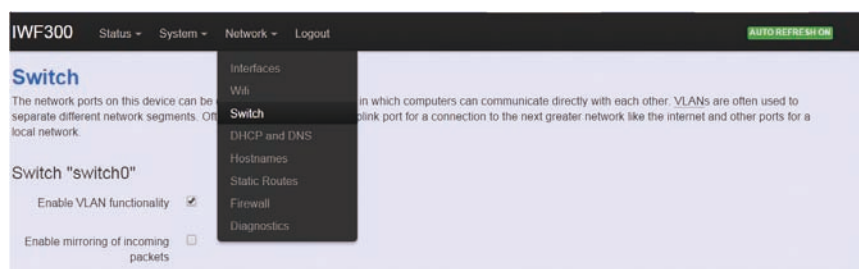
Allow all except listed

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

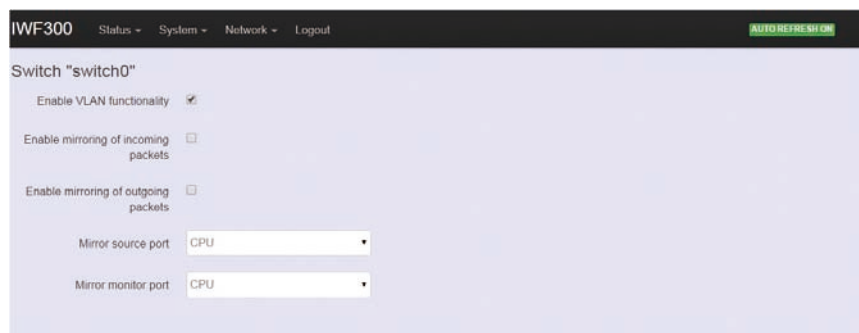
2.4.3 Switch

The network ports on this device can be combined to several VLANs in which computers can communicate directly with each other. VLANs are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network.

Click "Network" -> "Switch" in the GUI menu to configure VLANs.

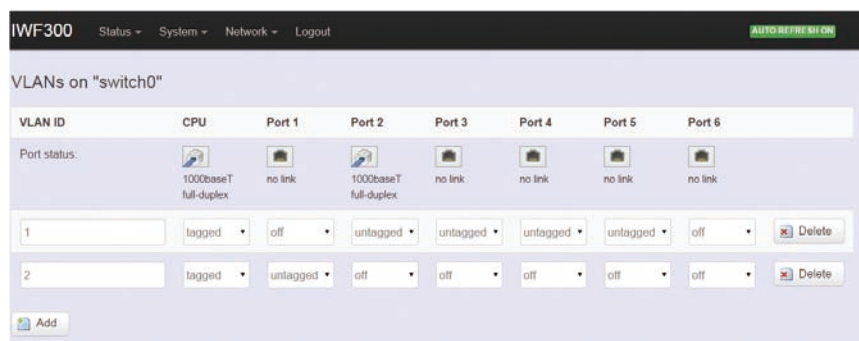


Scrolling down to this screen which enables/disables VLAN capability and configures mirror options in the "switch 0".



By default, VLAN functionality is enabled and other mirror options are disabled.

Keep scrolling to this screen for adding or editing VLANs in switch "switch 0".



VLAN ID	CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port status:	1000baseT full-duplex	no link	1000baseT full-duplex	no link	no link	no link	no link
1	tagged	off	untagged	untagged	untagged	untagged	off
2	tagged	untagged	off	off	off	off	off

Add

"Port 1" indicates the IWF 300/IWF 310's WAN port.

"Port 2 ~ Port 5" indicate the IWF 300/IWF 310's LAN ports (1 ~ 4).

"CPU" indicates the trunk port with tagged attribute of VLAN 1 and VLAN 2.

Port 6 is not used in the IWF 300/IWF 310.

Port status: This area displays the link status, speed, and duplex by auto negotiation for each port.

Delete: This button icon deletes the followed VLAN entry.

Add: This button icon adds a new VLAN entry with each "switch0" port (CPU port and Port 1 ~ 5) off.



VLAN ID	CPU	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6
Port status:	1000baseT full-duplex	no link	1000baseT full-duplex	no link	no link	no link	no link
1	tagged	off	untagged	untagged	untagged	untagged	off
2	tagged	untagged	off	off	off	off	off
3	off	off	off	off	off	off	off

Add

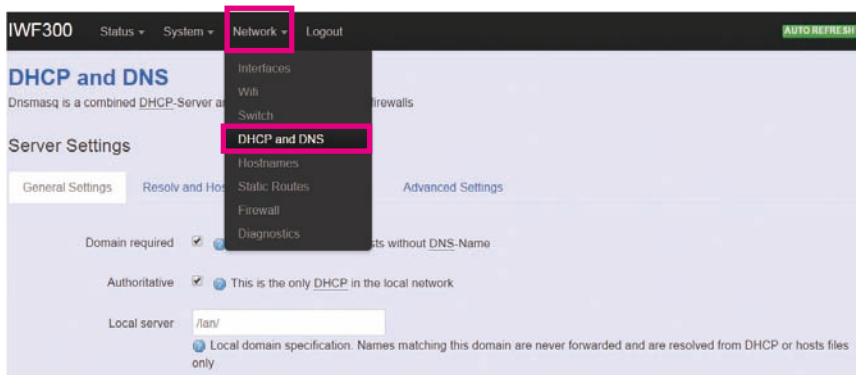


These “switch1” options are used for built-in switch embedded in the product’s SoC. This switch is not used for the product’s design and makes no effects on any functions.

