Henrich HWRD Series Access Point

Web-based Configuration Guide

Henrich Electronics Corporation

Contents

Copyright

Henrich Electronics Corporation
225 Deming Place Westmont, IL 60559 United States
Website: http://www.henrich-inc.com/
Tel: (860)-487-9869
Fax: (860)-487-9478
Email: don@henrich-inc.com

Chapter 1: Overview

1.1. Introduction

This user manual is a guide to the *HenrichWRT* firmware on a wireless router. *HenrichWRT* combines *OpenWRT* with the most advanced *Qualcomm Atheros 10.1.x* wireless drivers. *HenrichWRT* also includes a user-friendly *LuCI* web interface for configuring the router.

OpenWRT is an extensible *GNU/Linux* distribution for embedded devices. It is built from the ground up to be a full-featured, easily modifiable operating system. It is powered by a *Linux* kernel that's more recent than most other distributions. The latest stable version of *OpenWRT, 12.09 Attitude Adjustment*, is used in *HenrichWRT.*

LuCI is a free, clean, extensible and easily maintainable web user interface for embedded devices. It has high performance, small installation size, fast runtimes, and good maintainability.

The content of this guide is organized the same way as presented on the router's web page. After the *Login* and *Language* sections, the following sections correspond to the top-level tabs: *Status, System, Services,* and *Network*. The last section contains the Final Notes which include troubleshooting information.

1.2. Language

To change the language, please navigate to the *System* page, look for the *System Properties* section, click the *Language* and *Style* tab, and click the dropdown list for *Language*. You can change the language from *English* to another language e.g. Chinese ( ).

1.3. Supported Products

The HenrichWRT software resides in the following models of routers: the HWRD Series, the HWRD-300 Series, the HWRD-400 Series, and the HWRD-600 Series.

1.4. System Requirements

Operating System: Microsoft Windows XP, Windows Vista, Windows 7, Windows 8, Linux, or Mac OS X.

Web Browser: Mozilla Firefox, Google Chrome, Apple Safari, or Microsoft Internet Explorer 8 or above.

1.5. Getting Started

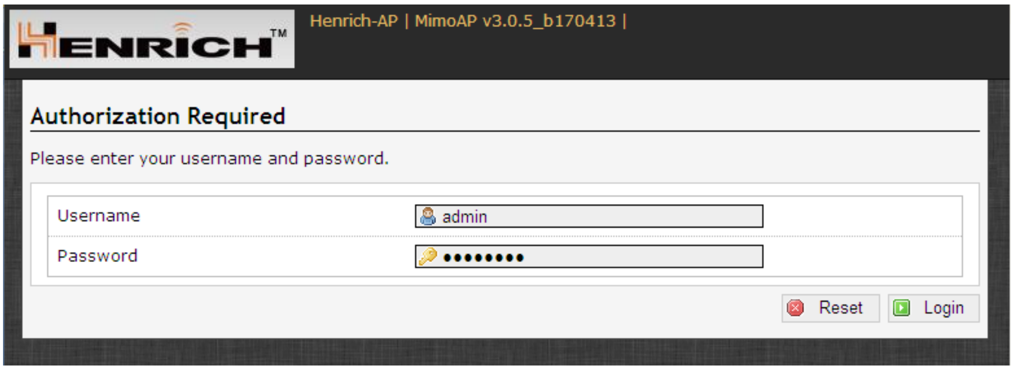
To access the HenrichWRT configuration interface, perform the following steps:

1. Connect the local area network (LAN) port of the router to the network port of your computer using an Ethernet cable. Ethernet cables are also known as LAN cables or

network cables. They connect devices such as computers, routers, and switches on wired networks.

2. Next, take the power adapter that comes with the set and connect it to a power socket as well as the router. Turn on the power.
3. Assign the Ethernet adapter on your computer with a static IP address on the 192.168.1.x network, e.g. 192.168.1.10 and with a subnet mask 255.255.255.0.
4. Launch a web browser and enter the default IP address of the router, 192.168.1.1, into the address bar. The router's configuration web page should be presented.

The first page that you see is the login page. The words on the top left denote the firmware build version e.g. MimoAP v3.0.5_b170413.



Henrich-AP | MimoAP v3.0.5_b170413 |

Authorization Required

Please enter your username and password.

