Manageable Wireless AC1300 Dual-Band Gigabit PoE Indoor Access Point and Router

User Manual

Model 525831 (IW-1300AC-AP)

INTELLINET NETWORK SOLUTIONS®

intellinetnetwork.com

Important: Read before use. • Importante: Leer antes de usar.

CONTENTS

Product Introduction

Thank you for your purchase of the AC1300 Wireless Wave2 High Power Dual Band Gigabit PoE Router. Please read the entire user manual before using the product and save it for future reference.

Product Overview

This Wireless Router is based on the 802.11ac standard, providing up to 1.3 Gbps wireless data transmission rate. If features a built-in high-power wireless signal amplifier, supports Wave 2, provides remote transmission, full coverage and strong signal penetration. The ceiling-type installation design provide wireless up to 1.3 Gbps, three times that of standard wireless Internet. The router's dual-band concurrency technology helps avoid interference. Both bands have power amplifiers to provide faster download speeds, smoother video playback and a better online gaming experience to end users. It provides an integrated router, Wi-Fi access point, a two-port gigabit switch and fire wall functions in one compact, sturdy design. With convenient and comprehensive network management functions, URL filtering, MAC address filtering and the QoS bandwidth control function, this router effectively allocates the client's download rate. It supports wireless data encryption and can guarantee the security of data transmission in wireless network.

Features

- Two 10/100/1000 Mbps LAN ports & one 10/100/1000 Mbps WAN port
- IEEE802.3at PoE power supply function
- Ceiling-type installation design
- Dual 2.4 / 5 GHz bands for fast speeds and more client access
- Standard IEEE802.11a/b/g/n/ac, supports Wave 2
- Up to 1.3 Gbps throughput that automatically adjusts its wireless transmission rate
- Built-in omni-directional antenna to effectively improve wireless signal quality
- Automatic best-channel selection to avoid co-channel interference and improve network stability
- A variety of measures to ensure network security, including 64/128-bit WEP, WPA / WPA2, WPA-PSK / WPA2-PSK encryption and security mechanism
- MAC address-based access control to effectively control access rights and support local and remote Web management

Package Contents

Before installing the Router, make sure that the following items are included in your packaging. If any part is lost or damaged, please contact your place of purchase. In addition, make sure that you have the tools to install the Router safely.

- One AC1300 Wireless Wave2 High Power Dual Band Gigabit PoE Router
- One set of installation components
- One power adapter
- One User Manual

Hardware Connection

Front Panel

The front panel of the Router consists of a series of LED indicators as shown:
The LED Indicators on the front panel show the status of the Router.

Name	Status	Indication
Power	Off	Power is off
	On	Power is on
5G Wi-Fi	Off	The wireless function is disabled
	Flashing	The wireless function is enabled
2.4G Wi-Fi	Off	The wireless function is disabled
	Flashing	The wireless function is enabled

Interface panel

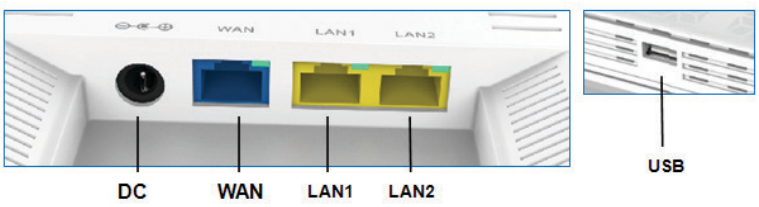


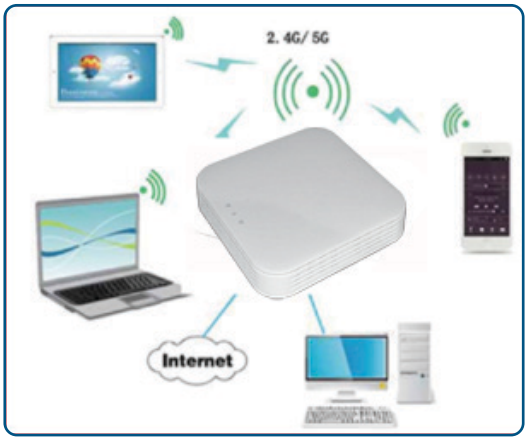
Figure 3: rear panel

WAN: 10/100/1000 Mbps RJ45 port to connect the Cable/xDSL Modem or other LAN; LED connection-status indicator is on the upper right corner of the port

LAN 1 – 2: two LAN ports to connect networked devices, such as PCs, print servers, remote hard drives, and any other compatible device to put on the network; LED connection-status indicator is on the upper right corner of the port
USB: the USB port provided for a 3G USB modem card to connect to the Internet or connect a USB storage device
DC: when PoE cannot be supplied, connect this port to the 12 VDC / 1.5 A power supply adapter

Installation

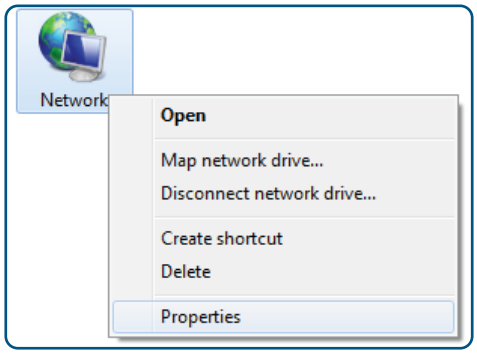
Before installing the Router, make sure the PC is successfully connected to the Internet through broadband service. For any problem, please contact your ISP. Install the Router according to the following steps.



1 Make sure all devices, including your PCs, modem and Router are powered off.
2 Using an Ethernet network cable, connect the LAN or Ethernet network port of the cable or xDSL modem to the Router's WAN port.
3 Power on the cable or xDSL modem, and power on the PC you wish to use to configure the Router.
4 Connect the power adapter to the Router and to an electrical outlet.
5 Setup via Computer

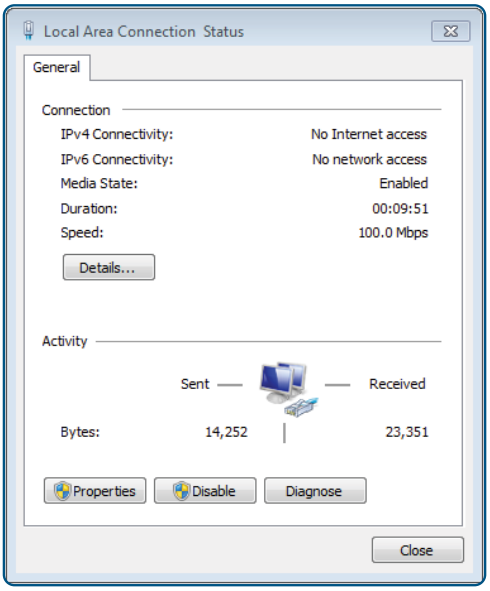
Configure Router through PC

1 On your computer desktop, right click on "Network" and select "Properties."

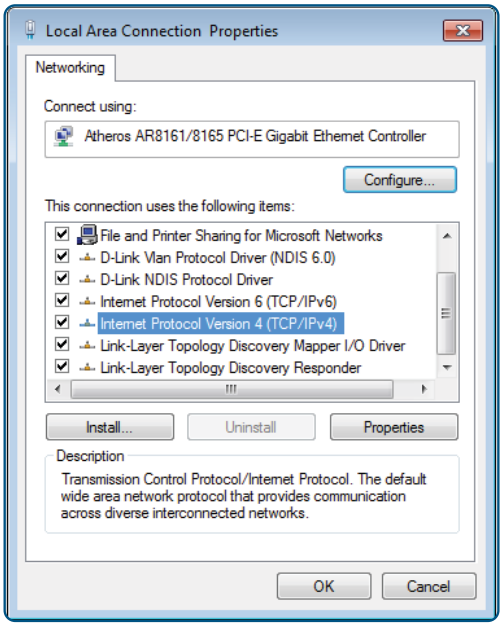


2 Click on "Local Area Connection."

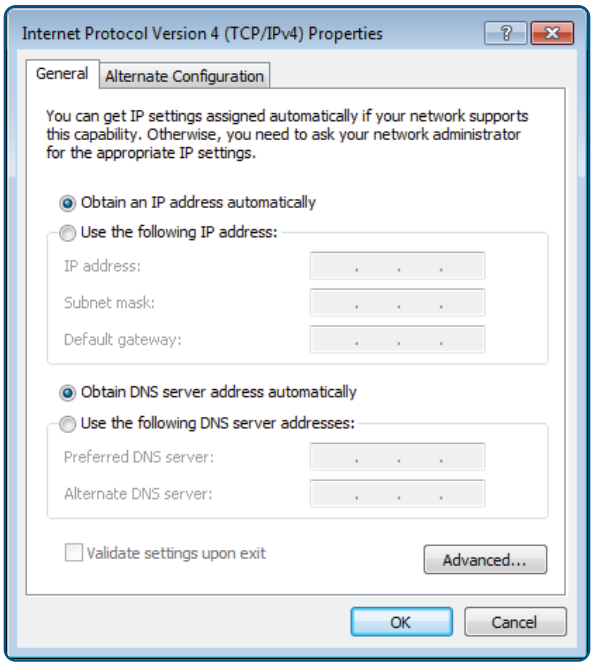
3 Click on "Properties."



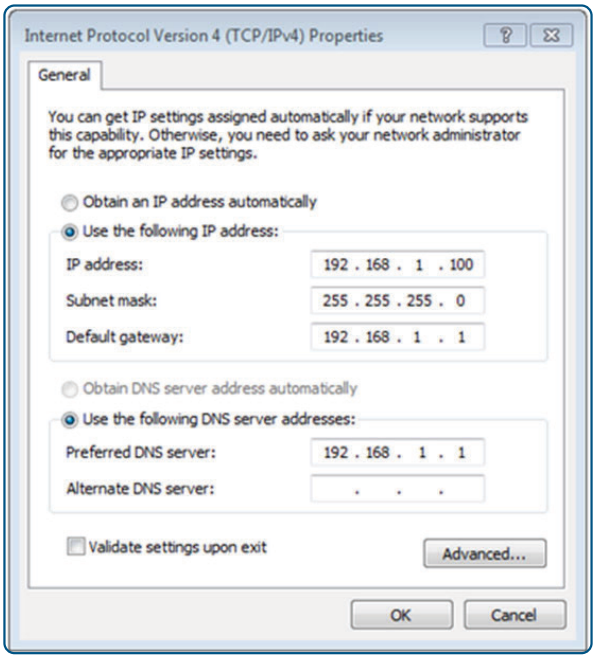
4 Select "Internet Protocol Version 4 (TCP/IPv4)," and then click "Properties."



5 Choose to obtain an IP address automatically or manually set your IP address using the "use the following IP address" option. Then, choose to automatically assign a DNS server or to set it manually:



6 Use the following IP address:



IP address: 192.168.1.XXX: (XXX is a number from 2 – 254)
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1
DNS Server: input the DNS server address provided by the ISP, or use the router default gateway as the DNS proxy server; click "OK" to save the configuration
Click **OK** to save the setting.

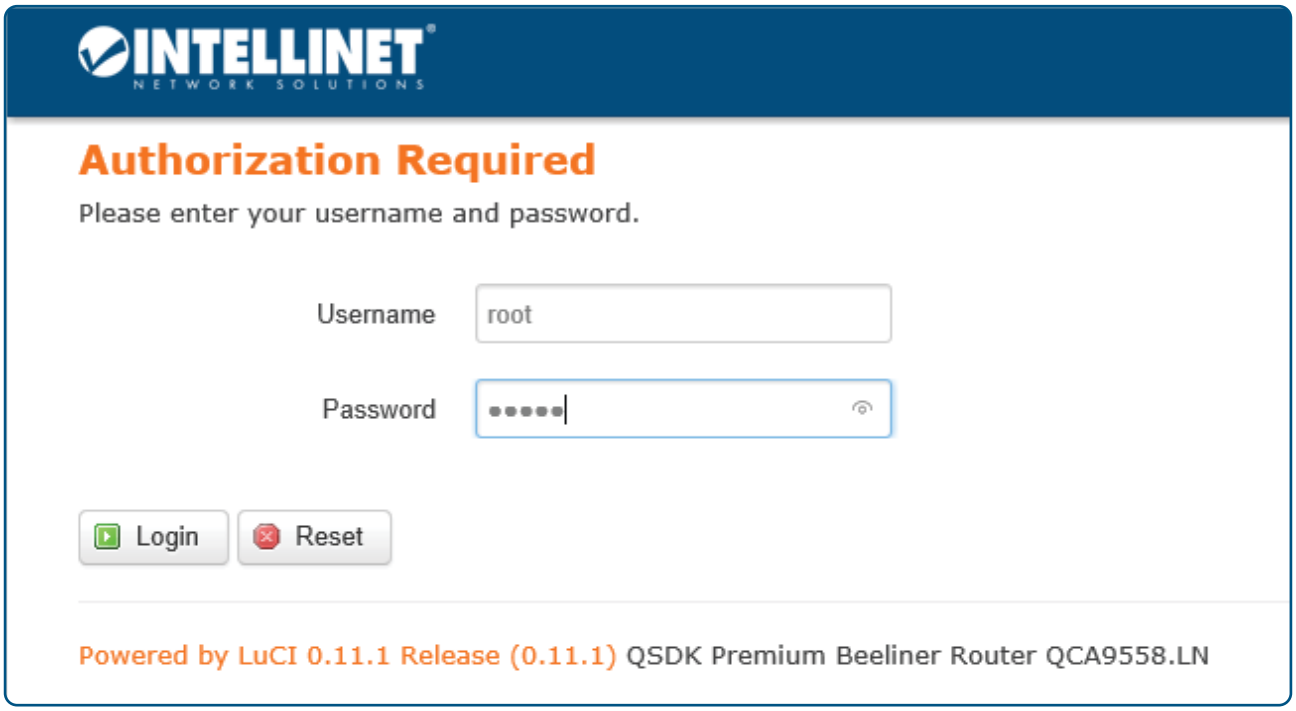
If the DNS server address is unknown, it is recommended to choose "Obtain an IP address automatically" and "Obtain DNS server address automatically."

Logon Screen

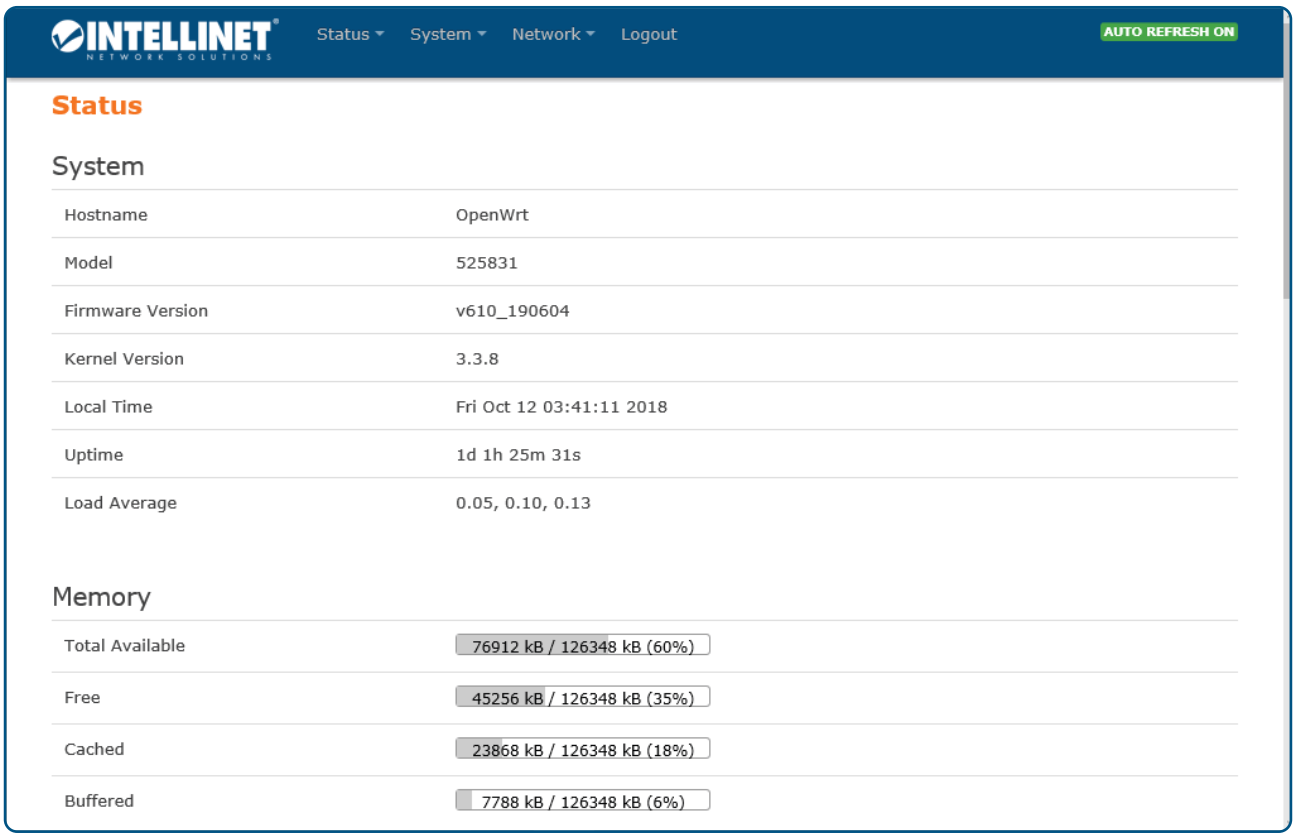
Log into the Router:

1 Open a browser window and enter http://192.168.1.1 in the address bar.

2 The username is "**root**", password is "**admin**". Click on the "Login," and the login page follows:



3 Once logged in, click the menu on the left side of the home page to go to the corresponding sub-page.



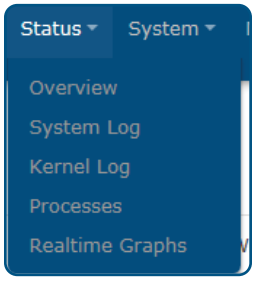
Common Interface Buttons and Operations

Button	Meaning
Save & Apply	Save and Apply current configuration information
Save	Save current configuration information
Reset	Restore factory settings
Connect	Reconnect this interface
Stop	Shutdown this interface
Edit	Edit this interface
Disable	Shutdown this interface
Remove	Delete this interface
Add	Add
Sync with browser	Synchronize local time with browser time
Generate archive	Back up the current system profile
Upload archive...	To restore configuration files, upload a previously generated backup archive here
Perform reset	Restore factory settings
Browse	Select file

Function Configuration

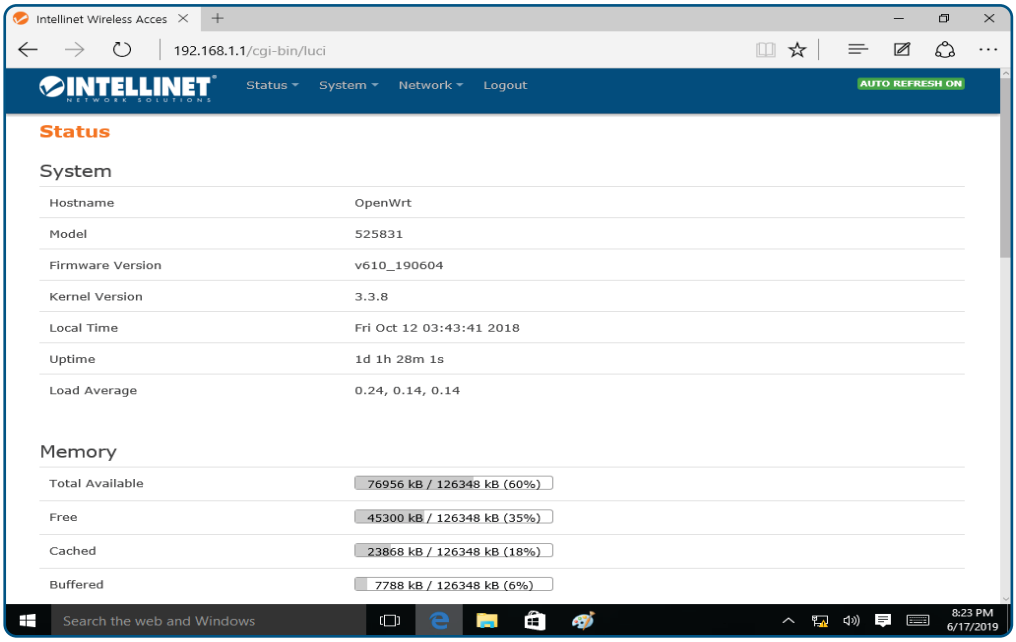
Status

Click the "**Status**" tab to view Overview, System Log, Kernel Log, Processes and Realtime Graphs.