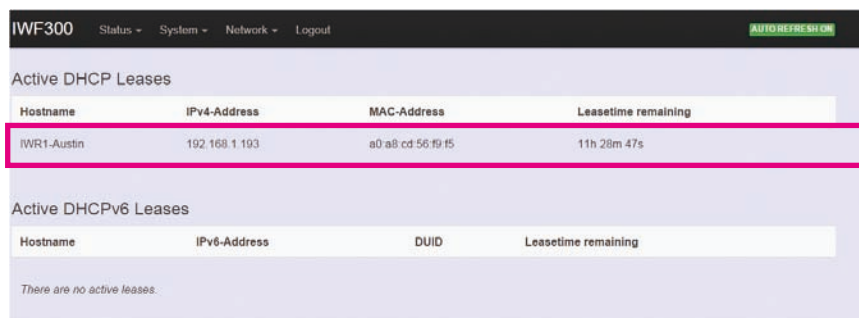
2.4.4 DHCP and DNS

A combined DHCP-Server and DNS-Forwarder for NAT firewall is provided in IWF 300/IWF 310.

Click “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.



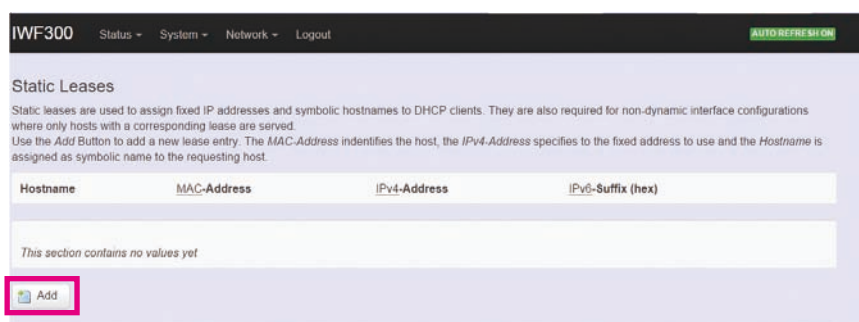
Active DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
IWR1-Austin	192.168.1.193	a0:a8:cd:56:f9:f5	11h 28m 47s

Active DHCPv6 Leases			
Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			


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.



Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
This section contains no values yet			

 Add

Add: Add a new lease entry.

After clicking the “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).

Static Leases

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 the fixed address to use and the Hostname is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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 IWF 300/IWF 310.

2.4.4.1 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

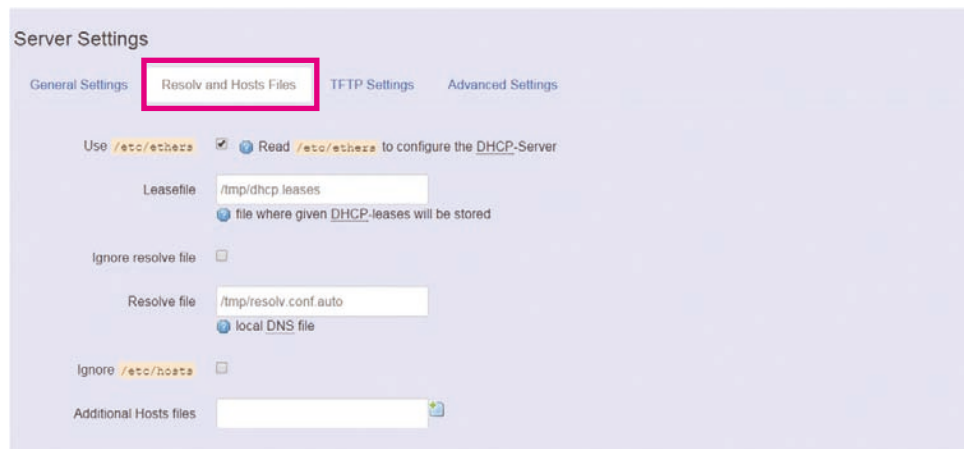
Allow localhost ☒ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist
 List of domains to allow RFC1918 responses for

Domain required: Default value is checked.

Authoritative: Default value is checked.

2.4.4.2 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

Leasefile
file where given DHCP leases will be stored

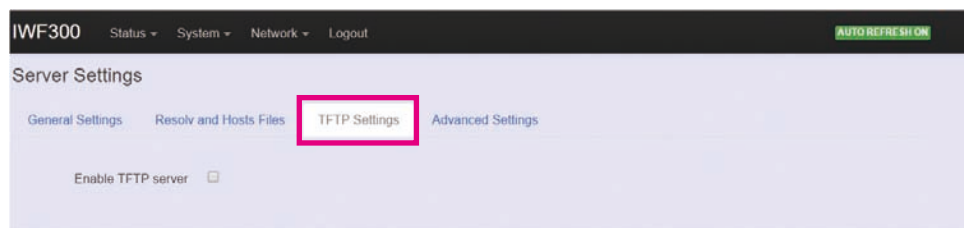
Ignore resolve file ☐

Resolve file
local DNS file

Ignore `/etc/hosts` ☐

Additional Hosts files

2.4.4.3 TFTP Settings



IWF300 Status System Network Logout AUTO REFRESH ON

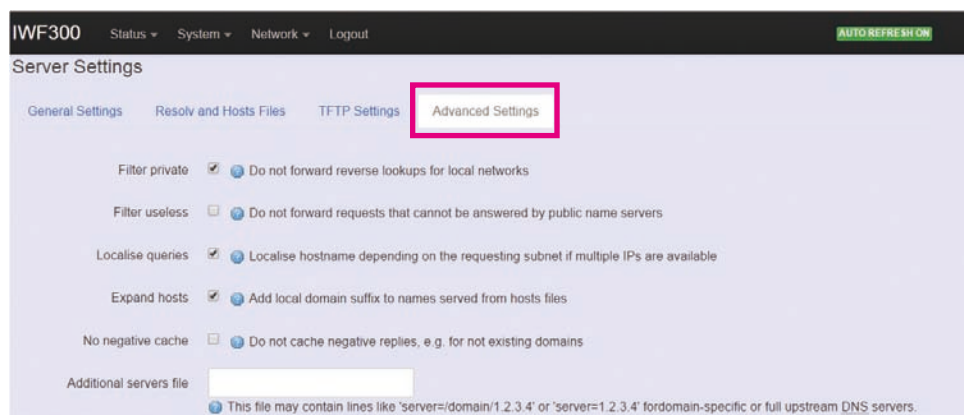
Server Settings

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

Enable TFTP server ☐

By default, TFTP server is not enabled.