Username	admin
Password	••••••••

Figure 1: The login page is presented upon requesting the router's IP address.

The default authorization details are:

Username: admin

Password: password

Advanced information: There is a 'root' user in the AP's Linux shell. It cannot be used to login to the AP's web page. You may wish to use the Access Point Controller (APc) to change the password of the 'root' user to a password of your choice. Following that, you can access the AP's Linux shell by using a serial cable or by SSH. The PuTTY software can be used for either method. The Henrich APc software is offered free of charge.

1.6. Operating Modes

The router can operate in the following modes:

1. Access Point / Master.
2. Station / Client.
3. Access Point WDS.
4. Station WDS.

A wide area network (WAN) is a network that covers a broad area. The world's most popular WAN is the Internet.

In a commonly used setup, the WAN port of an access point connects to a modem via an Ethernet cable. A modem can be a cable, digital subscriber line (DSL), or fiber optic modem. A modem translates the signal from the internet service provider (ISP) to Ethernet signals that the access point can understand. This allows the access point to have internet connection.

Other devices called stations connect wirelessly to this access point. These devices can be mobile phones, printers, IP cameras, laptops, or even other routers. The stations obtain internet connection from the access point.

An access point WDS and a station WDS together extend the wireless coverage, like a repeater. More information on the setup can be found on other page .

1.7. Buttons and Changes

The buttons are described here.

Reset: Undo the changes.

Save: Saves the changes. Currently please do not use this button.

Save & Apply: Saves and applies the changes. Please use this button instead of the 'Save' button so that the changes would be applied immediately. It is recommended to click this button before moving to a different page.

Logout: Logs out of the router's web page.

Changes: 0: Means that all changes on the configuration web page have been applied to the router.

Unsaved Changes: Shows the number of changes that have not yet been *Save & Apply.*

1.8. Reset Button

The reset button is a physical hardware button on the board. Please refer to Section 3.5 Reset Button.

1.9. LEDs

The light emitting diodes (LEDs) on the board are described in Section 3.6 *LEDs* on the *Board.*

1.10. Buzzer

New Series boards may have a buzzer. The buzzer makes the following sounds:

- Power up: Beep once.
- End of Firmware Loading: Beep twice.
- Alignment: Beep according to signal thresholds defined. The alignment buzzer is described in Section 2.1.9 *Link Status (for Station Mode)*.

1.11. Serial Console

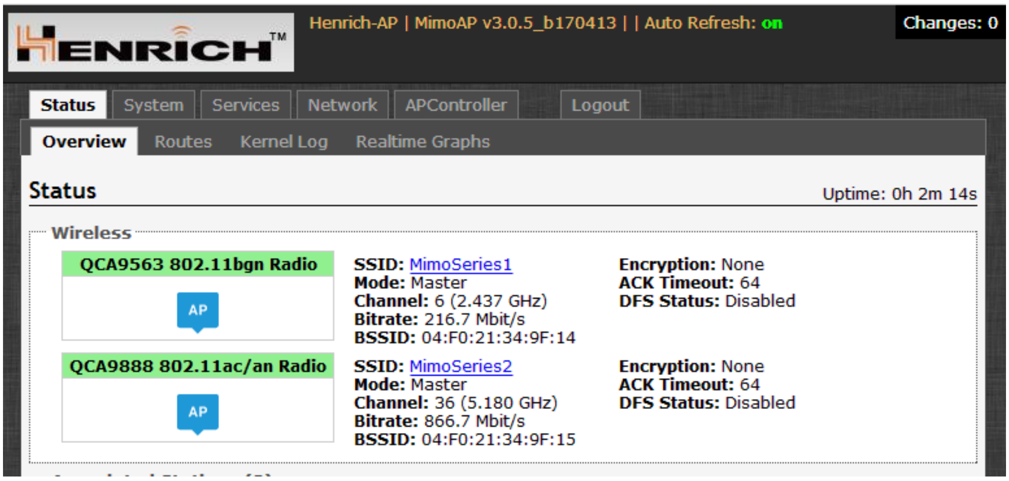
A serial console makes it easy to flash the firmware and to debug potential problems. A serial adapter may be purchased from Henrich. It plugs into a row of 4 pins on the board. More information can be found in the document of HenrichWRT Firmware Upgrade.