Overview

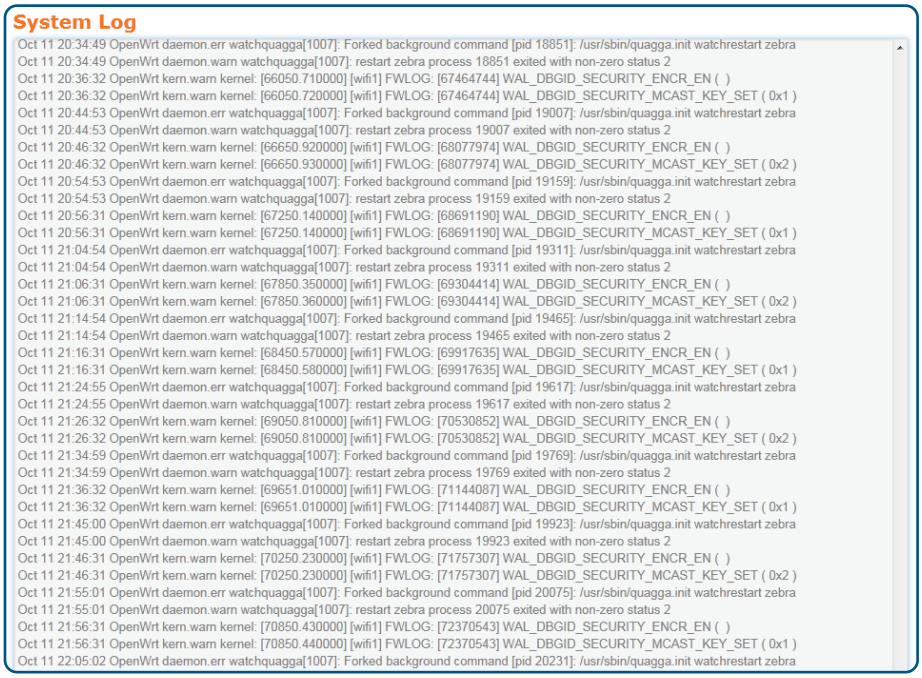
Click on the "Status>Overview" option for the following interface:



This interface shows "System" information (Hostname, Model, Firmware Version, Kernel Version, Local Time, Uptime, Load Average), "Memory" information (Total Available, Free, Cached, Buffered), "Network" information (IPv4 WAN Status, IPv6 WAN Status, Active Connections), "DHCP Leases" information, "DHCPv6 Leases" information, "Wireless" information, and "Associated Stations" information.

System Log

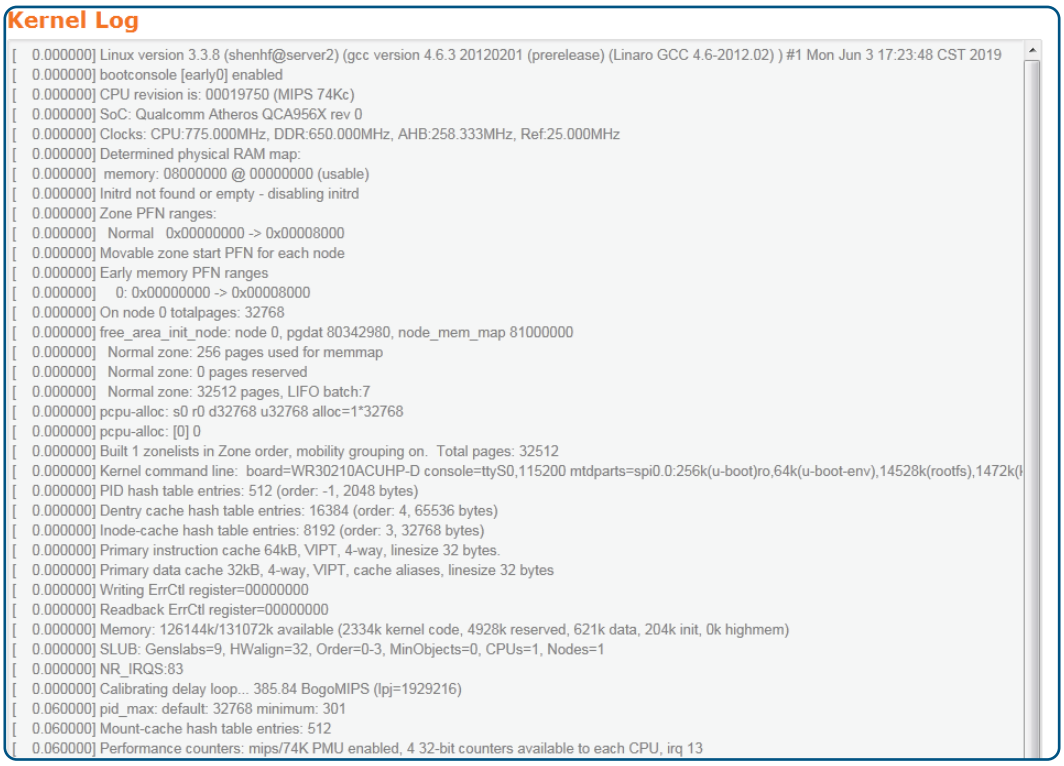
Click on the "Status>System Log" option for the following interface:



This interface offers a log of link establishment failures, packet filter log information, etc. By logging into the log host, the system administrator can analyze and understand log events. Logs can help administrators locate faults, troubleshoot, and also help manage network security.

Kernel Log

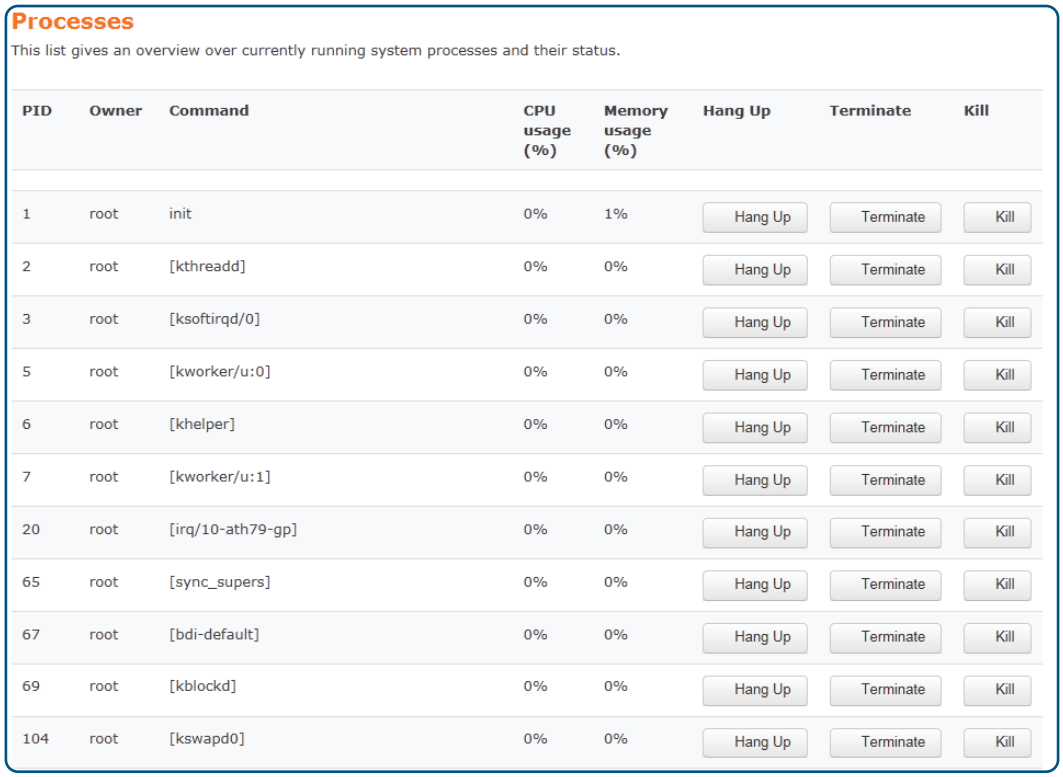
Click on the "Status>Kernel Log" option for the following interface:



This interface shows the live system log.

Processes

Click on the "Status>Processes" option for the following interface:



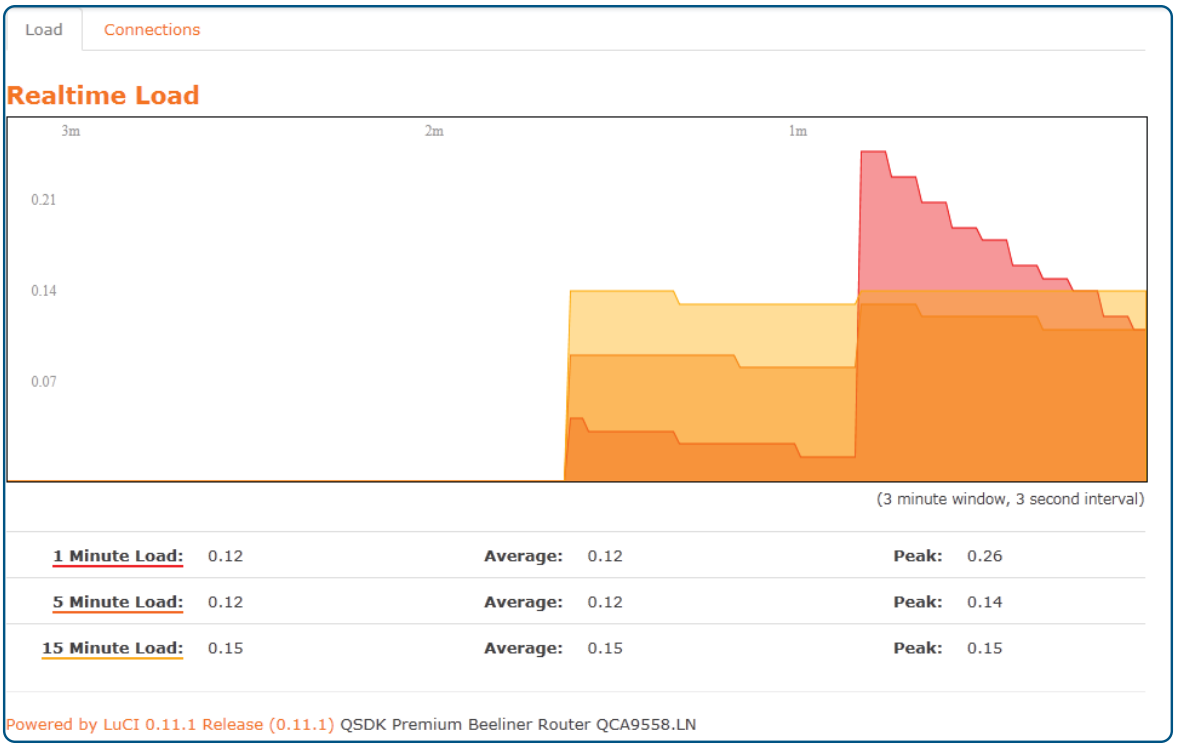
This interface shows system processes and their status. It also includes options to suspend/ hang up, terminate and, when terminate is non-responsive, kill operations.

Realtime Graphs

Click the "Status>Realtime Graphs" option to see Load, Traffic, Wireless and Connections options.

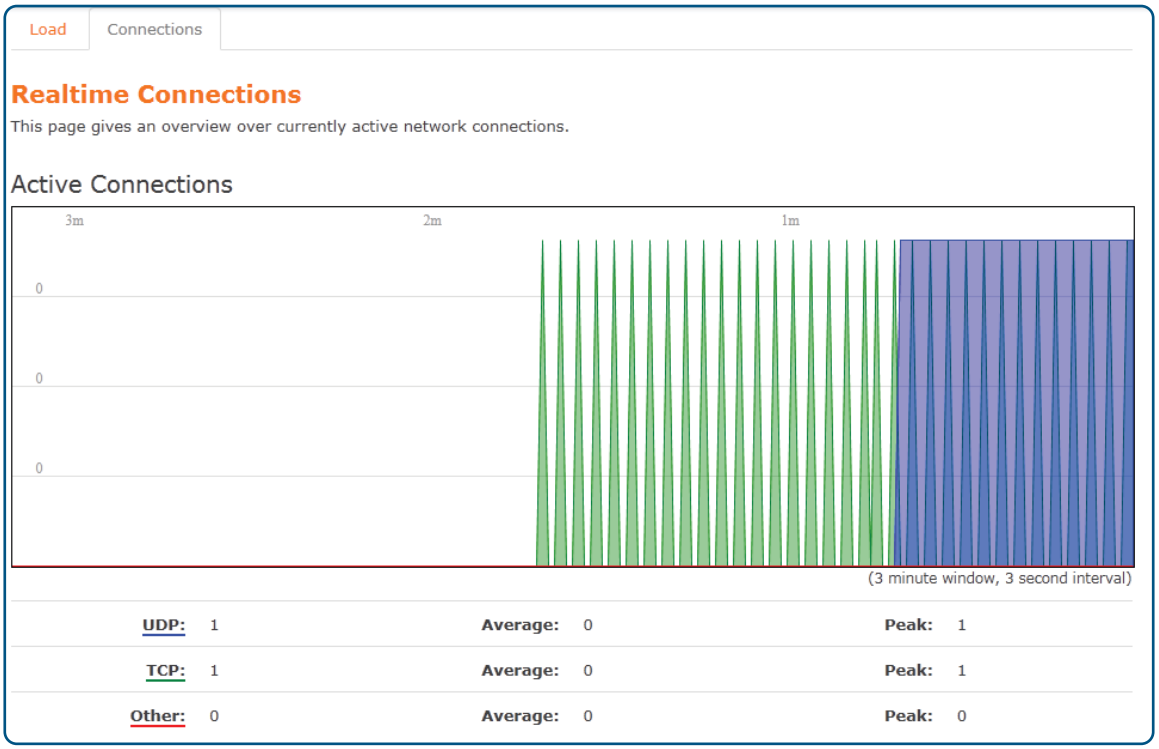
Status>Realtime Graphs>Load

Click the "Status>Realtime Graphs>Load" option for the following screen:



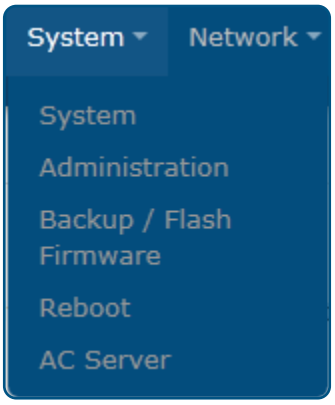
Status>Realtime Graphs>Connections

Click the "Status>Realtime Graphs>Connections" option to see Realtime Connections information.



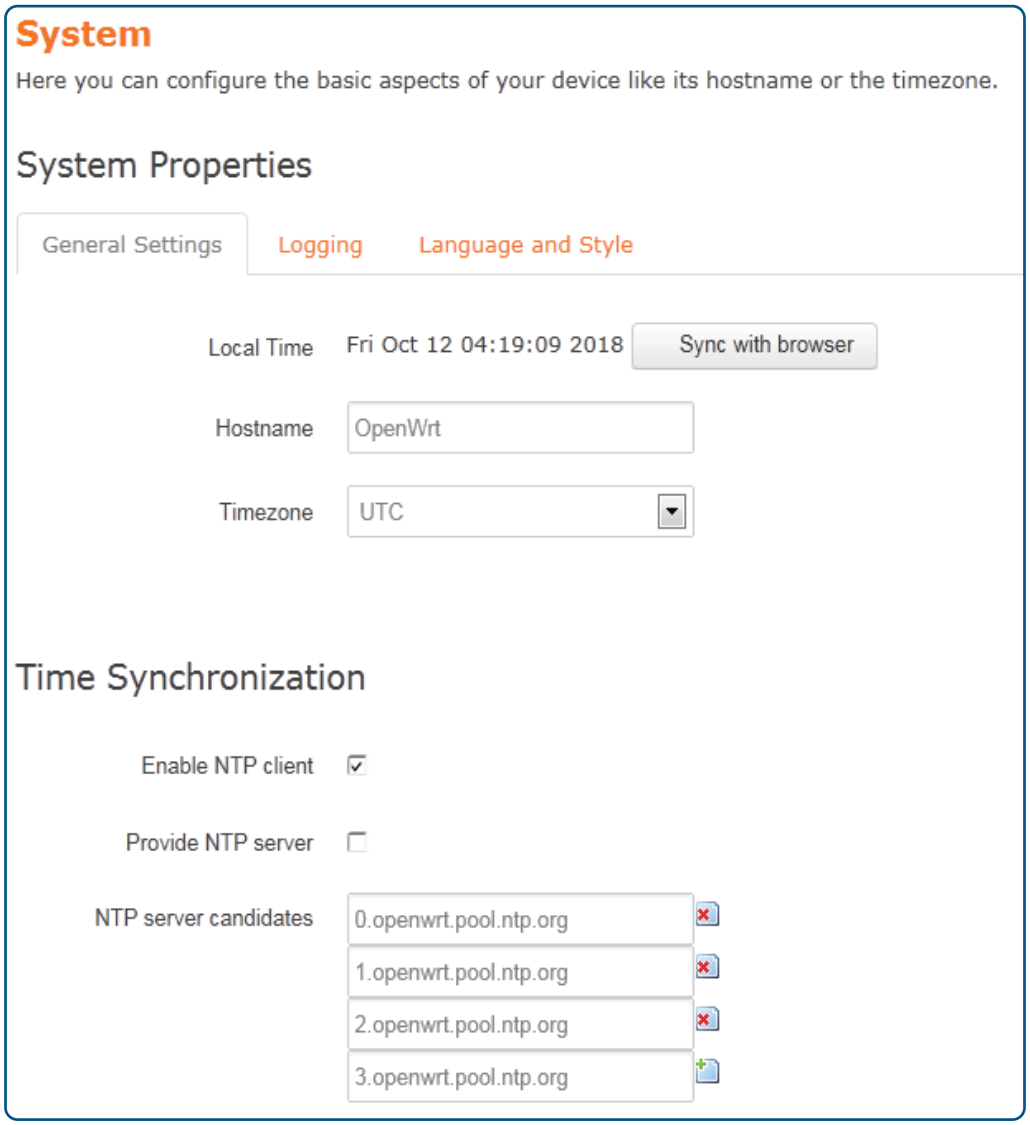
System

Click on "System" to see options for System, Administration, Backup/Flash Firmware, Reboot, and AC Server.

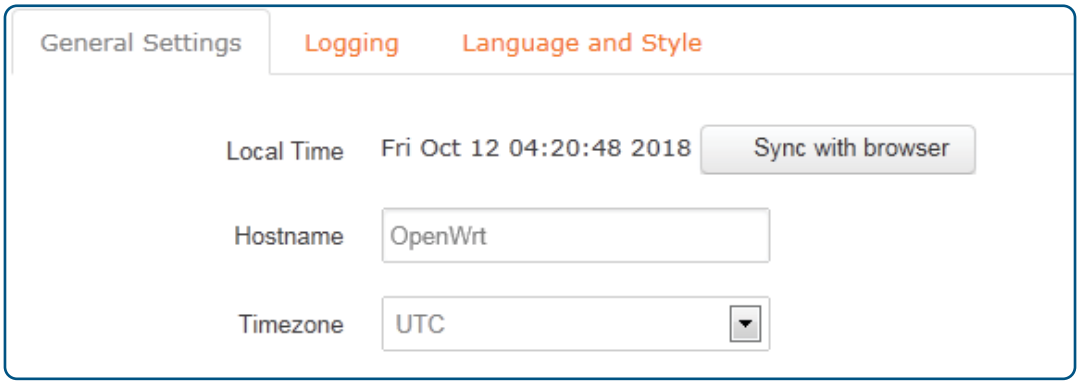


System

Click the "System>System" option to set System Properties and Time Synchronization.