2.4.4.4 Advanced Settings



IWF300 Status System Network Logout AUTO REFRESH ON

Server Settings

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

Filter private ☒ Do not forward reverse lookups for local networks

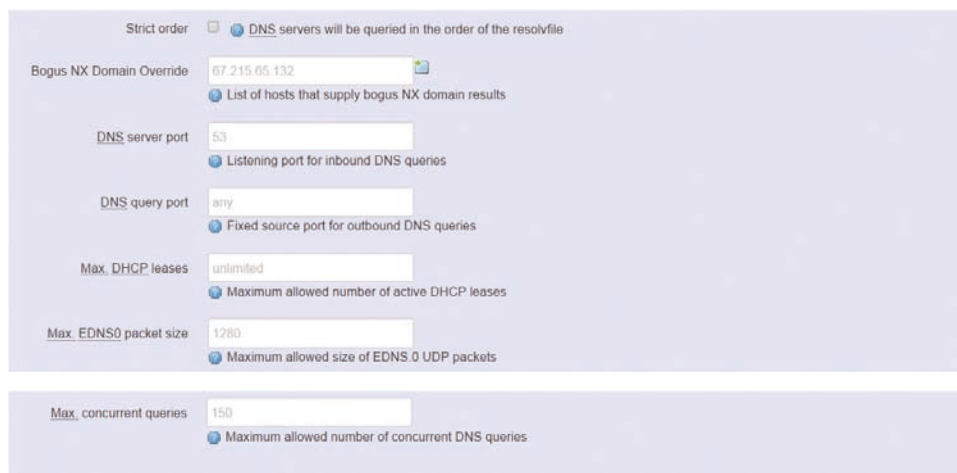
Filter useless ☐ Do not forward requests that cannot be answered by public name servers

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.

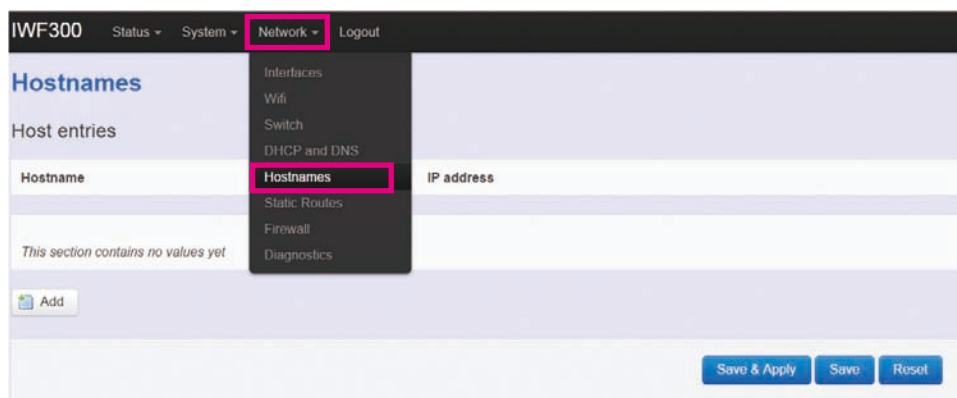


Max. DHCP Leases: Default value is unlimited.

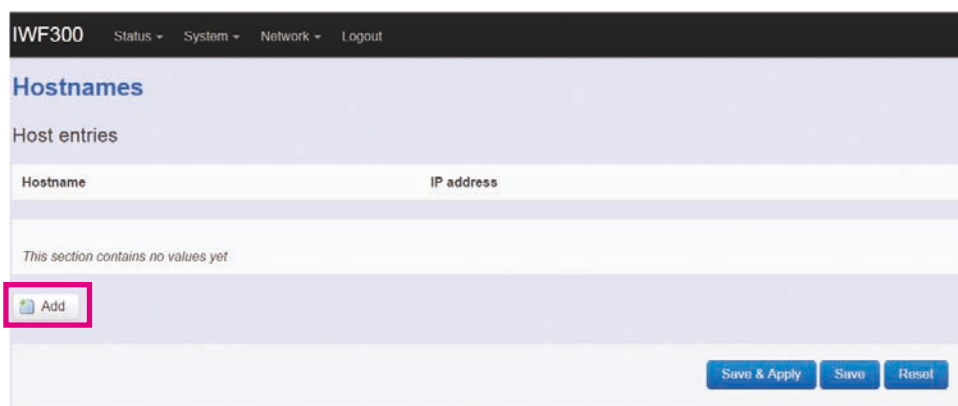
Max. concurrent queries: Default value is 150.

2.4.5 Hostnames

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



For devices that do not have hostname or do not resolve automatically, a hostname-IP paired to a specific device must be assigned.