1.12. Modifying the HenrichWRT Source Codes

With the proper tools, the HenrichWRT source codes can be modified. The router functions and the configuration webpage can be redesigned. More information can be found in the document of HenrichWRT Build Instructions and FAQ.

Chapter 2: Status Tab

After login, when you click on the *Status* top-level tab, you can see the second-level tabs of *Overview, Routes, System Log, Kernel Log*, and *Realtime Graphs*. This is shown in Figure 2.



Henrich-AP | MimoAP v3.0.5_b170413 | | Auto Refresh: on

Changes: 0

Status

Uptime: 0h 2m 14s

Wireless

QCA9563 802.11bgn Radio

SSID: MimoSeries1
Mode: Master
Channel: 6 (2.437 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

QCA9888 802.11ac/an Radio

SSID: MimoSeries2
Mode: Master
Channel: 36 (5.180 GHz)
Bitrate: 866.7 Mbit/s
BSSID: 04:F0:21:34:9F:15

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Figure 2: The *Status* → *Overview* page

Notice in the figure that the radio is using the latest and fastest 11ac wireless standard that supports a data rate of up to 1300Mbit/s.

2.1 Overview

The *Status* → *Overview* page is divided into the sections *Wireless, Associated Stations, System, Memory, Network,* and *DHCP Leases*.

Uptime: Displays the duration of time since the router was turned on or rebooted.

2.1.1 Wireless

The wireless chipset model is shown in the little box on the left e.g. QCA9882 802.11ac/an Radio. This box can be removed for OEM customers.

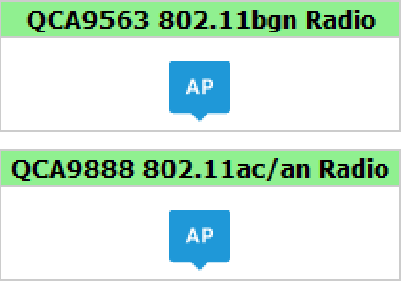
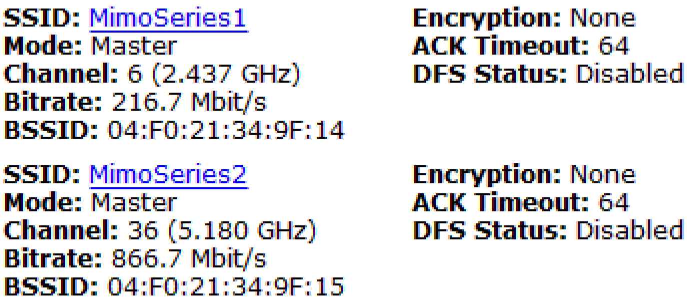


Figure 3: Wireless chipset model

The word *AP* in the small callout box means that the radio is operating in the Access Point (AP) mode. If the word is *CPE*, it means that the radio is operating as a customer-premises equipment (CPE) i.e. a station. The word X is shown if the radio is disabled.

2.1.2 Wireless (for AP Mode)

The *Wireless* section in the *Status* → *Overview* page shows a summary of the wireless parameters. The following describes the parameters when the device is in the *AP* mode.



SSID: MimoSeries1
Mode: Master
Channel: 6 (2.437 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

SSID: MimoSeries2
Mode: Master
Channel: 36 (5.180 GHz)
Bitrate: 866.7 Mbit/s
BSSID: 04:F0:21:34:9F:15

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Figure 4: A summary in the *Wireless* section for a device operating as an 802.11 access point

SSID: Displays the name of the wireless network that this access point (AP) is offering, the Service Set Identifier (SSID).

Mode: This is *'Master'* if the device is in AP mode or AP WDS mode.

Channel: Shows the channel number and frequency that this AP is using.

Bitrate: This is the maximum bitrate supported by the radio in the current configuration.

BSSID: This is the MAC address of the AP's radio.

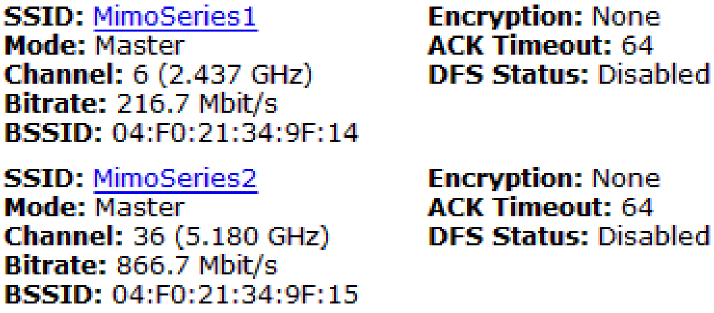
Encryption: Displays the wireless encryption used.