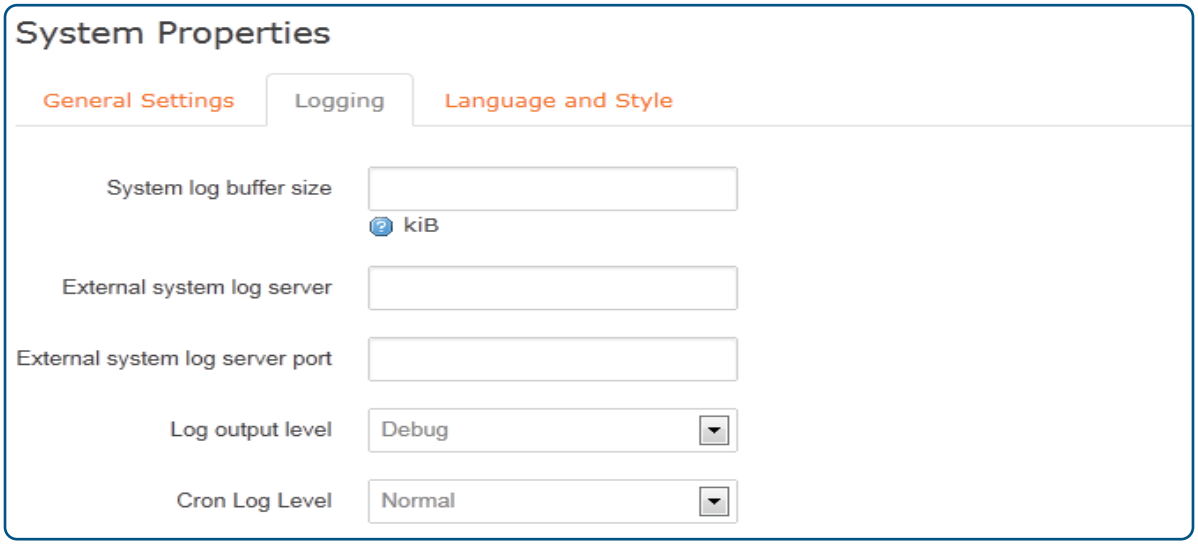


System Properties
System Properties are divided into "General Settings," "Logging" and "Language and Style" options.
Click on the "General Settings" option for the following interface:



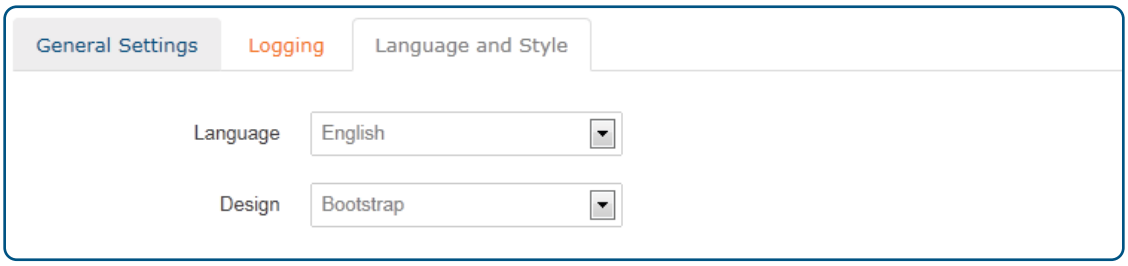
Local Time: click "Sync with browser" to synchronize the system time with the time on your computer
Hostname: provide a router name
Timezone: select the desired time zone from the drop-down list

Click on the "Logging" option for the following interface:

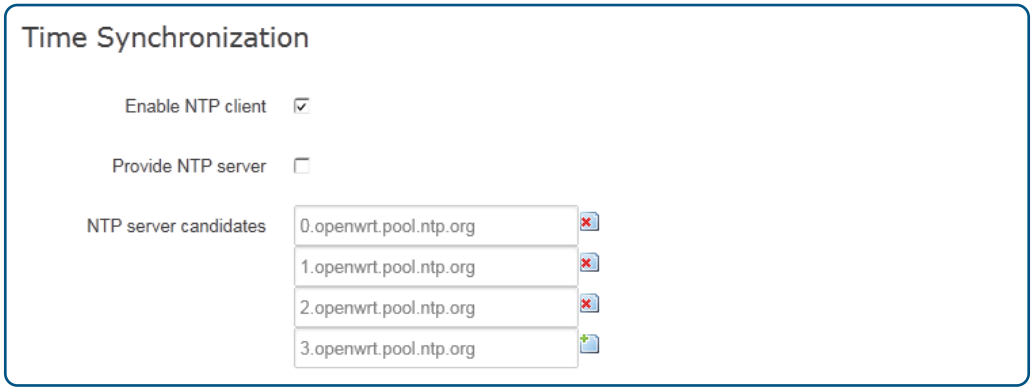


System log buffer size: specify the size of the log buffer
External system log server: configure a remote host to receive log information
External system log server port: configure a suitable port for the remote log server
Log output level: select the level of output log to include Debug, Info, Notice, Warning, Error, Critical, Alert or Emergency
Cron Log Level: select the level of Cron Log to include Debug, Normal and Warning

Click on the "Language and Style" option for the following interface:



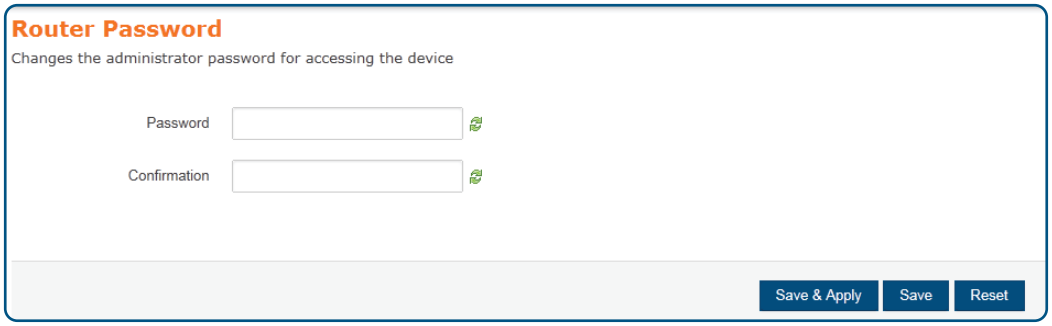
Language: select the language used by the router management interface; offers three options: auto (based on your computer's language), English and Chinese.
Time Synchronization: interface settings, as follows —



Enable NTP client: enables the Local Time of the router to be synchronized with the NTP servers
Provide NTP server: enables the router to work as an NTP server to provide time parameters to any requesters

Administration

Click on the "System>Administration" option for the following interface:



Password: Change the administrator password used to access the router; see warnings on password compliance at the end of the field and address requirements till resolved
Confirmation: verify the new password

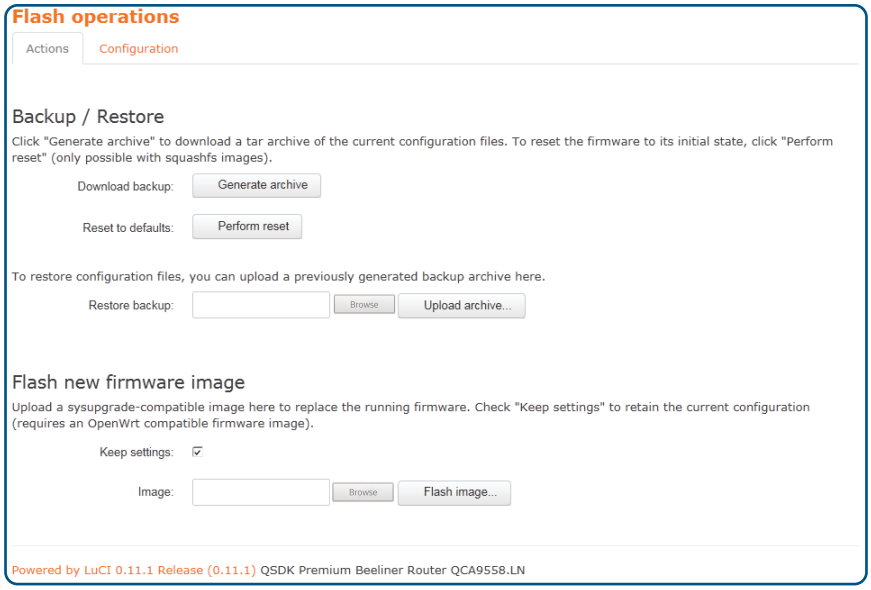
Click "Save & Apply" for settings to take effect.

Backup/Flash Firmware

Click the "System>Backup/Flash Firmware" option to see Action and Configuration options.

Action

Click "System>Backup/Flash Firmware>Action" option for the following interface:

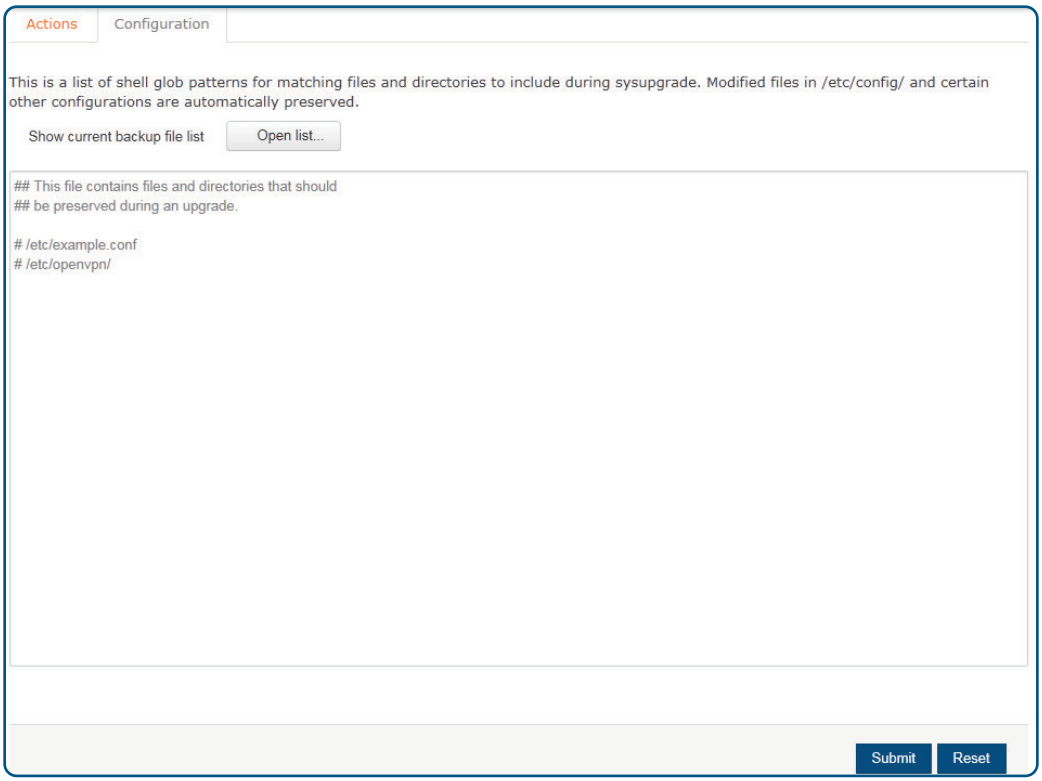


Download backup: to download a TAR archive of the current configuration files — upgrading the firmware of the router or changing its settings may delete the current configuration; save the current configuration files to easily restore the router to the original configuration if necessary

Reset to defaults: click the "Perform reset" button to restart the router and restore its settings to the factory default state (Includes:
the default user name: root; default password: empty; default IP address: 192.168.1.1; default netmask: 255.255.255.0)
Note: back up the configuration before restoring to factory-default settings; if necessary, load the backup configuration file to restore the router to its original state
Restore backup: click "Browse" to find the backup file; select the file and click "upload archive" to complete the recover configuration
Keep settings: check the box to write new firmware immediately while retaining the original system configuration;
if unchecked, new firmware written to the flash memory will erase the original configuration
Image: click "Browse" to find the new firmware file; select the new firmware file, then click on the "Flash image" to flash the new firmware operation.

Configuration

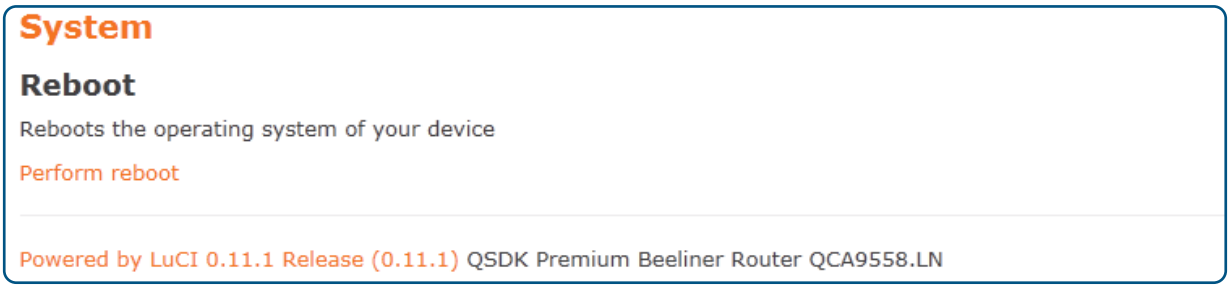
Click "System>Backup/Flash Firmware>Configuration" option for the following interface:



Click "Open list" for a list of files to be backed up. The configuration file contains the necessary foundation files and user-defined files to be backed up.

Reboot

Click on the "System>Reboot" option for the following interface:



Click "Perform reboot" to manually restart the router. Some settings may require a manual reboot of the router to take effect.

Functions that automatically restart the router after settings are changed:
- Immediately writing new router firmware
- Restore the router's factory settings
- Modify the basic network parameters of the LAN port

Functions that require a manual restart of the router to take effect:
- Set QSS security settings function
- Set DHCP services
- Set a static address assignment DHCP server function
- Set the basic parameters of the wireless network
- Modify the security settings of the wireless network
- Modify advanced settings of the wireless network
- Web modify remote router management port

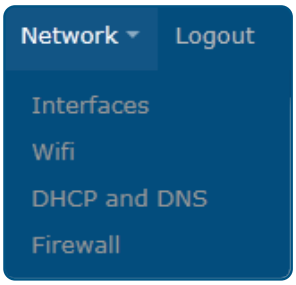
AC Server

Click on the "System>AC Server" option for the following interface:

AC Server Mode: Change the management mode for controlling the AP device.

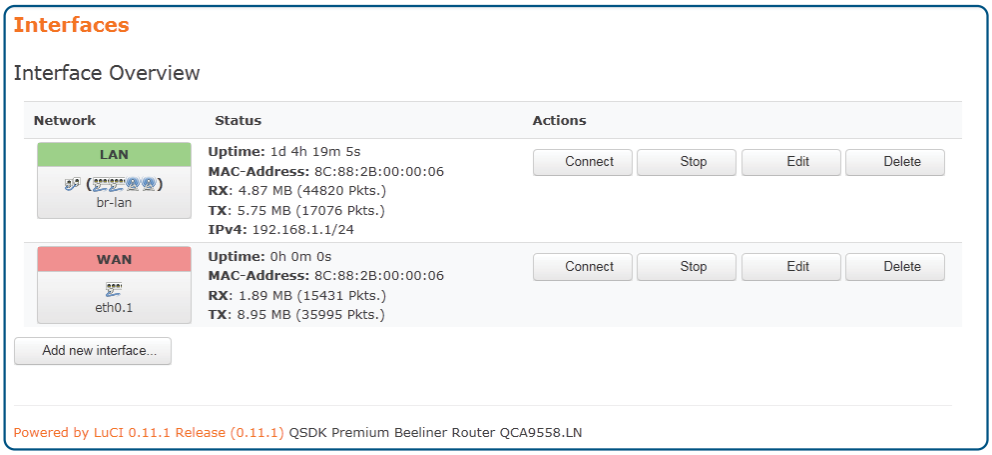
Network

Click "Network" for options on Interfaces, Wifi, DHCP and DNS, and Firewall.



Interfaces

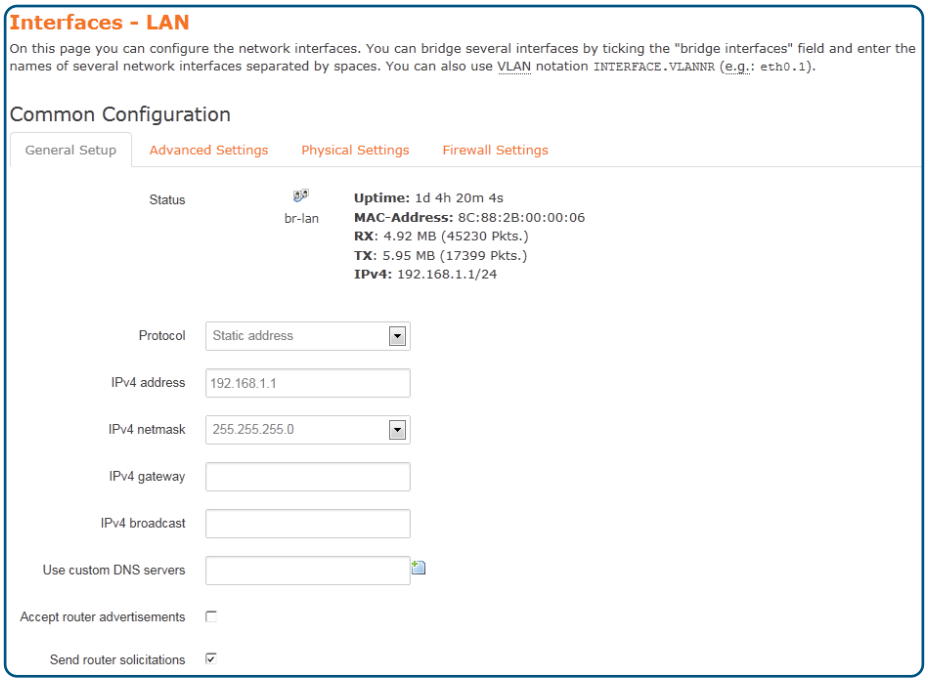
Click the "Network>Interfaces" option for the following screen:



On this page, select and set WAN or LAN preferences.