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

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

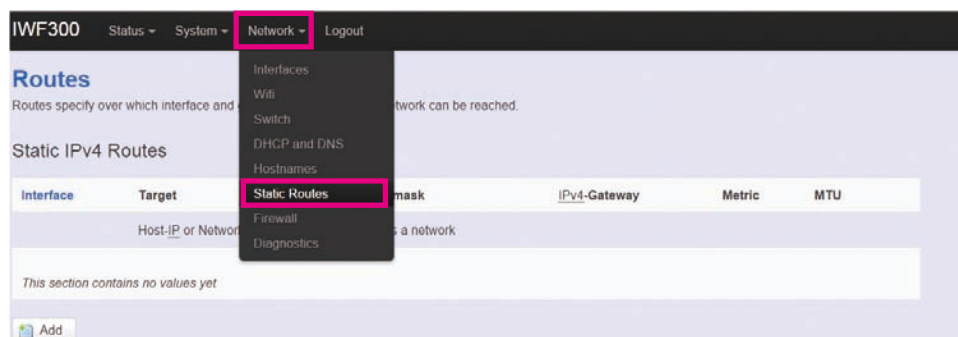


Delete: Delete the followed host entry.

2.4.6 Static Routes

Clicking "Network" -> "Static Routes" in the GUI menu will bring up the "Routes" page for two categories: "Static IPv4 Routes" and "Static IPv6 Routes".

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



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

IWF300 Status System Network Logout

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	If target is a network			

This section contains no values yet

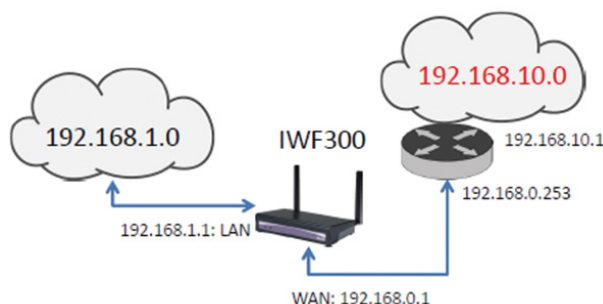
Add

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; IWF 300/IWF 310 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 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			
wan	192.168.10.0	255.255.255.0	192.168.0.253	0	1500

Delete

Add

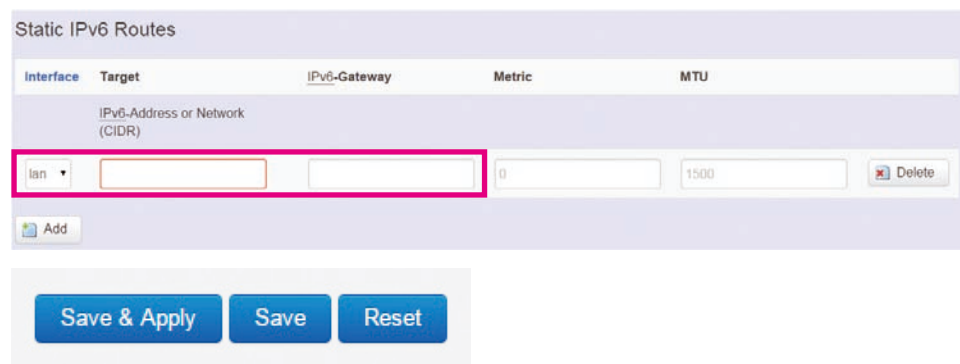
Delete: Delete a followed route entry.

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



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

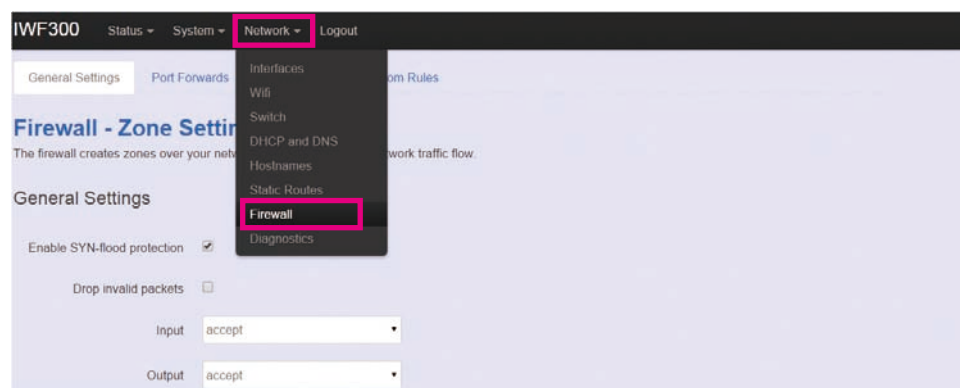
Clicking the “Add” button will show the following entry.



Clicking the “Save & Apply” button will activate the entries.