ACK Timeout: Shows the maximum acknowledgment time in microseconds.

DFS Status: If DFS is enabled, the AP automatically switches channel if radar is detected on the current channel.

2.1.3 Wireless (for Station Mode)

The following describes the parameters for a device operating in *Station* mode.



SSID: MimoSeries1
Mode: Master
Channel: 6 (2.437 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

SSID: MimoSeries2
Mode: Master
Channel: 36 (5.180 GHz)
Bitrate: 866.7 Mbit/s
BSSID: 04:F0:21:34:9F:15

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Figure 5: A summary in the *Wireless* section for a device operating as an 802.11 station

SSID: Displays the name of the wireless network that this station should be associated with.

Mode: This is *'Client'* if the device is in Station mode or in Station WDS mode.

Channel: Shows the channel number and frequency that this station is using. Normally, it would automatically select the same channel as the AP

Bitrate: This is the maximum bitrate supported by the radio in the current configuration.

MAC-Address: States the MAC address of the device's radio.

BSSID: This is the MAC address of the AP's radio.

Encryption: Displays the wireless encryption used.

ACK Timeout: Shows the maximum acknowledgment time in microseconds.

DFS Status: If DFS is enabled, the AP automatically switches channel if radar is detected on the current channel.

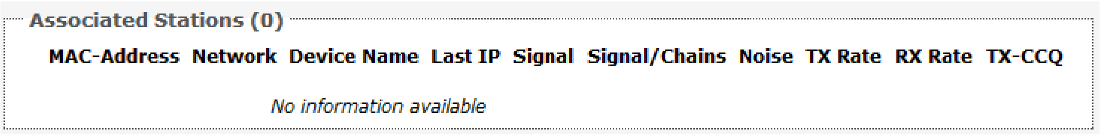
TX-CCQ: Displays the transmission quality in %. A higher percentage means a better wireless connection quality.

RX Rate: Shows the receive bit rate of this station.

TX Rate: Shows the transmit bit rate of this station.

2.1.4 Associated Stations (for AP Mode)

This section shows the connected devices, if the router is in the AP mode.



Associated Stations (0)

MAC-Address	Network	Device Name	Last IP	Signal	Signal/Chains	Noise	TX Rate	RX Rate	TX-CCQ

No information available

Figure 6: List of Associated Stations.

If there are no associated stations, the text “No information available” is displayed. The parameters shown are as follows:

MAC-Address: Displays the MAC address of the station's radio.

Network: States the name of the wireless network.

Device Name: Shows the name of the station.

Last IP: States the most recent IP address of the station as seen by the router

Signal: Displays the received signal strength from the station e.g. -31 dBm.

Signal/Chains: Shows the received signal strengths from the station on each antenna e.g. -52, -35, -34 dBm. The value of -95 dBm is taken to mean “no antenna” if the radio has only 2 antennas.

Noise: Displays the received noise power at the AP.

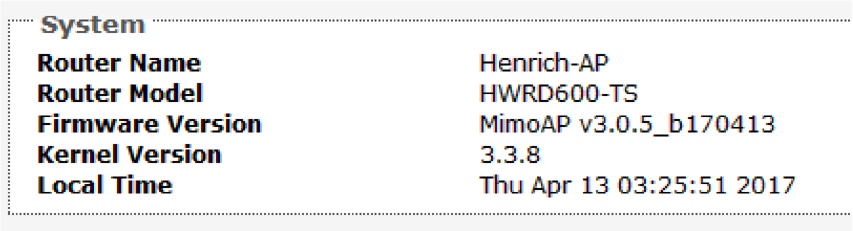
TX Rate: Shows the transmit bit rate from the AP towards this station.

RX Rate: Shows the receive bit rate at the AP from this station.

TX-CCQ: Indicates the wireless connection quality.