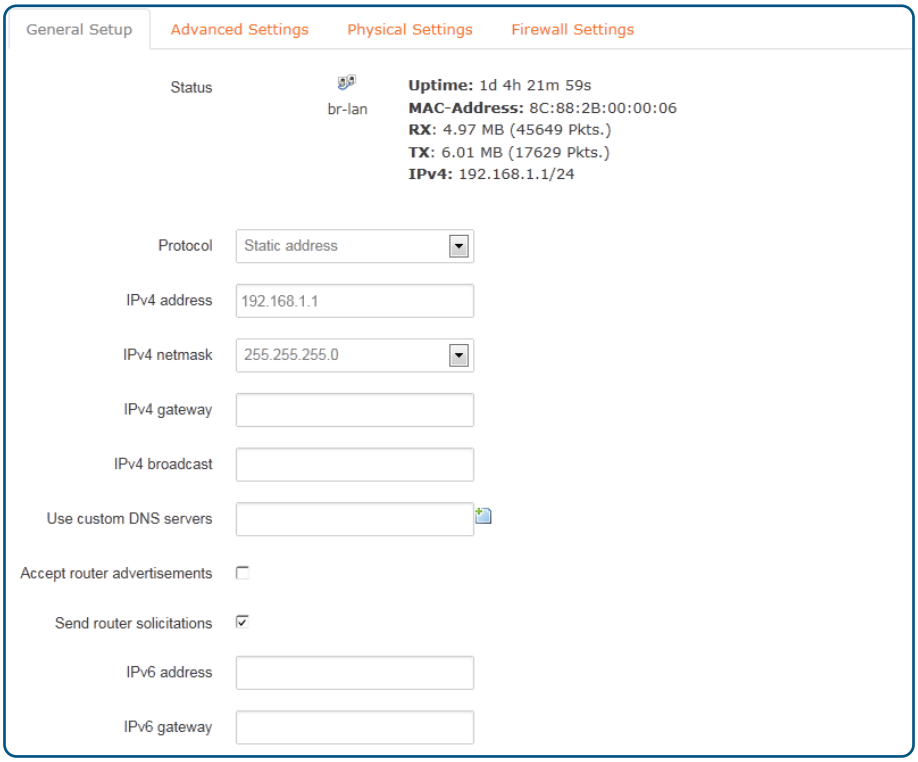
Network>Interfaces>LAN

Click the "Network>Interfaces>LAN" option to configure the network interfaces (LAN).



Common Configuration

The "Common Configuration" screen is as follows:



Set the IP address and netmask. You can, then, manage the router via this IP address. Or if not needed, keeps the default values.
Protocol: select the protocol type
IPv4 address: enter the router's IP address on the LAN; the IP address of all computers in the LAN must be in the same network segment and the default gateway is this IP address; the factory default IP address is 192.168.1.1; for Class C IP addresses; change it according to network needs
IPv4 netmask: here, you can set the relevant netmask
IPv4 gateway: enter this router on the LAN gateway; the default is 192.168.1.1
Use custom DNS servers: the DNS address provided by your ISP; if not provided, the default is 192.168.1.1

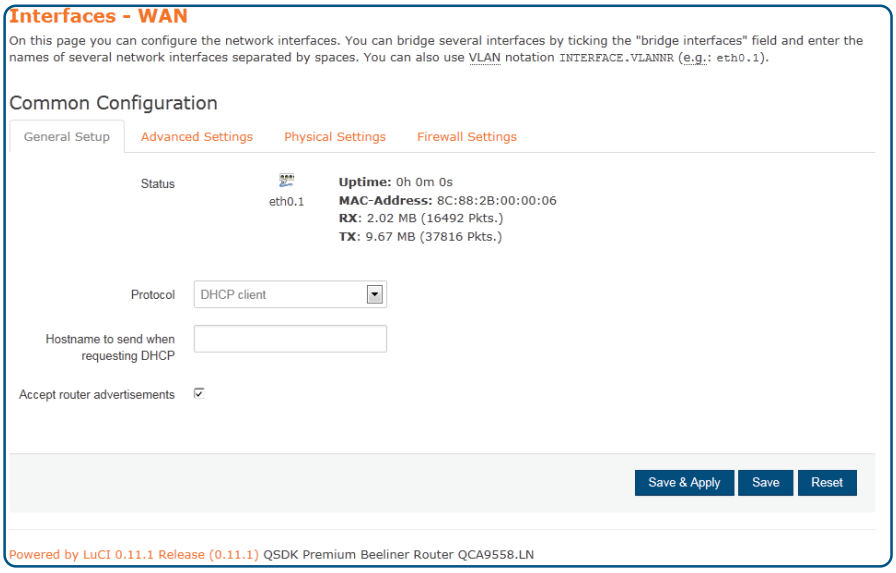
DHCP Server

The DHCP Server setting interface is as follows:

Ignore interface: Check this box to disable this DHCP function for the interface.

Network>Interfaces>WAN

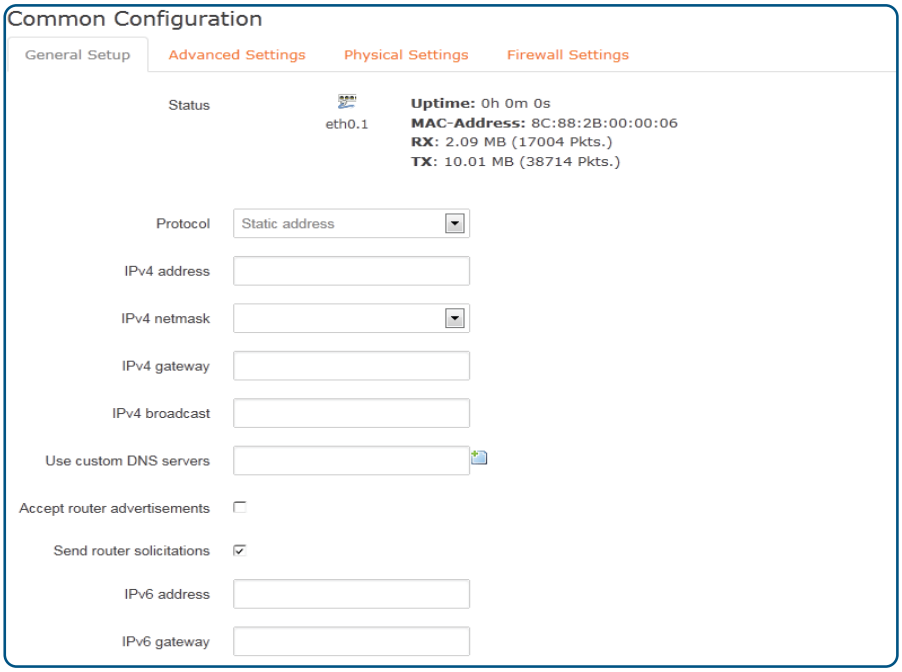
Click the "Network>Interfaces>WAN" option to enter the WAN port settings interface.

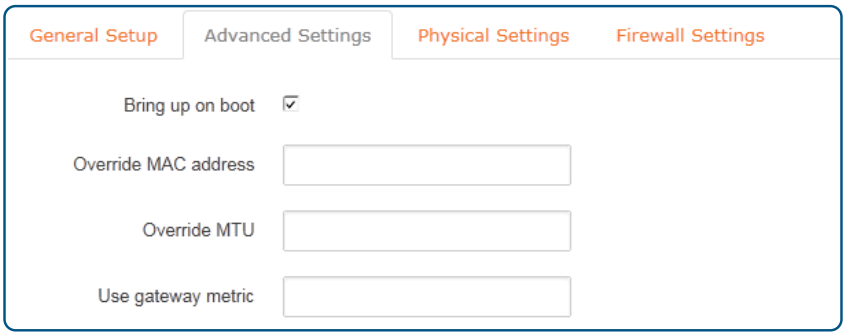


Selectable options for the Protocol: Static address, DHCP client, PPPoE, Unmanaged, PPP.

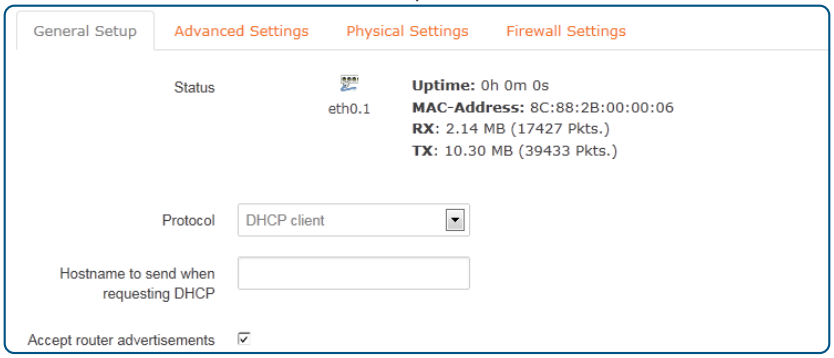
Static address

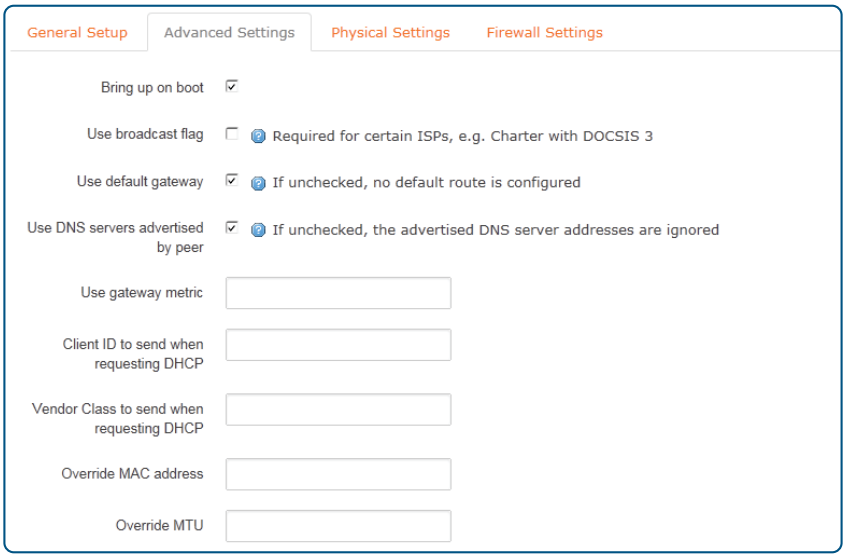
If the "static address" protocol is selected, provide the following information according to the supplier's (ISP) requirements. Click the "Save & Apply" button.



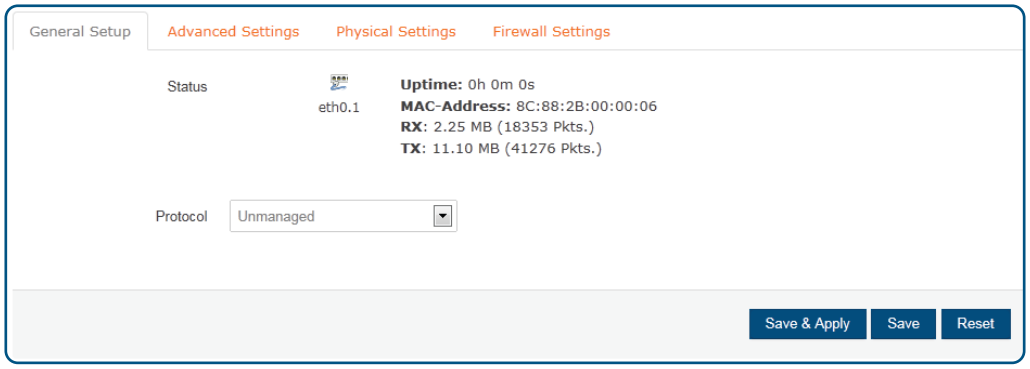


Ipv4 address: the router's IP address on the WAN; enter the public IP address provided by your ISP
Ipv4 netmask: the netmask for the WAN interface; enter the netmask provided by your ISP
Ipv4 gateway: fill in the gateway provided by the ISP
Use custom DNS server: fill with information provided by your ISP's
Override MAC address: the default value is the MAC address of the WAN interface of this router; some ISPs may require MAC address binding, and the ISP will provide a valid MAC address to the user; in this case, input the provided value in the "MAC address" column; changing the MAC address is not recommended unless the ISP has special requirements
Override MTU: the default value is 1500
DHCP client: select "DHCP client" protocol and enter the MAC address of the computer as the modem MAC address of the router; click the "Save & Apply" button.



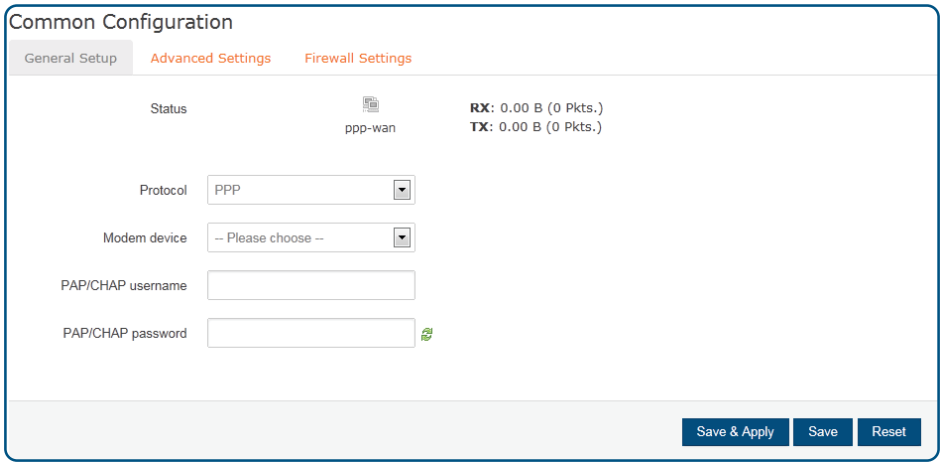


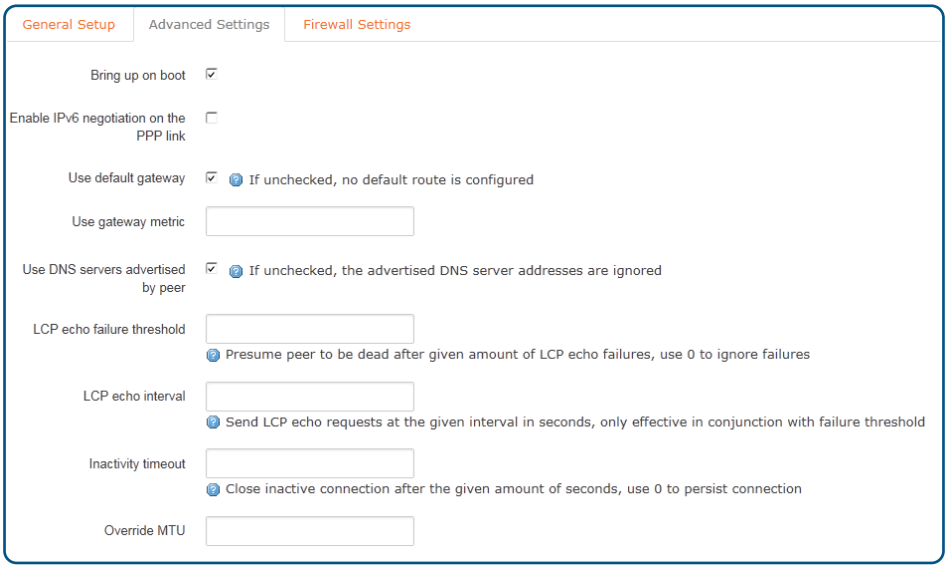
Hostname to send when requesting DHCP: enter the host name of this feature
Use broadcast flag: use this option according to ISP
Use default gateway: if unchecked, no default route is configured
Use DNS servers advertised by peer: if unchecked, the advertised DNS server address is ignored
Use gateway metric: for every gateway (e.g., router), the metric is increased by 1
Client ID to send when requesting DHCP: the identity number of the router that is used while obtaining the WAN IP address from ISP
Vendor Class to send when requesting DHCP: the vendor class of the router that is used while obtaining the WAN IP address from ISP
Override MAC address: the default value is the MAC address of the WAN interface of this router; some ISPs may require MAC address binding, and the ISP will provide a valid MAC address to the user; in this case, input the provided value in the "MAC address" column; changing the MAC address is not recommended unless the ISP has special requirements
Override MTU: the default value is 1500
Protocol: if "Unmanaged" is selected, there is no need to set.



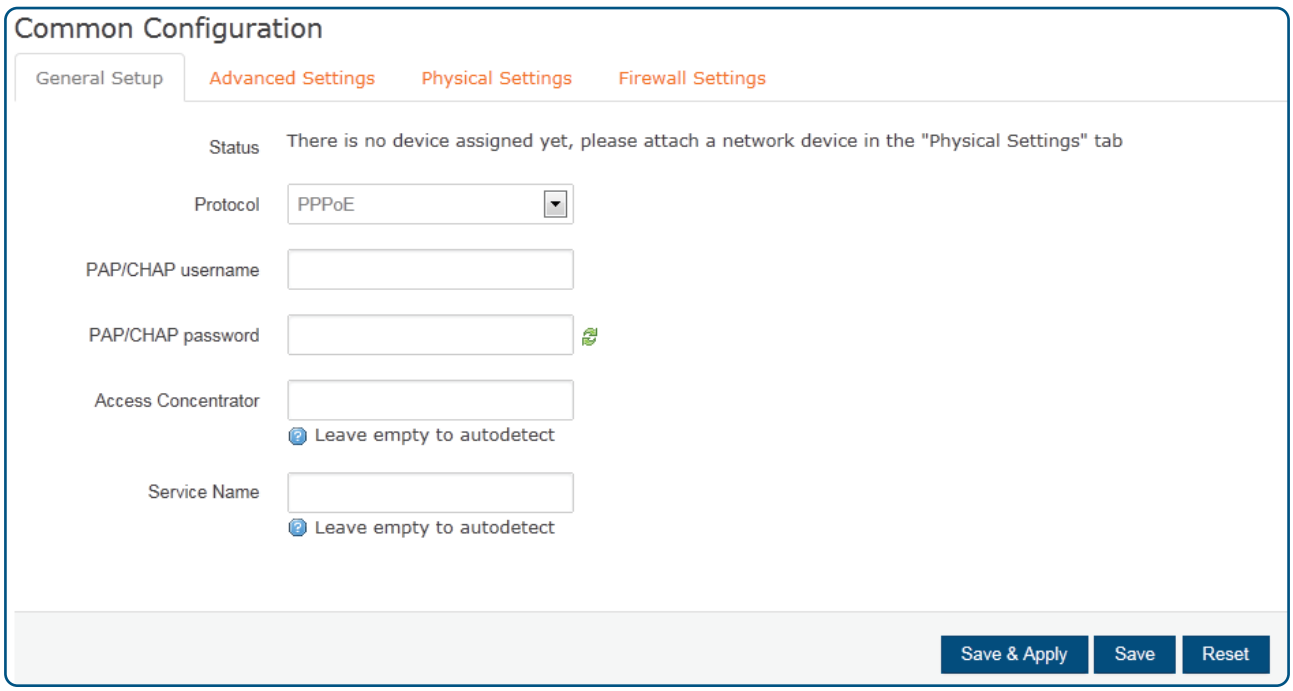
PPP

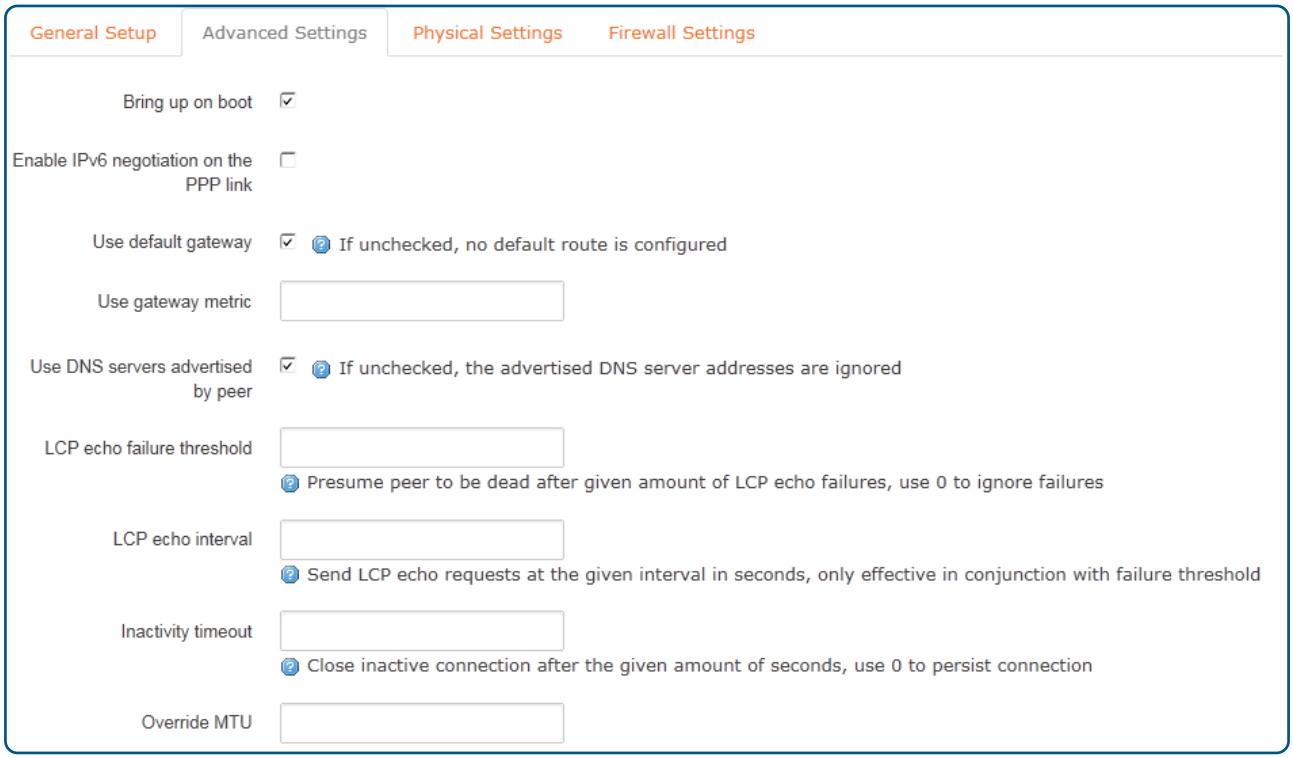
PPP (Point-to-Point Protocol) is a link-layer protocol. This link provides full-duplex operation and transfers data packets in order. It is designed primarily to establish a point-to-point connection in sending data via dial-up or leased line mode, making it a common solution. If PPP Internet mode is chosen, click the "Save & Apply" button.