2.4.7 Firewall

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

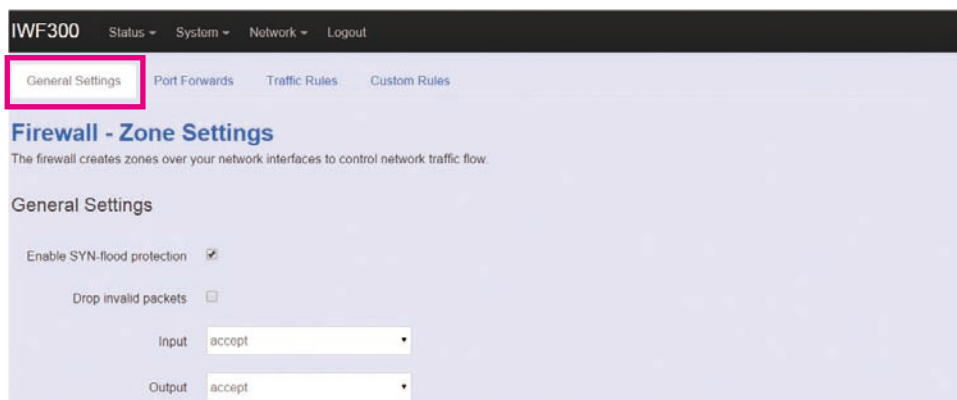


2.4.7.1 General Settings

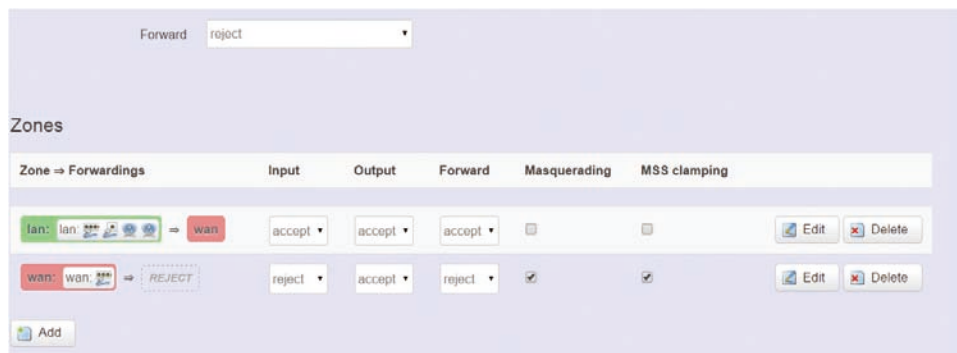
Clicking “General Settings” tab on the top of screen will show the “Zone Settings” configuration including “General Settings” and “Zones” categories.

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, create or edit zones over your network interfaces to control network traffic flow.



There are 3 control buttons for “Zones” settings:

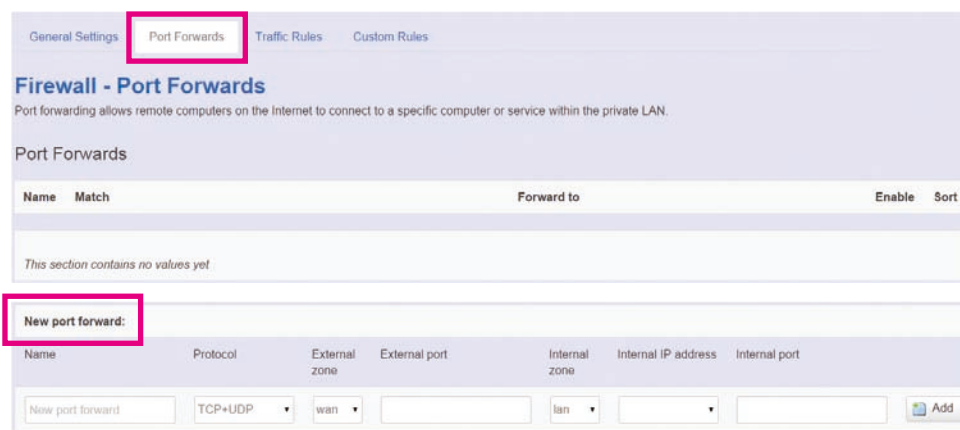
Edit: Edit the followed flow entry.

Delete: Delete the followed flow entry.

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

2.4.7.2 Port Forwards

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

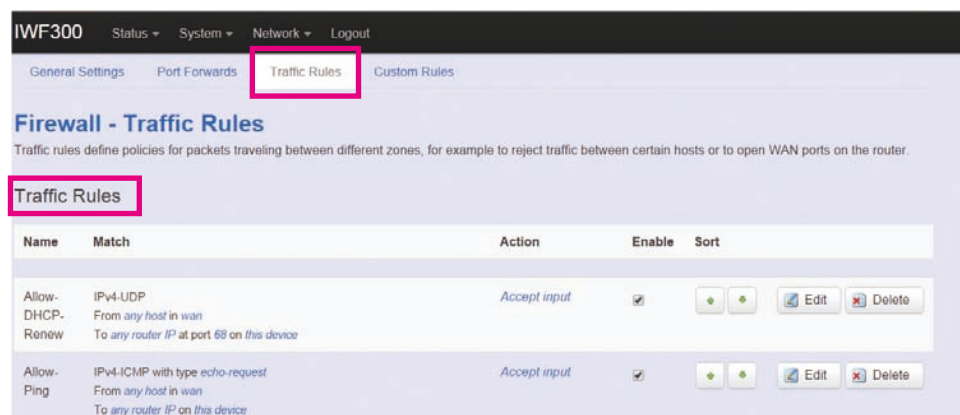


In the “New port forward” category, there is only one button for flow editing:













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

2.4.7.3 Traffic Rules

Clicking the “Traffic Rules” tab on the top of screen will bring up 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).

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"/>	 	 
Allow-ICMPv6-Input	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type, router-solicitation, neighbour-solicitation, router-advertisement, neighbour-advertisement From any host in wan To any router IP on this device	Accept input and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	 	 
Allow-ICMPv6-Forward	IPv6-ICMP with types echo-request, echo-reply, destination-unreachable, packet-too-big, time-exceeded, bad-header, unknown-header-type From any host in wan To any host in any zone	Accept forward and limit to 1000 pkts. per second	<input checked="" type="checkbox"/>	 	 


Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	



New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan



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
New SNAT rule	lan	wan	-- Please choos --	Do not rewrite



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

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





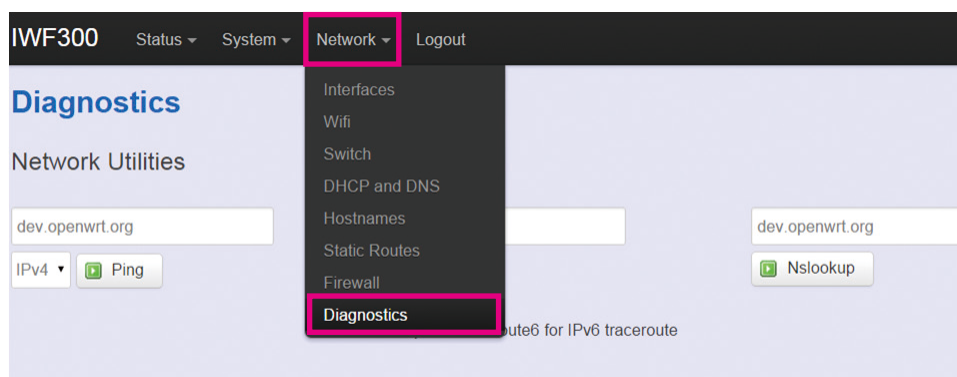
2.4.7.4 Custom Rules

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-starts, right after the default rule-set has been loaded.



2.4.8 Diagnostics

Click "Network" -> "Diagnostics" in the GUI menu, and navigate to the "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.

CHAPTER 3: PRODUCT SPECIFICATION

IWF 300



Main Features

- Dual radios and compliant with 1x 802.11an+1x 802.11 b/g/n 2x2 MIMO
- 1+4 port GbE RJ45 ports
- Up to 27dBm High RF power
- Multiple function: AP/Client/WDS/EZ MESH
- Support 12V DC input
- Support -40 ~ 80°C extended operating temperature

Specifications

Wireless Radio

- 1x IEEE 802.11an 2x2 MIMO
- 1x IEEE 802.11 b/g/n 2x2 MIMO

Frequency Ranges

- USA: 2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.5 ~ 5.7 GHz, 5.725 ~ 5.825 GHz
- Europe: 2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
- Japan: 2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
- China: 2.400 ~ 2.483 GHz, 5.725 ~ 5.85 GHz

RF Output Power: IEEE 802.11an (± 2 dBm)

- IEEE802.11a
 - 12dBm@54M

- IEEE802.11an HT20
 - 12dBm@MCS7
- IEEE802.11an HT40
 - 11dBm@MCS7

RF Output Power: IEEE 802.11 b/g/n (± 2 dBm)

- IEEE802.11b
 - 27dBm@1M
 - 24dBm@11M
- IEEE802.11g
 - 27dBm@6M
 - 24dBm@54M
- IEEE802.11g/n HT20
 - 23dBm@MCS0/8
 - 19dBm@MCS7/15
- IEEE802.11g/n HT40
 - 22dBm@MCS0/8
 - 18dBm@MCS7/15

Receive Sensitivity: IEEE 802.11an

- IEEE802.11a
 - 76dBm@54M
- IEEE802.11a/n HT20
 - 74dBm@MCS7
- IEEE802.11a/n HT40
 - 71dBm@MCS7

Receive Sensitivity: IEEE 802.11a/b/g/n 2Rx

- IEEE802.11b
 - 93dBm@1M
 - 91dBm@11M
- IEEE802.11g
 - 94dBm@6M
 - 80dBm@54M
- IEEE802.11g/n HT20
 - 94dBm@MCS0/8
 - 77dBm@MCS7/15
- IEEE802.11g/n HT40
 - 89dBm@MCS0/8
 - 73dBm@MCS7/15

Hardware

- WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 4
- Compliant with :
 - IEEE802.3/802.3u
 - Hardware based 10/100/1000, full/half, flow control auto negotiation
- Push buttons: 1x Reset; 1x WES
- LED: 1x power & status; 5x RJ45; 1x WES
- Dual band antenna: 2x with RP-SMA connectors

Operating Mode

- AP
- AP router
- Client router
- EZ mesh (at 802.11ac, 5GHz)

Security

- WEP (64/128)
- WAP/WPA2 Mixed
- WPA2-personal (PSK+CCMP/AES)
- WPA2- enterprise (802.1X certification)
- Hidden ESSID support
- MAC address filtering (MAC ACL)
- Station isolation

System Management

- Web-based administration
- SNMP V1/V2c
- SYSLOG information support
- Statistics
- Configuration backup and restore
- One-button-click to restore factory default setting
- Firmware upgrade
- WES

Built-in Servers & Client Interfaces to Other Services

- DHCP client
- SNMP v1/v2 client (coming soon)

Physical and Power

- 12VDC power input
- Wall mountable
- Dimension: 205 x 105 x 25 mm
- Weight: 640g

Environment Protection

- Operating temperature: -40~80°C
- Storage temperature: -45~85°C
- Humidity: 0% to 95% maximum (Non-condensing)
- Vibration: random 0.3g

Certification

- FCC
- CE
- RoHS compliant

Package Contents

- IWF 300 unit x 1
- Dual band antenna x 2
- Wall-mount kit x 1
- AC-DC power adaptor x 1

*Note: The available RF output power will be given by certified power in different region.

IWF 310



Main Features

- Dual radios and compliant with 1x 802.11an+1x 802.11 b/g/n 2x2 MIMO
- 1+4 port GbE RJ45 ports
- Up to 27dBm High RF power
- Multiple function: AP/Router/EZ MESH
- Support 12V DC input
- Support -40 ~ 80°C extended operating temperature

Specifications

Wireless Radio

- 1x IEEE 802.11an 2x2 MIMO
- 1x IEEE 802.11 b/g/n 2x2 MIMO

Frequency Ranges

- USA: 2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.5 ~ 5.7 GHz, 5.725 ~ 5.825 GHz
- Europe: 2.400 ~ 2.483 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
- Japan: 2.400 ~ 2.497 GHz, 5.15 ~ 5.35 GHz, 5.47 ~ 5.725 GHz
- China: 2.400 ~ 2.483 GHz, 5.725 ~ 5.85 GHz

RF Output Power: IEEE 802.11an (± 2 dBm)

- IEEE802.11a
 - 12dBm@54M
- IEEE802.11an HT20
 - 12dBm@MCS7
- IEEE802.11an HT40
 - 11dBm@MCS7

RF Output Power: IEEE 802.11 b/g/n (± 2 dBm)