PAP/CHAP username, PAP/CHAP password: enter your ISP username and password
Use Default Gateway: if unchecked, no default route is configured
Use gateway metric: for every gateway (e.g., router), the metric is increased by 1
Use DNS server advertised by peer: if unchecked, the advertised DNS server addresses are ignored
LCP echo failure threshold: Link Control Protocol (LCP) is a subset of the PPP agreement
LCP echo interval: send LCP echo requests at the given interval in seconds (only effective in conjunction with failure threshold)
Inactivity Timeout: close an inactive connection after a given number of seconds; use 0 for persistent connections
Override MTU: the default value is 1500
PPPoE: If "PPPoE" protocol is selected, click the "Save & Apply" button

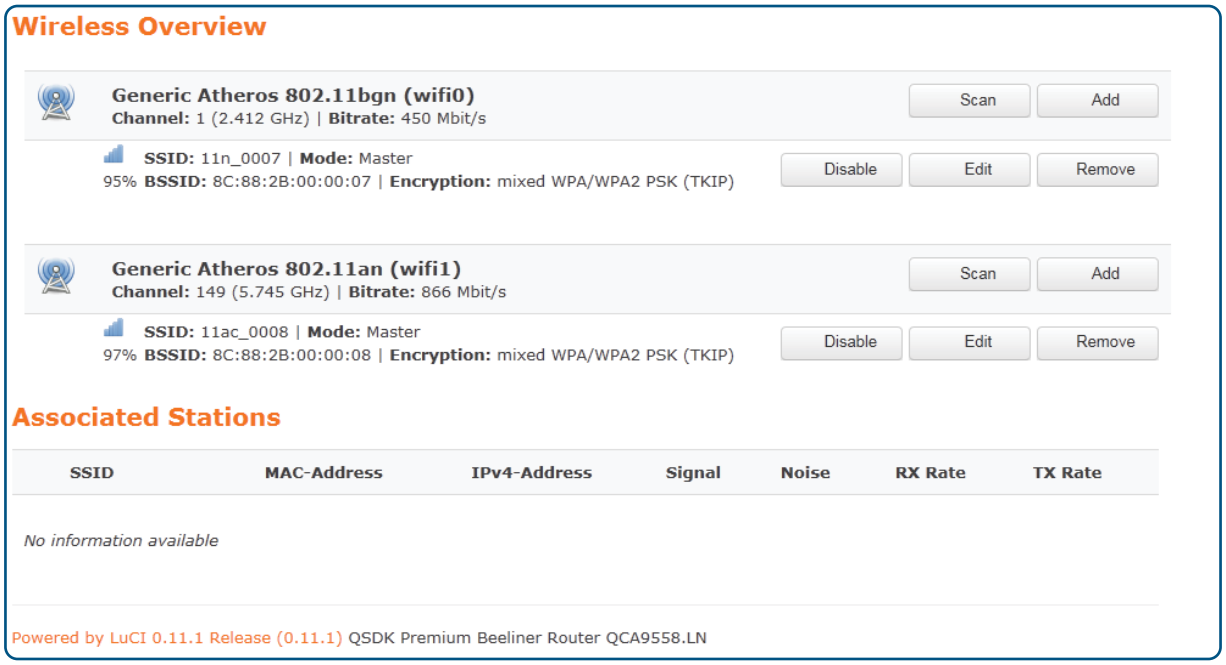




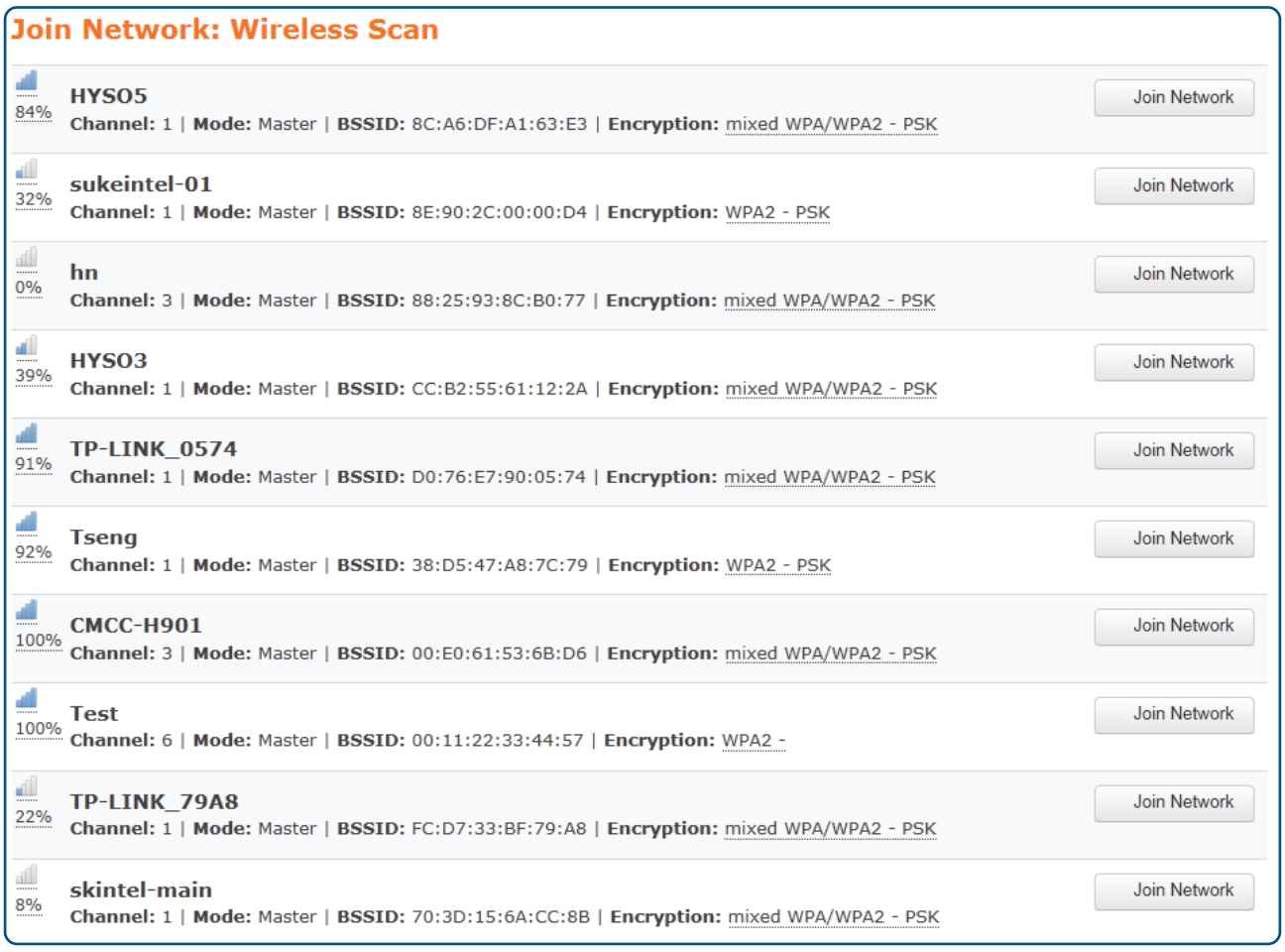
PAP/CHAP username, PAP/CHAP password: enter the ISP username and password
Access Concentrator: input connector center terminal, computer or communications device connection point device; leave empty to autodetect
Service Name: enter the name of the broadband connection; leave empty to autodetect
Use default gateway: check to use default gateway
Use gateway metric: for every gateway (e.g., router), the metric is increased by 1
Use DNS servers advertised by peer: check to use DNS server's address(es) advertised by peer
LCP echo failure threshold: Link Control Protocol (LCP) is a subset of the PPP agreement; after a specified number of LCP response failures assumed link is disconnected, 0 to ignore failure.
LCP echo interval: time to send LCP response(s), only when combined with effective fault threshold.
Inactivity timeout: timing of inactive link(s); enter 0 for persistent connections
Override MTU: the default is 1500

Wi-Fi

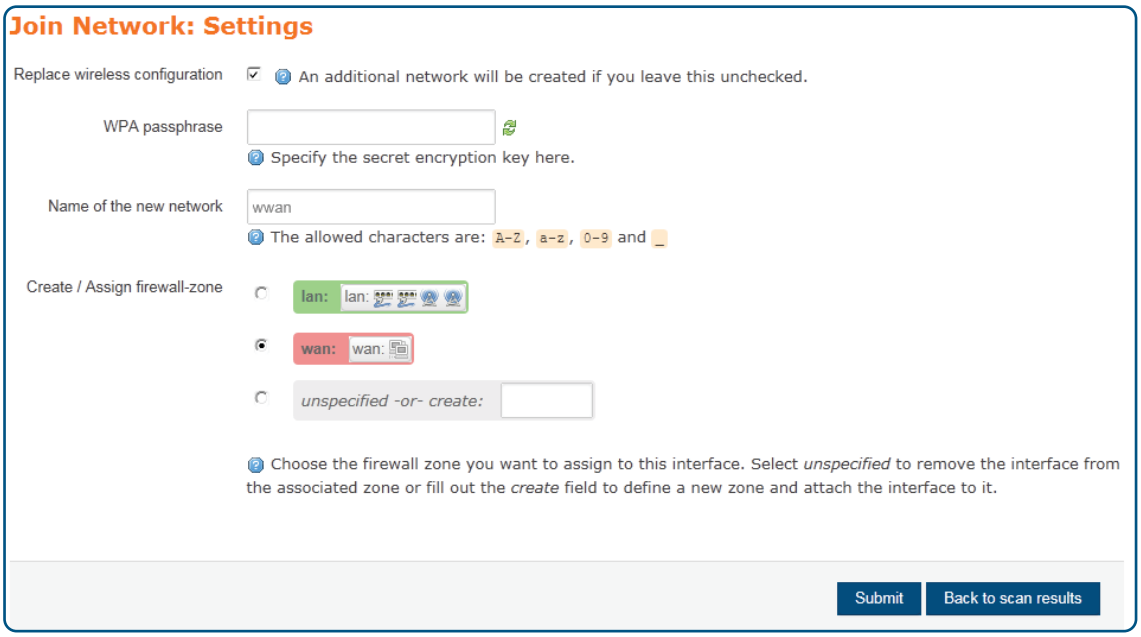
Click the "Network>Wifi" option for the following screen. The Router supports 2.4- and 5-GHz wireless signals, but its default is the 2.4 GHz band. Complete settings for the 5 GHz band if required in addition.



Click on the "Scan" button for the following interface. If a wireless router already exists in the environment, choose this function to connect the router to the original one via Wi-Fi.



For example, to join any of the wireless networks click, Join Network.



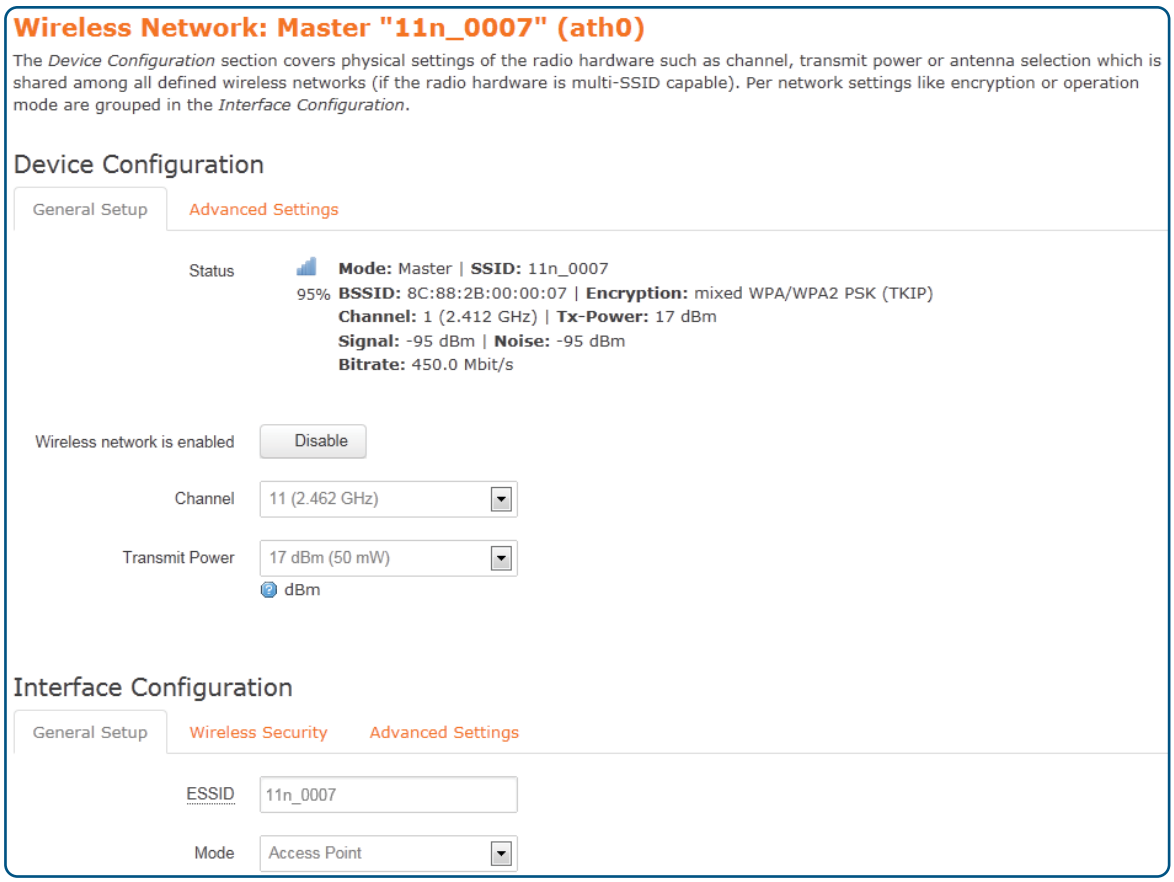
1 Fill in the WPA passphrase (the AP wireless password; the same of the new network).
2 Select "Create/Assign firewall-zone". You can select one or create one.
3 Click the Submit button.

Associated Stations

Once successfully connected, review the parameters of the connection, including the MAC address, IP address, signal, noise, transmission and receive rates and other information.

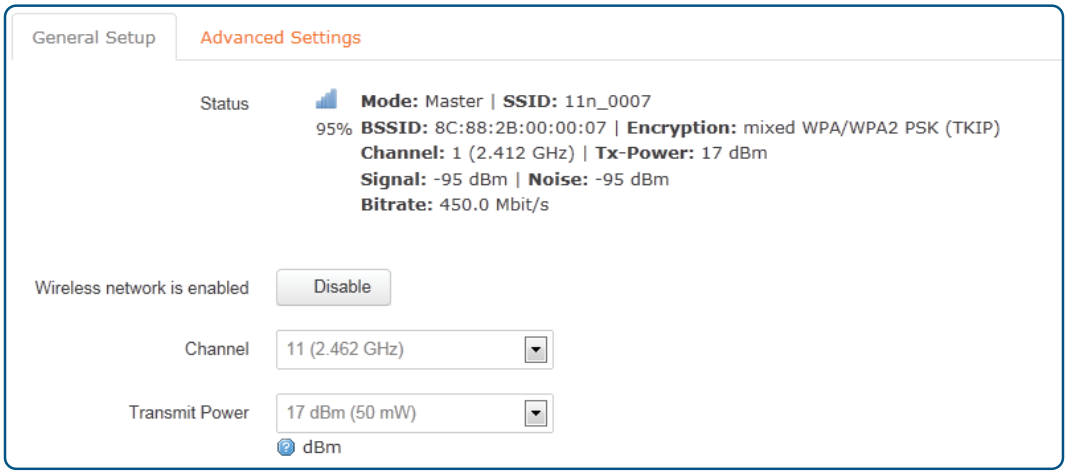
Network>Wifi>wifi0: Master "11n_0007"

Click the "Network>Wifi>wifi0: Master "11n_0007"" option, Device Configuration and Interface Configuration can be configured.



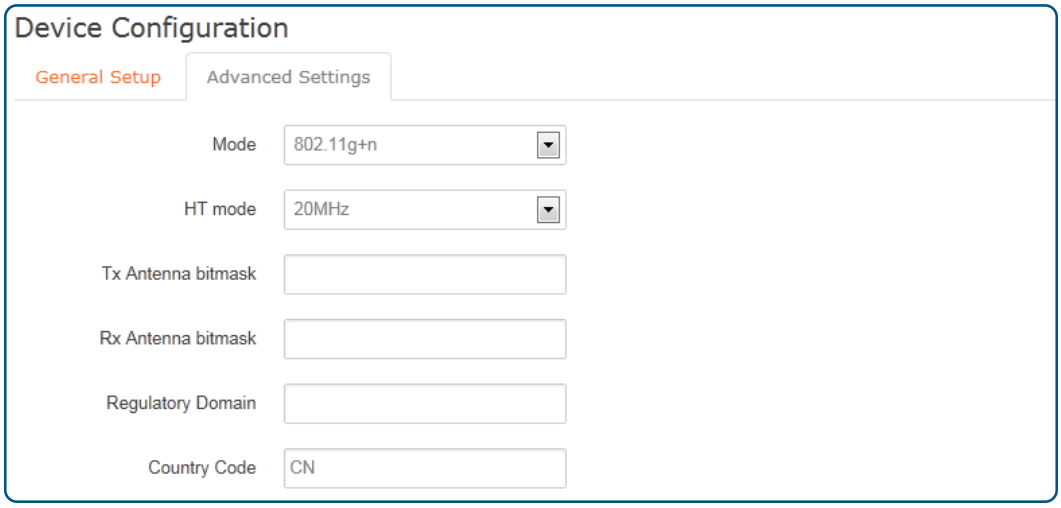
Device Configuration

Device Configuration is divided into General Setup and Advance Settings.
Click on the "General Setup" subpage for the following interface.