- IEEE802.11b
 - 27dBm@1M
 - 24dBm@11M
- IEEE802.11g
 - 27dBm@6M
 - 24dBm@54M
- IEEE802.11g/n HT20
 - 23dBm@MCS0/8
 - 19dBm@MCS7/15
- IEEE802.11g/n HT40
 - 22dBm@MCS0/8
 - 18dBm@MCS7/15

Receive Sensitivity: IEEE 802.11an

- IEEE802.11a
 - 76dBm@54M
- IEEE802.11a/n HT20
 - 74dBm@MCS7
- IEEE802.11a/n HT40
 - 71dBm@MCS7

Receive Sensitivity: IEEE 802.11 b/g/n

- IEEE802.11b
 - 93dBm@1M
 - 91dBm@11M
- IEEE802.11g
 - 94dBm@6M
 - 80dBm@54M
- IEEE802.11g/n HT20
 - 94dBm@MCS0/8
 - 77dBm@MCS7/15
- IEEE802.11g/n HT40
 - 89dBm@MCS0/8
 - 73dBm@MCS7/15

Hardware

- WAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 1
- LAN: 10/100/1000 Base-TX MDI/MDIX RJ-45 x 4
- Compliant with :
 - IEEE802.3/802.3u
 - Hardware based 10/100/1000, full/half, flow control auto negotiation
- Push buttons: 1x Reset
- LED: 1x power & status; 5x RJ45
- Antenna connectors: 2x with RP-SMA

Operating Mode

- AP
- AP router
- Client router
- EZ mesh

Security

- WEP (64/128)
- WPA/WPA2 Mixed
- WPA2-personal (PSK+CCMP/AES)
- Hidden ESSID support
- MAC address filtering (MAC ACL)

System Management

- Web-based administration
- SNMP v1/v2c (coming soon)
- SYSLOG information support
- Statistics
- Configuration backup and restore
- One-button-click to restore factory default setting
- Firmware upgrade

Built-in Servers & Client Interfaces to Other Services

- DHCP client
- SNMP v1/v2 client (coming soon)

Physical and Power

- 12VDC power input with DC jack
- Wall mountable
- Dimension: 185 x 108 x 43 mm

Environment Protection

- Operating temperature: -40~80°C
- Storage temperature: -45~85°C
- Humidity: 0% to 95% maximum (Non-condensing)
- Vibration: random 0.3g

Certification

- FCC
- CE
- RoHS compliant
- EN50155 compliant

Package Contents

- IWF 310 unit x 1
- Dual band antenna x 2
- Wall-mount kit x 1
- AC-DC power adaptor x 1

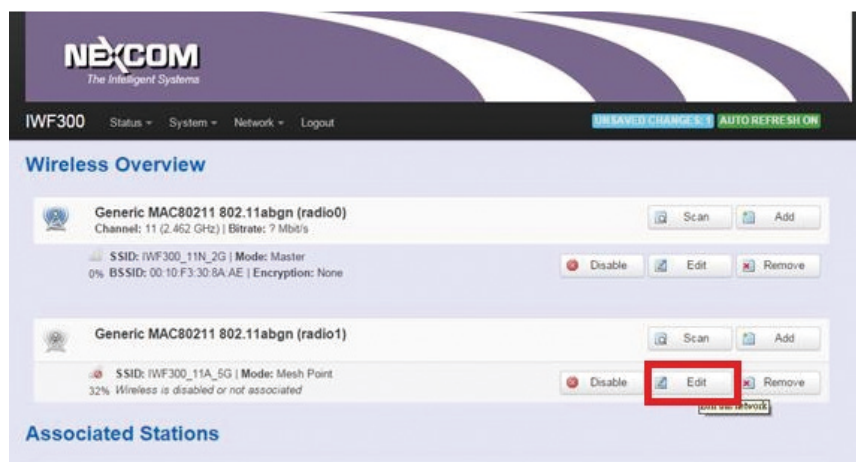
*Note: The available RF output power will be given by certified power in different region.

CHAPTER 4: APPENDIX

4.1 Setting Example

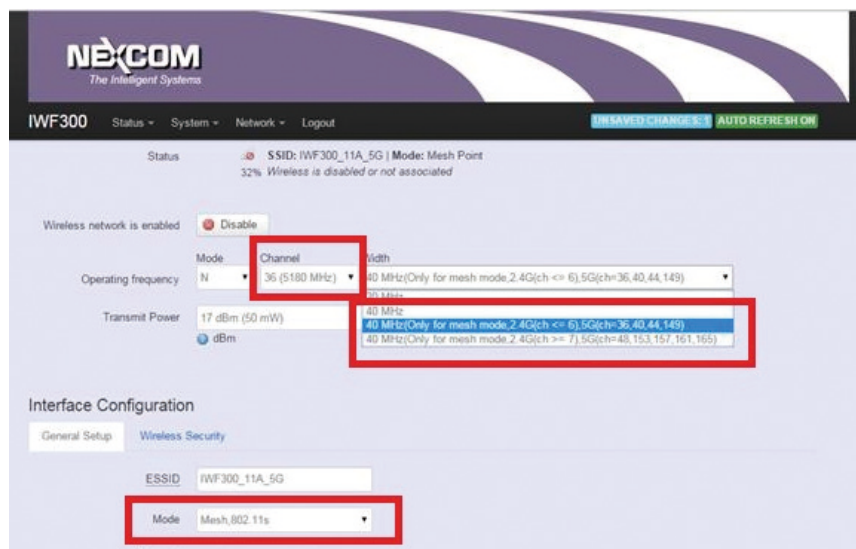
4.1.1 How to configure 5G mesh?

Step 1. In the Network -> Wifi page, press the radio1 (ar9382) "Edit" button.