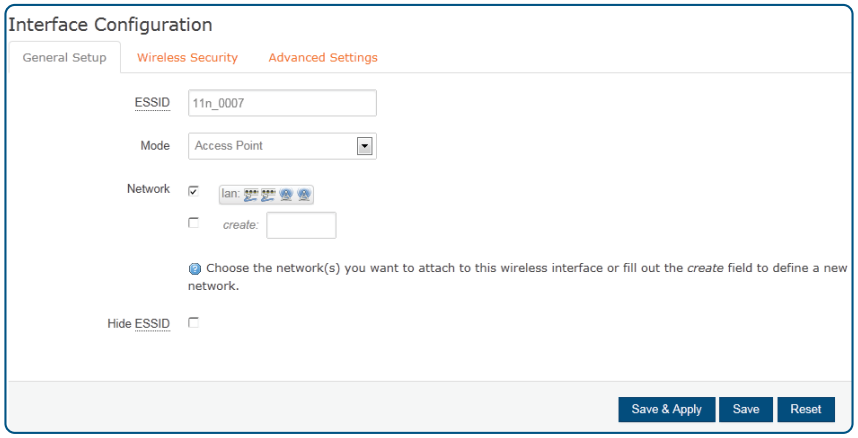
Channel: select from the range 1 to 13
Transmit Power: choose the appropriate power to meet network needs.

Click on the "Advanced Settings" subpage for the following interface.



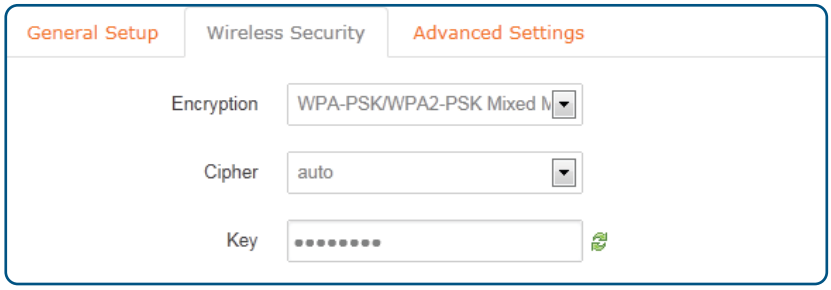
Mode: select "auto," "802.11b," "802.11g" or "802.11g+n" mode for the router
HT mode: "20MHz," "40MHz 2nd channel below," "40MHz 2nd channel above," "80MHz" modes
Country Code: select the desired country code from the drop-down list

Interface Configuration
Interface Configuration is divided into General Setup, Wireless Security and MAC-Filter subpages.
Click on the "General Setup" tab for the following interface:



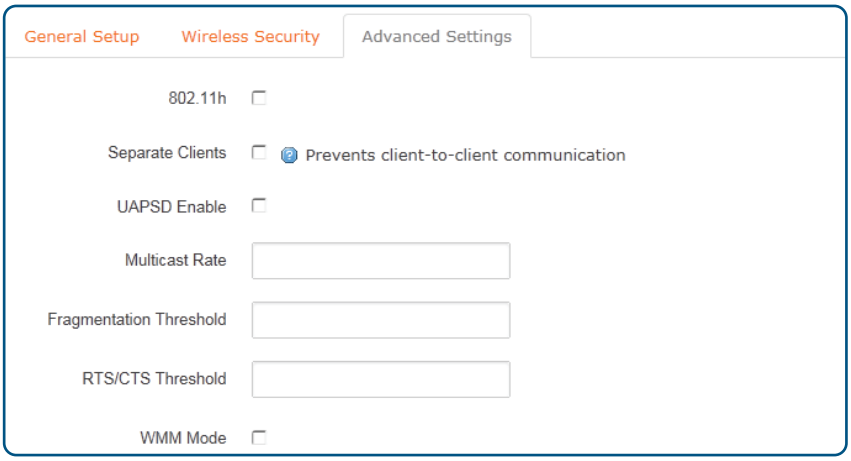
ESSID: create a second or subsequent
Mode: select the desired interface mode via the drop-down list
Network: choose the network(s) that are desired to be attached to this wireless interface or fill out the "create" field to define a new network
Hide ESSID: If checked, Wi-Fi devices can't search the SSID anymore (to connect the SSID must be input manually)

Click on the "Wireless Security" tab for the following interface:



Encryption: the router offers "WEP Open System/Shared Key," "WPA-PSK/WPA2
-PSK," "WPA-PSK/WPA2-PSK Mixed Mode" and other encryption types
Cipher: The router offers "auto," "Force CCMP(AES)," "Force TKIP," "Force TKIP and CCMP(AES)" options
Key: WEP (enter 5 or 10 characters); WPA/WPA2 (enter 8 or more characters; WPA/WPA2 mode is recommended)

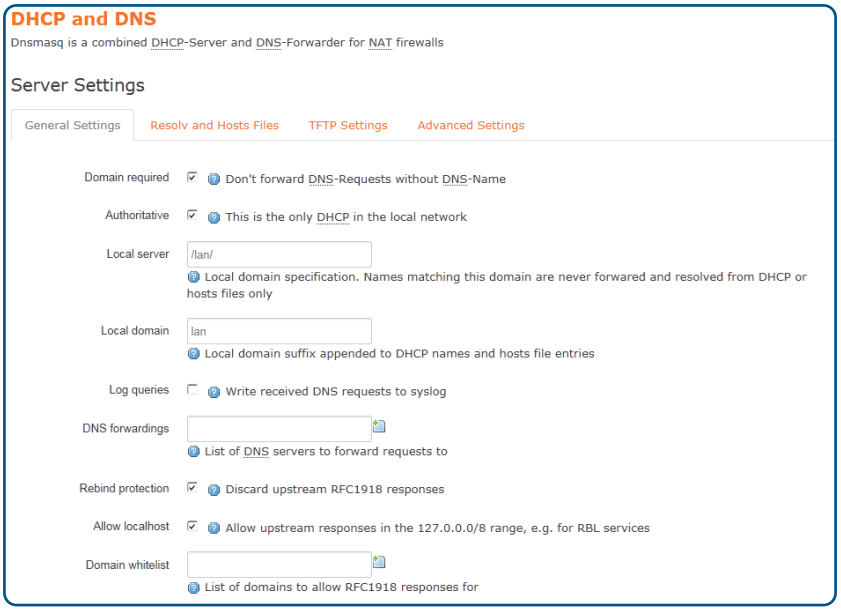
Click on the "Advanced Settings" tab for the following interface:



Separate Clients: prevent client-to-client communication
Fragmentation Threshold: the default value of 2346 should be left as-is unless you have a specific reason to modify
RTS/CTS Threshold: Request-To-Send (RTS) and Clear-To-Send (CTS); if the RTS threshold is exceeded once it is established, an RTS message is sent before data is transmitted to reduce interference; the corresponding CTS will respond after the RTS is received
WMM Mode: a sub-protocol of wireless transmission protocol; if enabled, only wireless devices
(mobile phones, laptops, etc.) with this function can connect to this router

DHCP and DNS

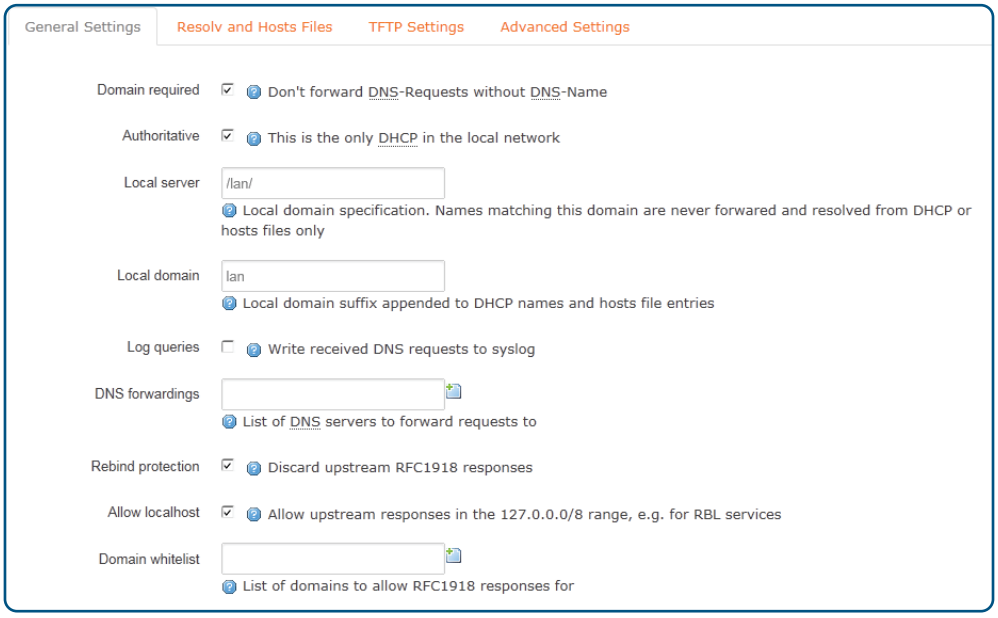
Click "Network>DHCP and DNS" for the following interface:



Server Settings

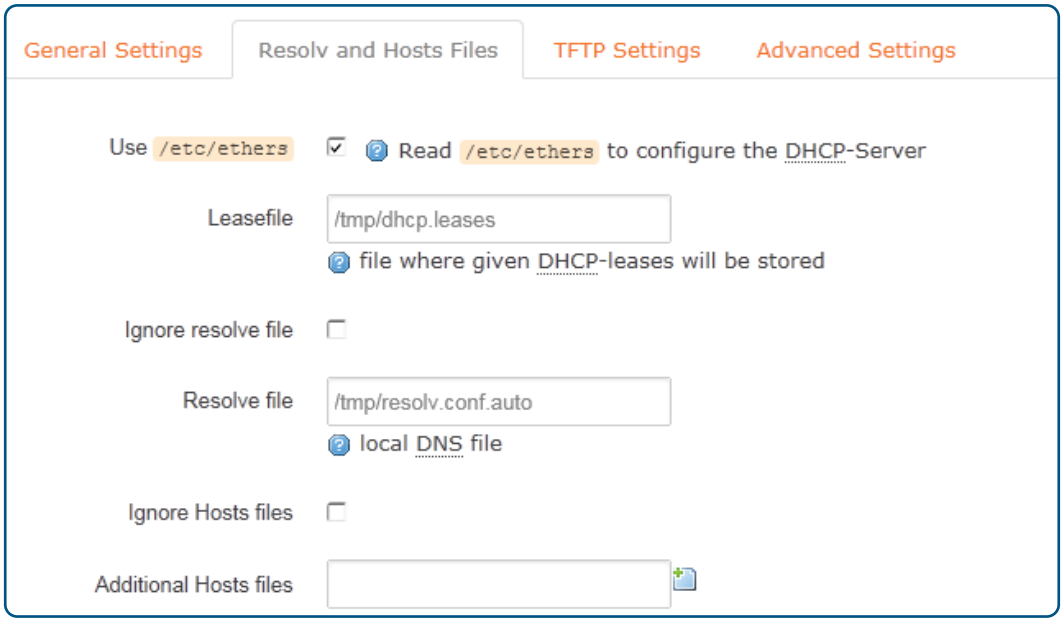
Dnsmasq for NAT firewall provides an integrated DHCP server and DNS forwarder.

Click on "General Settings" tab as shown below:



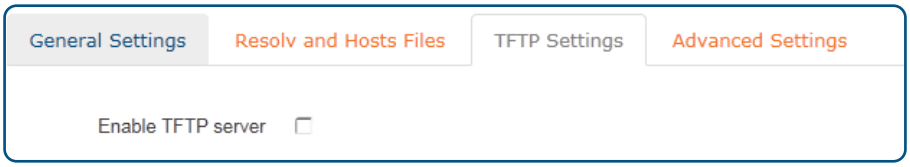
Domain required: don't forward DNS-Requests without DNS-Name
Authoritative: this DHCP is the only one in the local network
Local server: the local domain rule, never forwarded and processed, only resolved from the local DHCP or Host's file name data
Local domain: local domain suffix appended to DHCP names and hosts file entries
DNS forwardings: enter here any DNS servers to forward requests to
Rebind protection: discard upstream RFC 1918 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 RFC 1918 responses for

Click the "Resolv and Hosts Files" tab for the following interface:

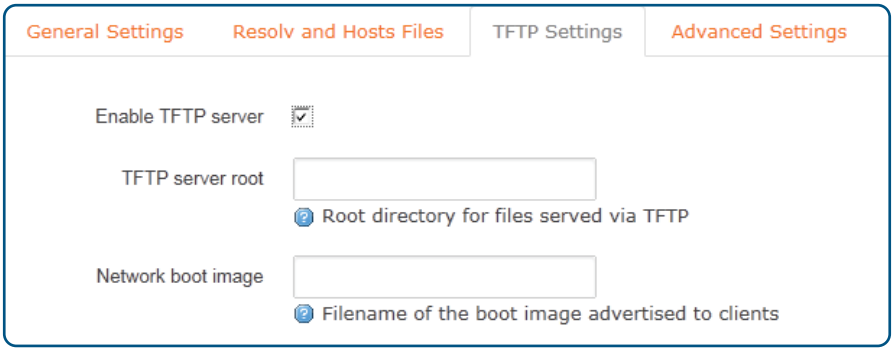


Use /etc/ethers: enable according to /etc/ethers to configure the DHCP-Server
Leasefile: file where given DHCP-leases will be stored
Ignore resolve file: if checked, feature is enabled
Resolve file: local file where DNS resolutions are stored
Ignore Hosts files: if checked, feature is enabled
Additional Hosts files: provide the name of files which will be ignored

Click the "TFTP Settings" tab for the following interface:

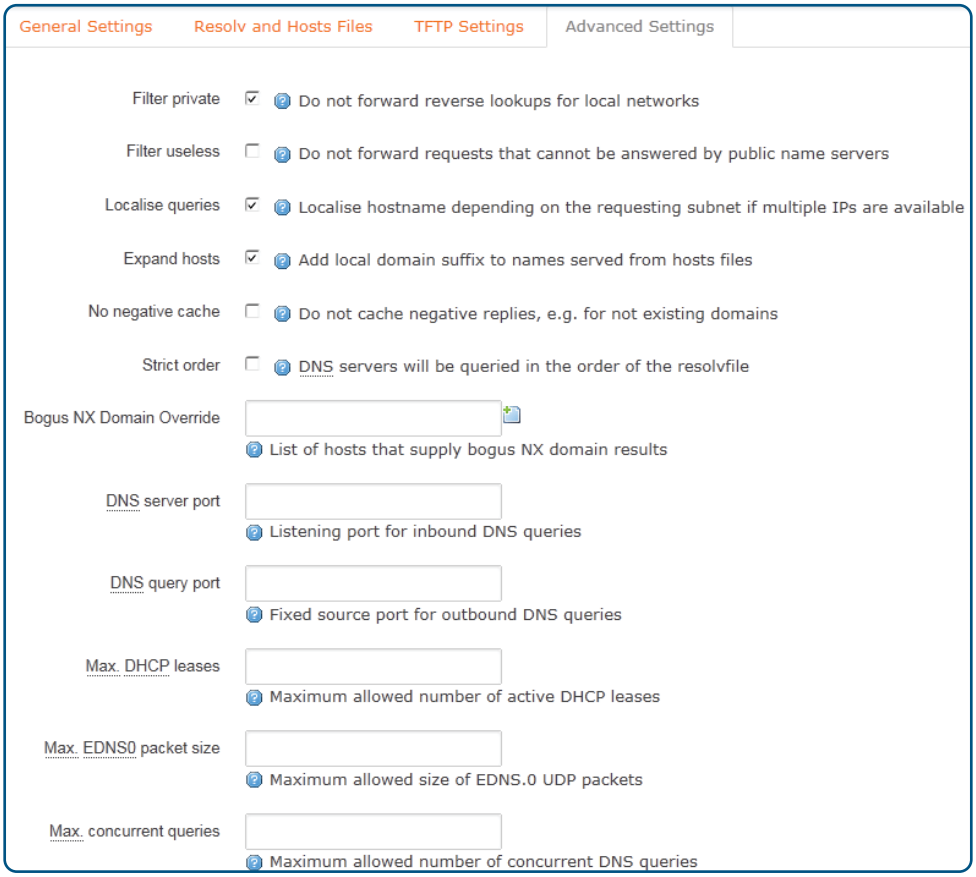


If "Enable TFTP server" is checked, the following interface appears:



TFTP server root: specify the root directory for files served via TFTP
Network boot image: filename of the boot image advertised to clients

Click on the "Advanced Settings" tab for the following interface:

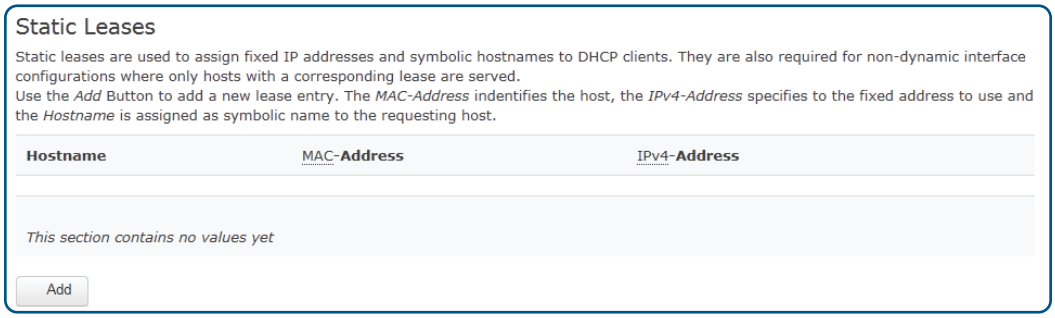


Filter private: do not forward reverse lookups for local networks
Filter useless: do not forward requests that cannot be answered by public name servers
Localization queries: localize hostname depending on the requesting subnet if multiple IPs are available
Expand hosts: add local domain suffix to names served from hosts files
No negative cache: do not cache negative replies (e.g., for not existent domains)
Strict order: DNS servers will be queried in the order of the resolvfile
Bogus NX Domain Override: list of hosts that supply bogus NX domain results
DNS server port: listening port for inbound DNS queries
DNS query port: fixed-source port for outbound DNS queries
Max. DHCP lease: maximum allowed number of active DHCP leases
Max. EDNS.0 packet size: maximum allowed size of EDNS.0 UDP packets
Max. concurrent queries: maximum allowed number of concurrent DNS queries

Active DHCP Leases

The Active DHCP Leases table lists the information for the connected device, including Host name, the IPv4 address, MAC address and the remaining lease time.

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 a symbolic name to the requesting host.

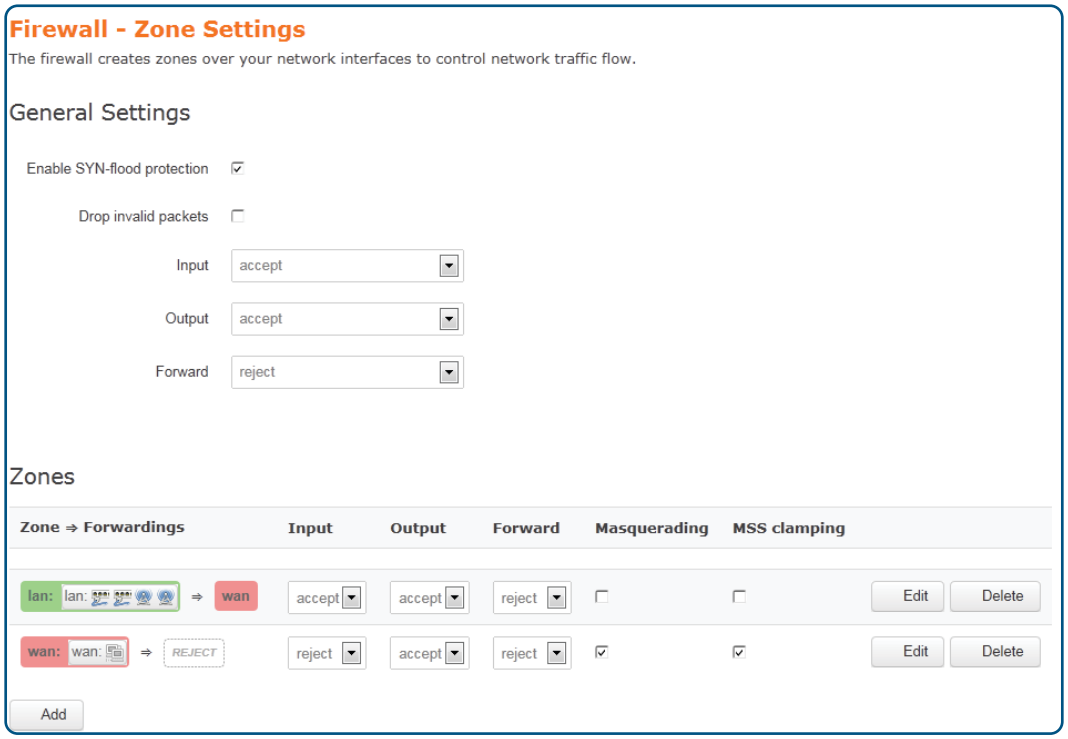


Firewall

Click on the "Network>Firewall" option to configure General Settings, Port Forwards, Traffic Rules and Custom Rules.

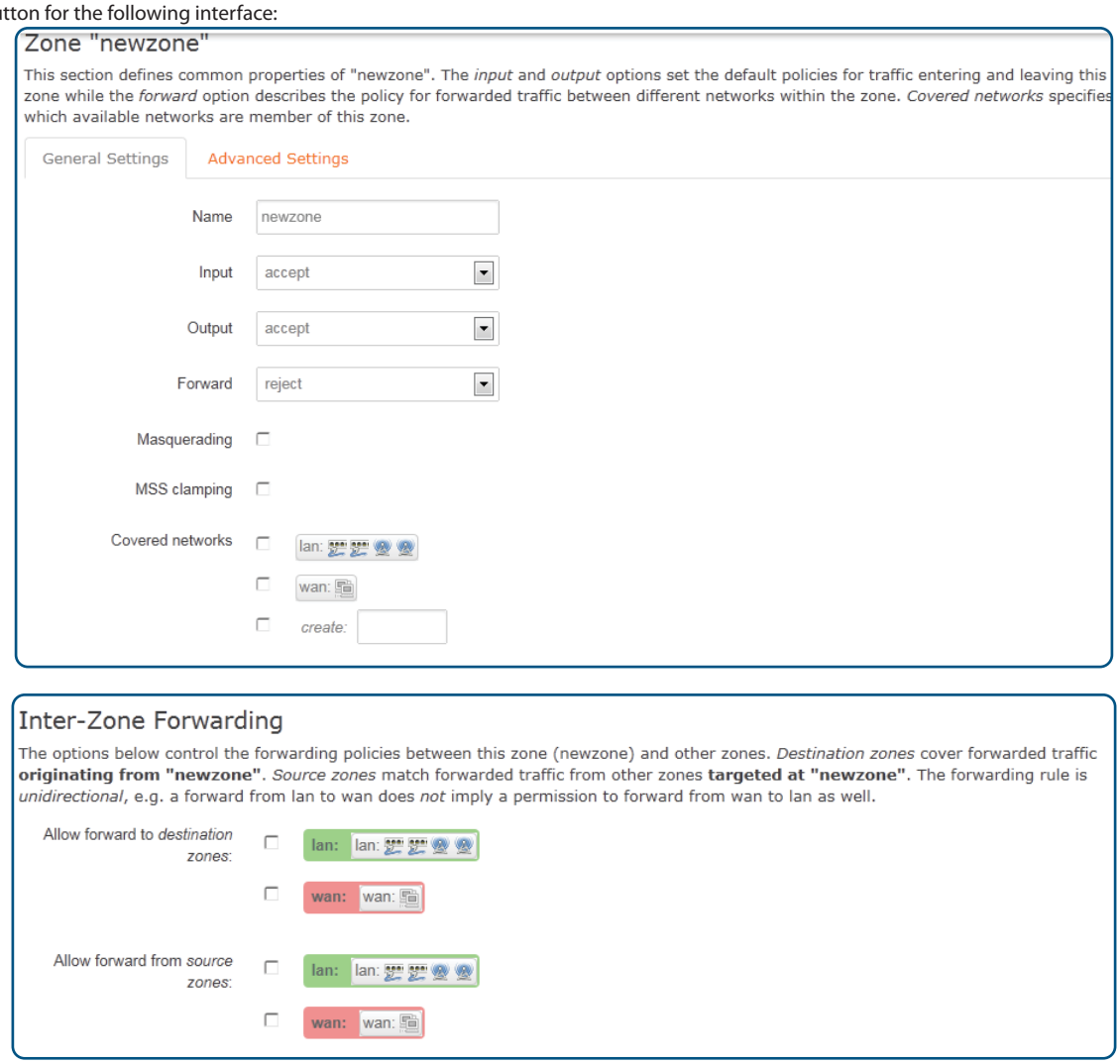
Network>Firewall>General Settings

Click on the "Network>Firewall>General Settings" option for the following interface:

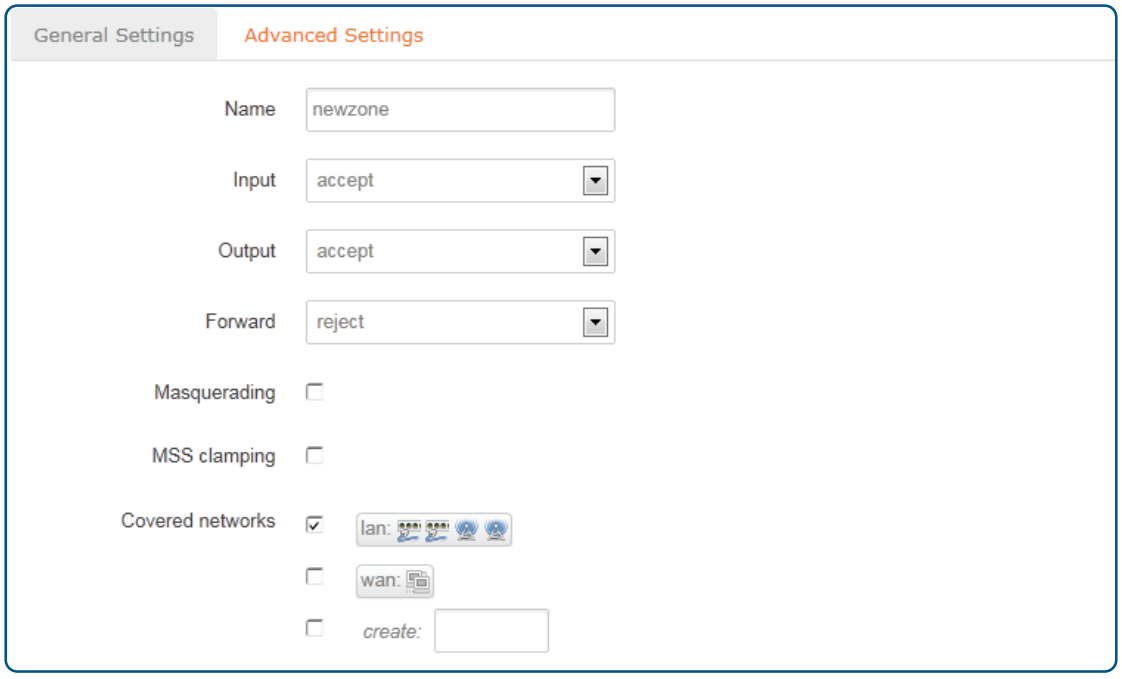


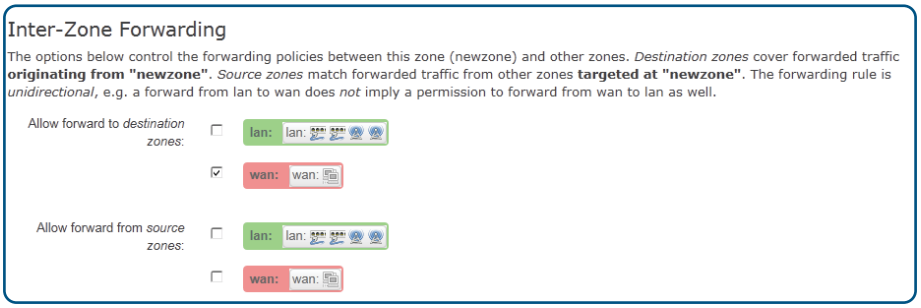
General Settings
Enable SYN-flood protection: SYN Flood is currently the most popular DoS (Denial of Service attack) with one of the DDoS (Distributed Denial of Service attack) approaches, which uses a TCP protocol flaw, sending a large number of forged TCP connection requests, thereby causing the attacker depletion of resources (CPU full load or insufficient memory) way to attack; enabling this option helps defend against some denial of service attacks
Drop invalid packets: if checked, invalid packets will be discarded
Input: the target object is data received from a remote device; options included — discarded (discards invalid data and does not respond to any feedback; customers waiting for a timeout will likely be blocked by a firewall); refused (to return [terminate] invalid data packets (TCP FIN or UDP-ICMP-PORT-UNREACHABLE), explicitly rejected the other's connection action); accept (receive effective inbound data)
Output: the target object is data transmitted from a local device
Forward: refers to specific (one or more) data packets between different subnets

Regional
Click the "Add" button for the following interface:



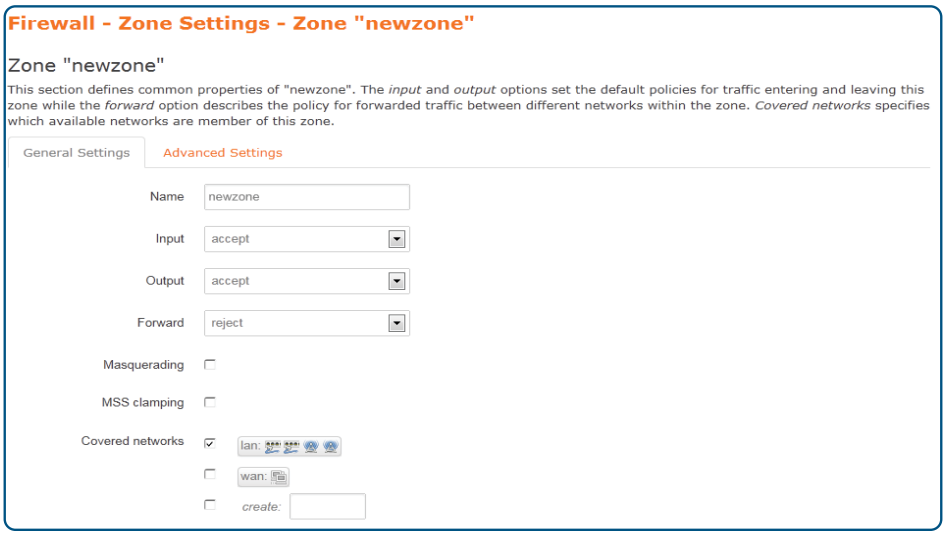
For example, to add "lan => wan," make the following settings:





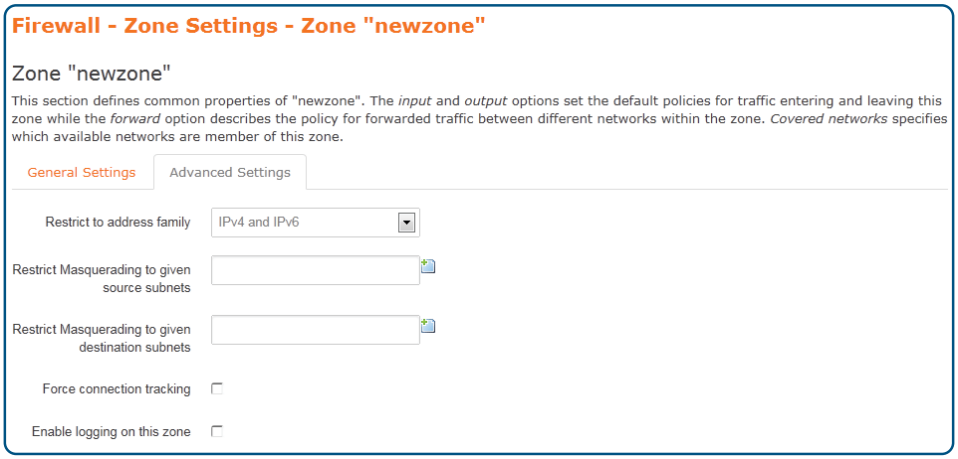
Regional "newzone"

General Settings



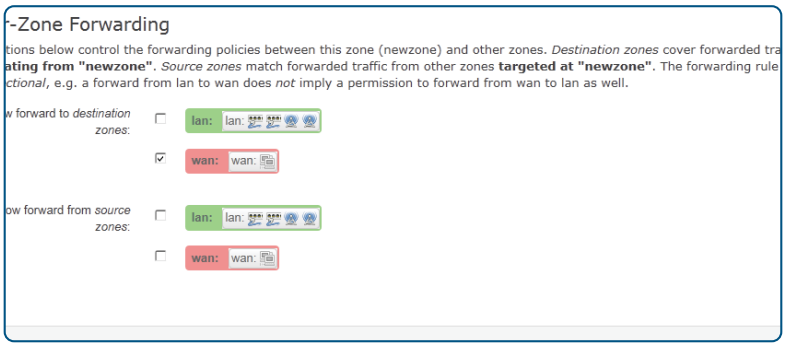
Name: lan; the zone or an area of your network
Input/Output: drop, reject, accept
Forward: refers to specific (one or more) data packets between different subnet
Masquerading: IP masquerading is a special kind of SNAT rule; when a computer within the network of computers accesses the external network through the router, it replaces the source address of IP packets to a predetermined address (usually the external network card address)
MSS clamping: MSS value that is the largest data segment for each TCP packet can be transmitted
Covered networks: select the network belonging to this region

Click the "Advanced Settings" tab for the following interface:



Restrict to address family: choose to limit the type of address
Restrict Masquerading to given source subnets: enter the IP address of your internal network
Restrict Masquerading to given destination subnets: enter the IP address of the firewall (usually outside the network card address)
Forced connection tracking: if checked, then the feature is enabled
Enable logging on this zone: if checked, then the feature is enabled

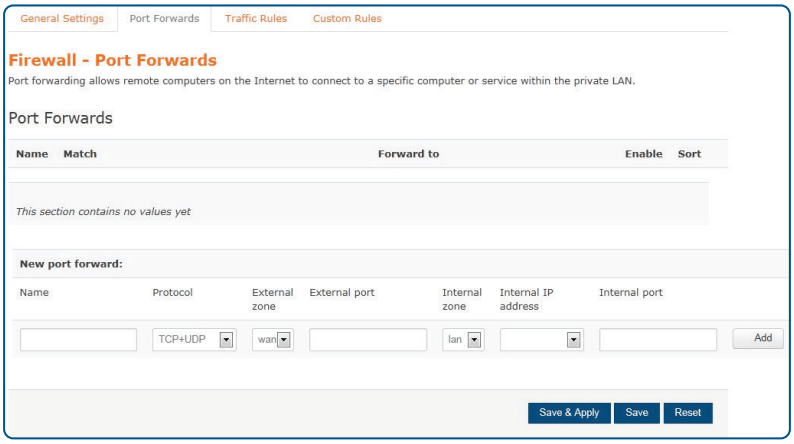
Inter-Zone Forwarding



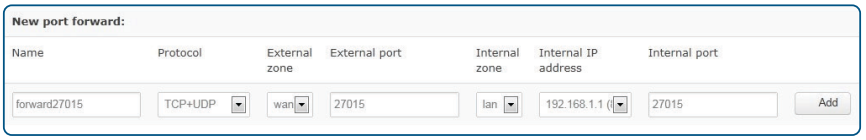
The figure above shows options for the control area (lan) and forwarding rules for other regions.
After the above are set, click the "Save & Apply" button to successfully add a firewall area.

Network>Firewall>Port Forwards

Click on the "Network>Firewall>Port Forwards" tab for the following interface:



This interface configures port-forwarding rules. Here you can forward an external network port to an internal network port.
Example: There are 50 computers in the network that have been configured to an FTP server; its IP address is 192.168.1.102. So that Internet users can also access this server, click the "Add" button and make the following configuration. After configuration is complete, click the "Save & Apply" button.



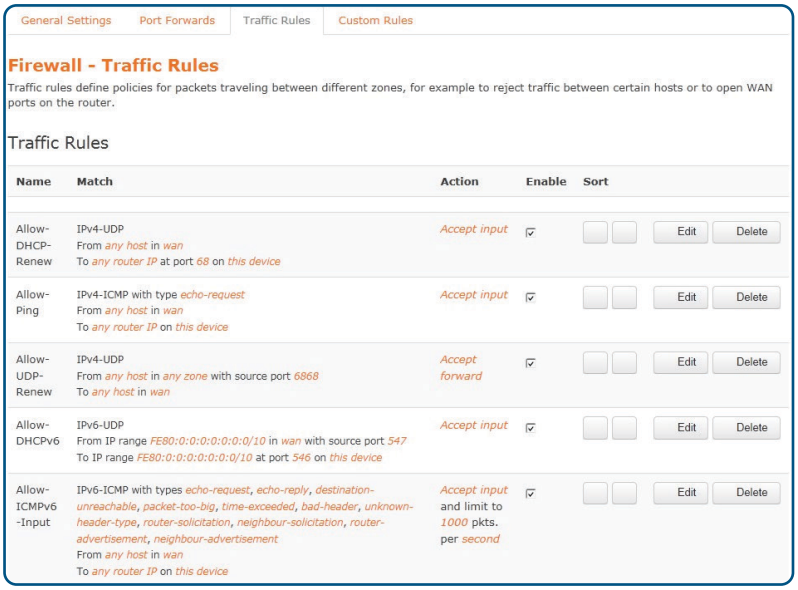
Name: enter an easy to remember name
Protocol: protocol provided by the server; if not clear what kind of agreement, choose "TCP+UDP" protocol; refer to the "common ports and services table"
External zone: WAN area
External port: specify opening ports mapping to the internal server provided ports; if not specified, the external port and internal port will be the same; fill in the range 1 – 65535.
Internal zone: internal LAN area
Internal IP address: IP address of the network server
Internal port: ports using by the network server to provide corresponding service; refer to the "Common Ports and Services Table"

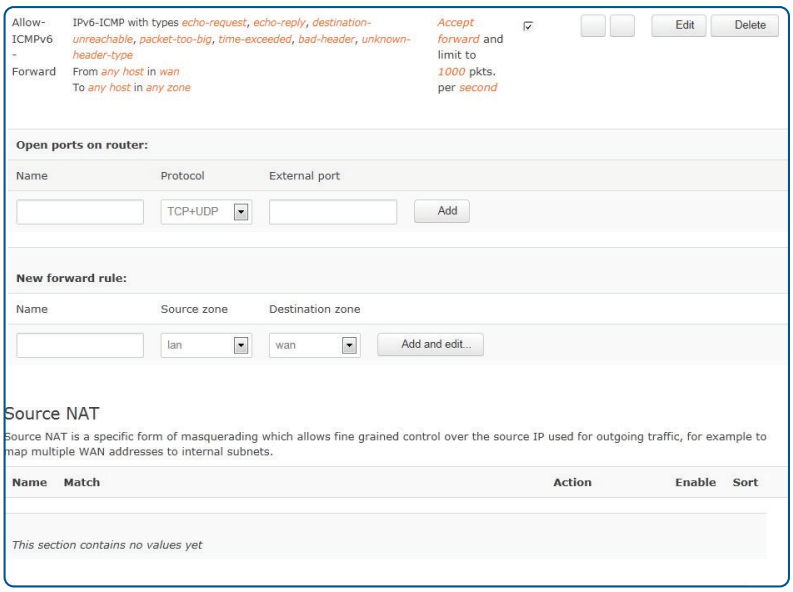
Common Ports and Services Table

Network Services	Agreement	Port
FTP	TCP	21
SSH	TCP	22
telnet	TCP	23
SMTP	TCP	25
Time	TCP	37
DNS	UDP	53
WWW	TCP	80
POP3	TCP	110
SNMP	UDP	161
CS server	TCP	27015