Step 2. Select the 2.4G channel. Mode=**Access Point**, ESSID, **Bandwidth=20** or **40MHz**.

Step 3. If your 5G channel is 36, 40, 44, 149, select the 40MHz (Only for mesh mode... ch=36, 40, 44, 149) option. If your 5G channel is 48, 153, 157, 161, 165, select the 40MHz (Only for mesh mode... ch=48, 153, 157, 161, 169) option.

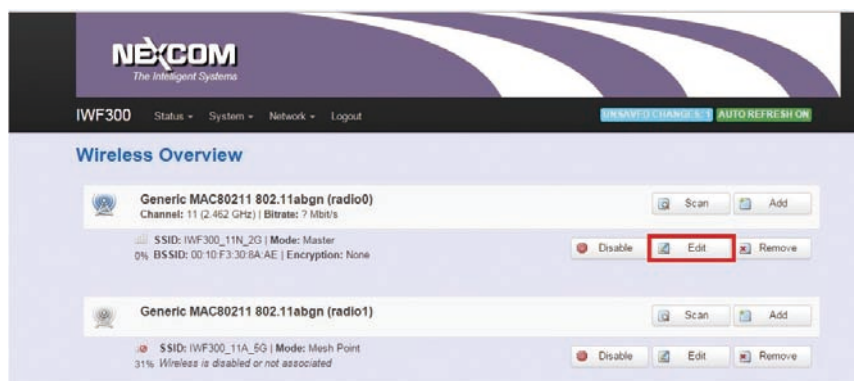


Step 4. Press the "Save & Apply" button.

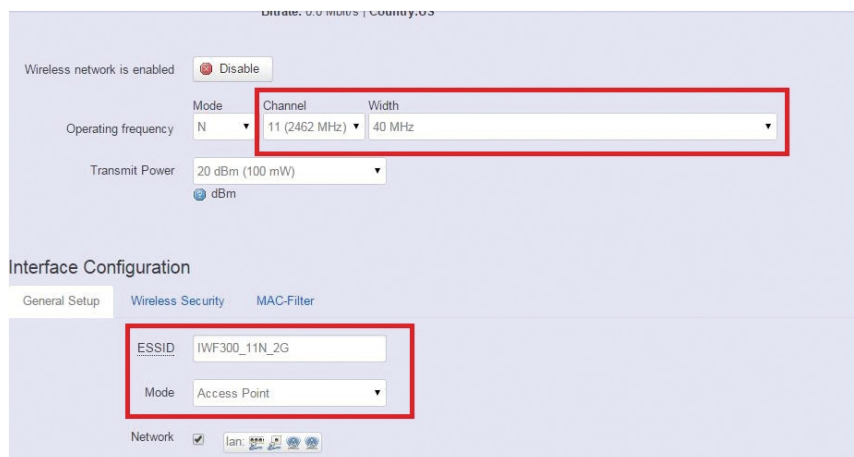


4.1.2 How to configure 2.4G AP?

Step 1. In the Network -> Wifi page, press the radio0 (ar9344) "Edit" button.



Step 2. Select the 2.4G channel. Mode=**Access Point**, ESSID, Bandwidth=20 or 40MHz.

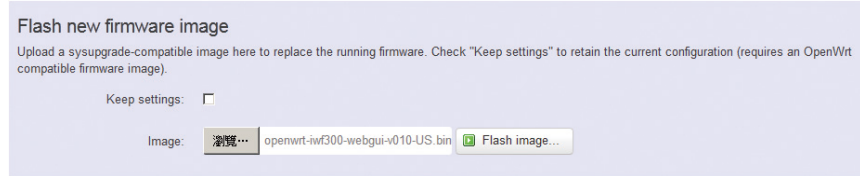


Step 3. Press the "Save & Apply" button.



4.1.3 How to run firmware upgrade?

Step 1. In the System -> Flash firmware page, select your image and press the "Flash image" button.



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ☐

Image:

Step 2. Press the "Proceed" button, then the image will be flashed to the device, please wait for 2 minutes.



Flash Firmware - Verify

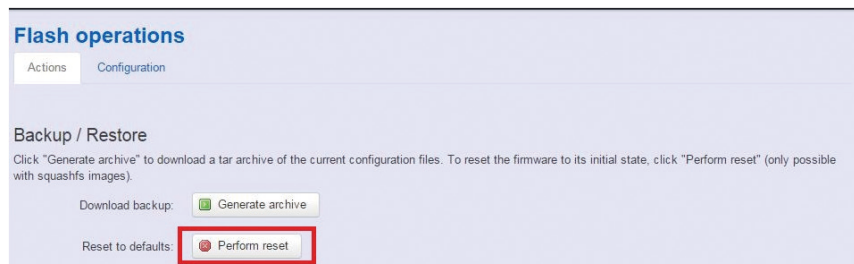
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

- Checksum: 9ebcf94e12237ebee11213911f52c0bf
- Size: 15.24 MB (15.56 MB available)
- Note: Configuration files will be erased.

Powered by LuCI (git-15.236.28194-084d435) / OpenWrt (EU) v0.1.0

4.1.4 How to restore to default settings?

Step 1. In the System->Flash firmware page, press the "Platform reset" button.



IWF 300/IWF 310 Default Parameters:

LAN port default IP = 192.168.1.1

WAN port default IP = DHCP Client

Login user name: root

Login password: admin

WiFi 2G default operating mode = AP mode (SSID: IWF 300/
IWF 310_11N_2G)

WiFi 2G default channel = 11

WiFi 2G default wireless password = (no password)

WiFi 5G default operating mode= Mesh mode (Mesh ID: IWF
300/IWF 310_11A_5G)

WiFi 5G default channel = 36

WiFi 5G default wireless password = (no password)