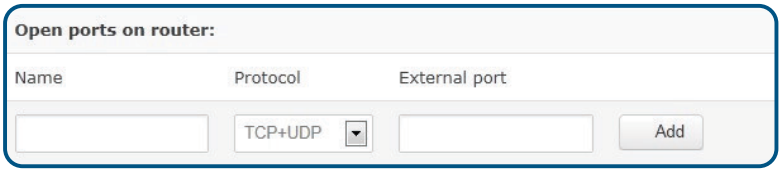
Network>Firewall>Traffic Rules

Click on the "Network>Firewall>Traffic Rules" tab for the following interface:

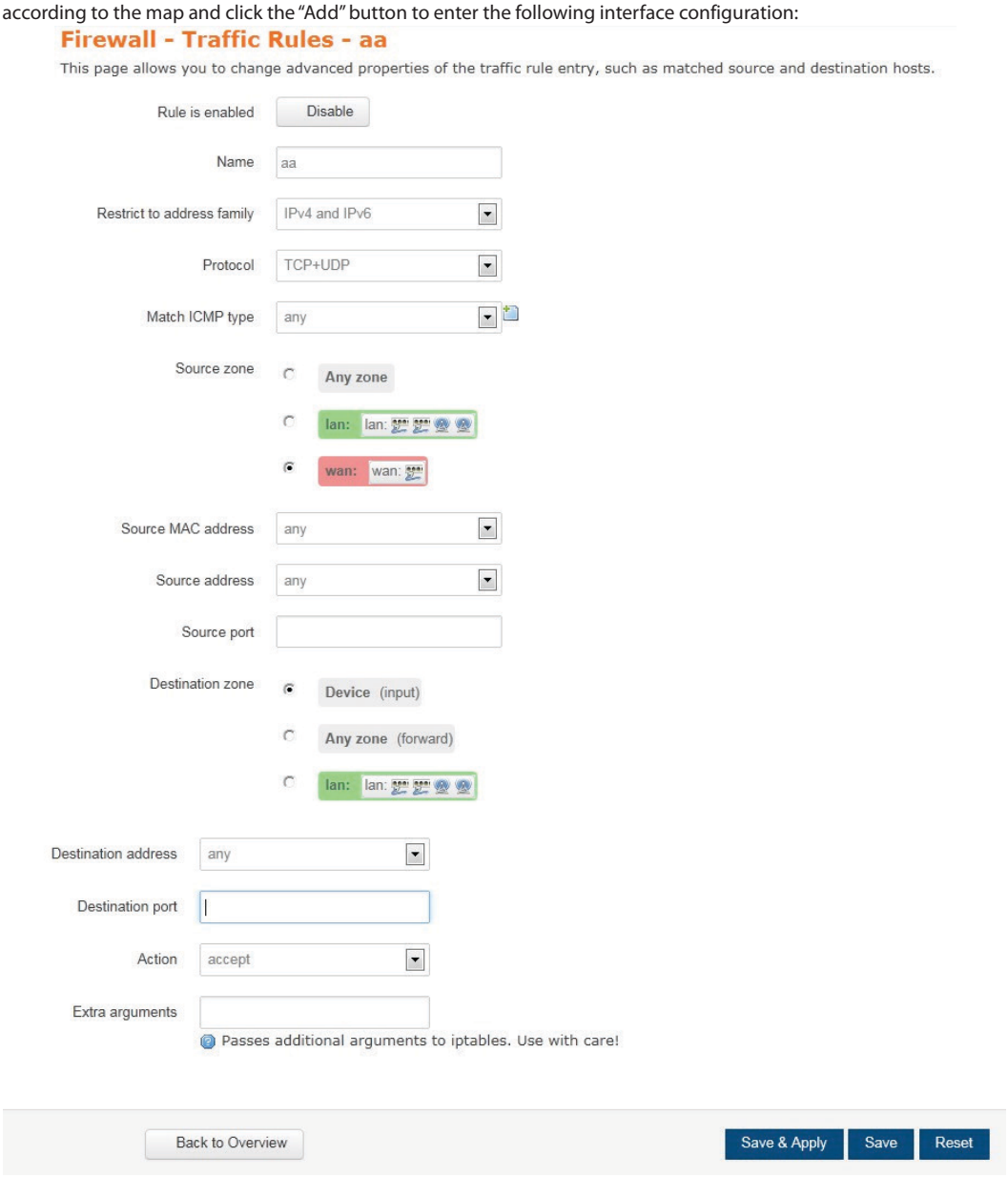




Communication rules define the traffic transmitted between different regions (e.g., items to reject traffic between certain hosts or items to open WAN ports on the router).
For example, to add the name of aa traffic rules, follow these steps to configure:



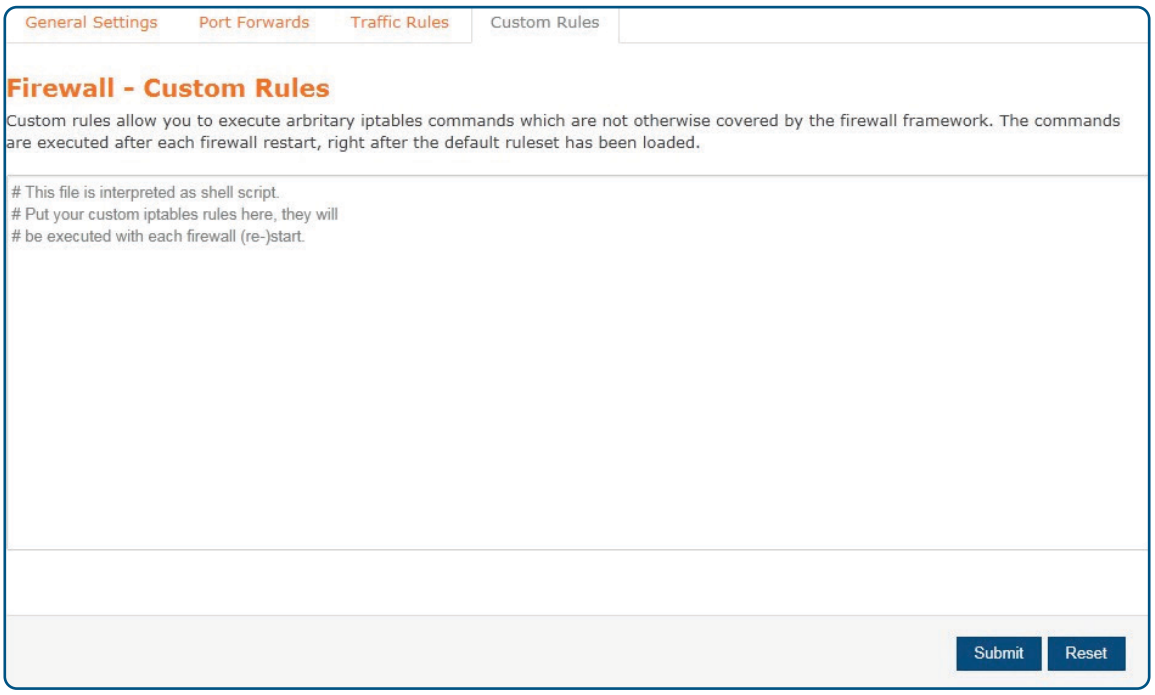
Fill in the information according to the map and click the "Add" button to enter the following interface configuration:



Name: add a name, such as aa
Restrict to address family: IPv4 and IPv6, only IPv4, only IPv6, any for you to choose, according to the traffic rules desired to implement
Protocol: select the protocol based on your intranet server
Match ICMP type: select the type of ICMP packet; if unsure of the type, choose "any"
Source zone: select lan, wan or all areas
Source MAC address: the source MAC address
Source address: customize the source IP address
Source Port: port of services provided by the source server used
Destination Zone: select lan, wan or all areas
Destination Address: customize the destination IP address here
Destination Port: enter the port services provided by the target server used
Action: choose discard, accept, reject, or no action
Extra arguments: additional parameters passed to iptables — be careful when using!

Network>Firewall>Custom Rules

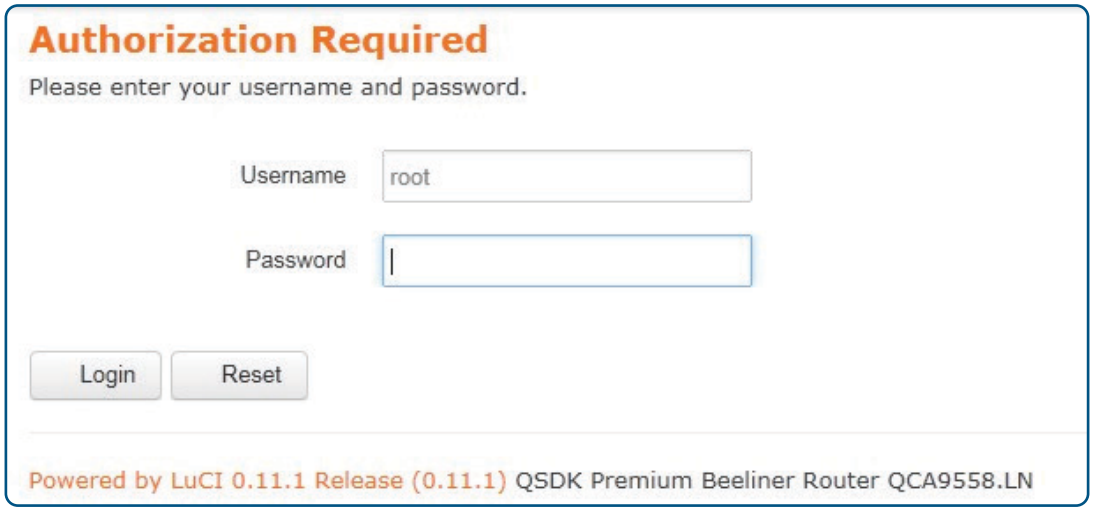
Click on the "Network>Firewall>Custom Rules" option for the following interface:



In this interface, define some functions not included in the firewall so that the router can provide additional protection.

Logout

Click the "Logout" button to return to the login screen.



Appendix: Technical Specifications

Hardware Specification		
CPU Frequency		775 MHz
RAM capacity		128 MB (DDR2)
ROM capacity		16 MB (SPI flash)
Standards and Protocols	Wireless	5 GHz: IEEE 802.11ac, IEEE 802.11n, IEEE 802.11a 2.4 GHz: IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
	Wired	IEEE802.3i, IEEE802.3u, IEEE802.3ab
Wi-Fi	Operating Frequency	2.4 GHz & 5 GHz
	Signal Rate	2.4 GHz: up to 450 Mbps 5 GHz: up to 867 Mbps
	Modulation	IEEE 802.11b: CCK, QPSK, BPSK IEEE11g/a: OFDM IEEE11n: QPSK, BPSK, 16-QAM, 64-QAM IEEE11ac: BPSK, QPSK, 16QAM, 64QAM, 256QAM
	Transmit Power	2.4 GHz: ≦ 24 dBm 5 GHz: ≦ 23 dBm
Interfaces		1 x 10/100/1000 Mbps WAN port (RJ45) 2 x 10/100/1000 Mbps LAN ports (RJ45) 1 x USB 2.0 Host port, 1 x power DC jack
Button		1 x reset
Antenna		3 x 2.4 GHz 3 dBi built-in FPC antennas 2 x 5 GHz 3 dBi built-in FPC antennas
Indicators		5G WLAN LED, Power LED, 2.4G WLAN LED
Power Supply		12 V / 1.5 A adapter or IEEE802.3at standard PoE
Dimensions (W x D x H)		180 X 180 X 25.5 mm
Environment		Operating temperature: 0 – 40°C Storage temperature: -40 – 70°C operating Humidity: 10 – 90% non-condensing Storage humidity: 5 – 90% non-condensing

Software Specification		
Practical function DDNS Wireless relay Quick Setup	**Network Settings** WAN connection types supported: PPPoE, DHCP, Static IP, PPtP, L2TP MAC Clone Diagnostics Static Router	**System configuration** Software upgrade Save & reload settings System log NTP server Language & Style
Security Settings WEB management Remote WEB management SSH access Telnet	**DHCP Settings** DHCP Server DHCP Client The client list Static IP	**Firewall** DMZ Port Forward Port/URL/MAC filter
Wireless basic function Wireless enable/disable WDS WPS Mutiple SSID	**Wireless Security** 64/128-bit WEP Encryption WPA/ WPA2, WPA-PSK/WPA2-PSKK	

Notes

Additional Information

WASTE ELECTRICAL & ELECTRONIC EQUIPMENT

DISPOSAL OF ELECTRIC AND ELECTRONIC EQUIPMENT

(Applicable In The European Union And Other European Countries With Separate Collection Systems)

ENGLISH: This symbol on the product or its packaging means that this product must not be treated as unsorted household waste. In accordance with EU Directive 2012/19/EU on Waste Electrical and Electronic Equipment (WEEE), this electrical product must be disposed of in accordance with the user's local regulations for electrical or electronic waste. Please dispose of this product by returning it to your local point of sale or recycling pickup point in your municipality.

DEUTSCH: Dieses auf dem Produkt oder der Verpackung angebrachte Symbol zeigt an, dass dieses Produkt nicht mit dem Hausmüll entsorgtwerden darf. In Übereinstimmung mit der Richtlinie 2012/19/EU des Europäischen Parlaments und des Rates über Elektro- und Elektronik-Altgeräte (WEEE) darf dieses Elektrogerät nicht im normalen Hausmüll oder dem Gelben Sack entsorgt werden. Wenn Sie dieses Produkt entsorgen möchten, bringen Sie es bitte zur Verkaufsstelle zurück oder zum Recycling-Sammelpunkt Ihrer Gemeinde.

ESPAÑOL: Este símbolo en el producto o su embalaje indica que el producto no debe tratarse como residuo doméstico. De conformidad con la Directiva 2012/19/EU de la UE sobre residuos de aparatos eléctricos y electrónicos (RAEE), este producto eléctrico no puede desecharse se con el resto de residuos no clasificados. Deshágase de este producto devolviéndolo a su punto de venta o a un punto de recolección municipal para su reciclaje.

FRANÇAIS: Ce symbole sur le produit ou son emballage signifie que ce produit ne doit pas être traité comme un déchet ménager. Conformément à la Directive 2012/19/EU sur les déchets d'équipements électriques et électroniques (DEEE), ce produit électrique ne doit en aucun cas être mis au rebut sous forme de déchet municipal non trié. Veuillez vous débarrasser de ce produit en le renvoyant à son point de vente ou au point de ramassage local dans votre municipalité, à des fins de recyclage.

POLSKI: Jeśli na produkcie lub jego opakowaniu umieszczono ten symbol, wówczas w czasie utylizacji nie wolno wyrzucać tego produktu wraz z odpadami komunalnymi. Zgodnie z Dyrektywą Nr 2012/19/EU w sprawie zużytego sprzętu elektrycznego i elektronicznego (WEEE), niniejszego produktu elektrycznego nie wolno usuwać jako nie posortowanego odpadu komunalnego. Prosimy o usuniecie niniejszego produktu poprzez jego zwrot do punktu zakupu lub oddanie do miejscowego komunalnego punktu zbiórki odpadów przeznaczonych do recyklingu.

ITALIANO: Questo simbolo sui prodotto o sulla relativa confezione indica che il prodotto non va trattato come un rifiuto domestico. In ottemperanza alla Direttiva UE 2012/19/EU sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE), questa prodotto elettrico non deve essere smaltito come rifiuto municipale misto. Si prega di smaltire il prodotto riportandolo al punto vendita o al punto di raccolta municipale locale per un opportuno riciclaggio.

WARRANTY INFORMATION • GARANTIEINFORMATIONEN • GARANTÍA • GARANTIE • GWARANCJI • GARANZIA

USA & CANADA: intellinetsolutions.us
EUROPA: intellinetnetwork.eu
DEUTSCHLAND: intellinetnetwork.de
ITALIA: intellinetnetwork.it

EN MÉXICO: intellinetsolutions.mx | Póliza de Garantía Intellinet — Datos del importador y responsable ante el consumidor IC Intracom México, S.A.P.I. de C.V. • Av. Interceptor Poniente # 73, Col. Parque Industrial La Joya, Cuautitlán Izcalli, Estado de México, C.P. 54730, México. • Tel. (55)1500-4500
La presente garantía cubre los siguientes productos contra cualquier defecto de fabricación en sus materiales y mano de obra.

- **A** Garantizamos los productos de limpieza, aire comprimido y consumibles, por 60 dias a partir de la fecha de entrega, o por el tiempo en que se agote totalmente su contenido por su propia función de uso, lo que suceda primero.
- **B** Garantizamos los productos con partes móviles por 3 años.
- **C** Garantizamos los demás productos por 5 años (productos sin partes móviles), bajo las siguientes condiciones:
  - **1** Todos los productos a que se refiere esta garantía, ampara su cambio físico, sin ningún cargo para el consumidor.
  - **2** El comercializador no tiene talleres de servicio, debido a que los productos que se garantizan

no cuentan con reparaciones, ni refacciones, ya que su garantía es de cambio físico.

3 La garantía cubre exclusivamente aquellas partes, equipos o sub-ensambles que hayan sido instaladas de fábrica y no incluye en ningún caso el equipo adicional o cualesquiera que hayan sido adicionados al mismo por el usuario o distribuidor.

Para hacer efectiva esta garantía bastará con presentar el producto al distribuidor en el domicilio donde fue adquirido o en el domicilio de IC Intracom México, S.A.P.I. de C.V., junto con los accesorios contenidos en su empaque, acompañado de su póliza debidamente llenada y sellada por la casa vendedora (indispensable el sello y fecha de compra) donde lo adquirió, o bien, la factura o ticket de compra original donde se mencione claramente el modelo, número de serie (cuando aplique) y fecha de adquisición. Esta garantía no es válida en los siguientes casos: Si el producto se hubiese utilizado en condiciones distintas a las normales; si el producto no ha sido operado conforme a los instructivos de uso; o si el producto ha sido alterado o tratado de ser reparado por el consumidor o terceras personas.

REGULATORY STATEMENTS

FCC Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of Federal Communications Commission (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 or more of the following measures: reorient or relocate the receiving antenna; increase the separation between the equipment and the receiver; connect the equipment to an outlet on a circuit different from the receiver; or consult the dealer or an experienced radio/TV technician for help.

CE

ENGLISH: This device complies with the requirements of CE RED 2014/53/EU, 2014/30/EU and/or 2014/35/EU. The Declaration of Conformity for is available at:
DEUTSCH: Dieses Gerät enspricht der CE RED 2014/53/EU, 2014/30/EU und / oder 2014/35/EU. Die Konformitätserklärung für dieses Produkt finden Sie unter:
ESPAÑOL: Este dispositivo cumple con los requerimientos de CE RED 2014/53/EU, 2014/30/EU y / o 2014/35/EU. La declaración de conformidad esta disponible en:
FRANÇAIS: Cet appareil satisfait aux exigences de CE RED 2014/53/EU, 2014/30/EU et / ou 2014/35/EU. La Déclaration de Conformité est disponible à :
POLSKI: Urządzenie spełnia wymagania CE RED 2014/53/EU, 2014/30/EU I / lub 2014/35/EU. Deklaracja zgodności dostępna jest na stronie internetowej producenta:
ITALIANO: Questo dispositivo è conforme alla CE RED 2014/53/EU, 2014/30/EU e / o 2014/35/EU. La dichiarazione di conformità è disponibile al:

intellinetnetwork.com

North America	Asia & Africa	Europe
IC Intracom America 550 Commerce Blvd. Oldsmar, FL 34677, USA	IC Intracom Asia 4-F, No. 77, Sec. 1, Xintai 5th Rd. Xizhi Dist., New Taipei City 221, Taiwan	IC Intracom Europe Löhbacher Str. 7, D-58553 Halver, Germany

intellinetnetwork.com

INT_525831_UM_1219_REV_5.01