2.1.5 System

This section shows the *Router Name, Router Model, Firmware Version, Kernel Version*, and *Local Time.*



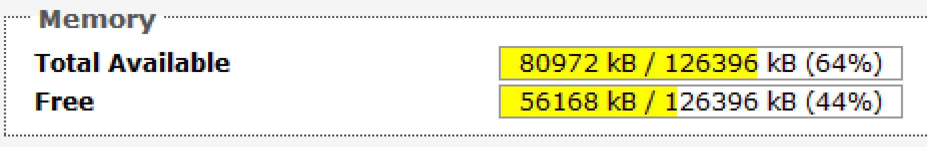
System

Router Name	Henrich-AP
Router Model	HWRD600-TS
Firmware Version	MimoAP v3.0.5_b170413
Kernel Version	3.3.8
Local Time	Thu Apr 13 03:25:51 2017

Figure 7: System parameters

2.1.6 Memory

Here, the *Total Available* and *Free* memory are shown.



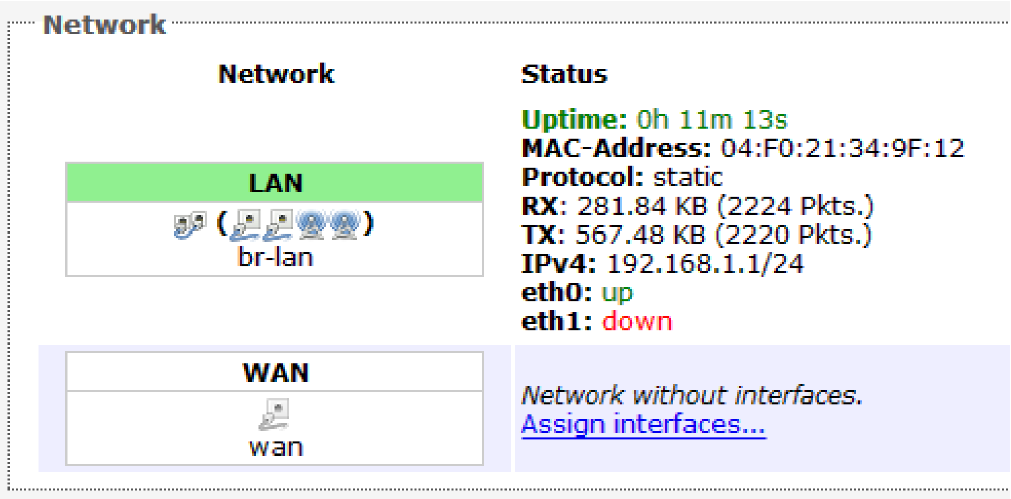
Memory

Total Available	80972 kB / 126396 kB (64%)
Free	56168 kB / 126396 kB (44%)

Figure 8: *Total Available* and *Free* Memory

2.1.7 Network

This section displays the status of the LAN and WAN networks.



Network

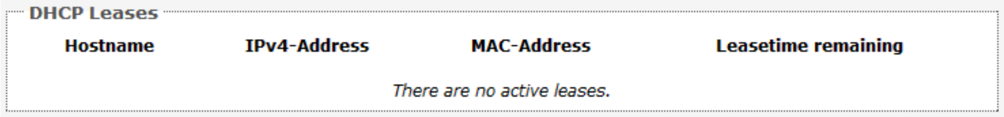
Network	**Status**
LAN br-lan	**Uptime:** 0h 11m 13s **MAC-Address:** 04:F0:21:34:9F:12 **Protocol:** static **RX**: 281.84 KB (2224 Pkts.) **TX**: 567.48 KB (2220 Pkts.) **IPv4:** 192.168.1.1/24 **eth0:** up **eth1:** down
WAN wan	*Network without interfaces.* Assign interfaces...

Figure 9: Network summary

Status: Shows summaries of the interfaces for the LAN and WAN zones. This may include uptime, MAC address, protocol, bytes and packets received by the device, bytes and packets transmitted by the device, and its IPv4 address.

2.1.8 DHCP Leases

This section shows a table of MAC and IP addresses of connected computers with static DHCP leases. They are specified in the *Network* → *Interfaces* → *LAN* → *Static Leases* section of the device's configuration web page. More explanation is given in the *Network* section of this user manual on other page .



DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining

There are no active leases.

Figure 10: Currently active static DHCP leases

2.1.9 Link Status (for Station Mode)

This section only applies if the device operates as an 02.11 station.

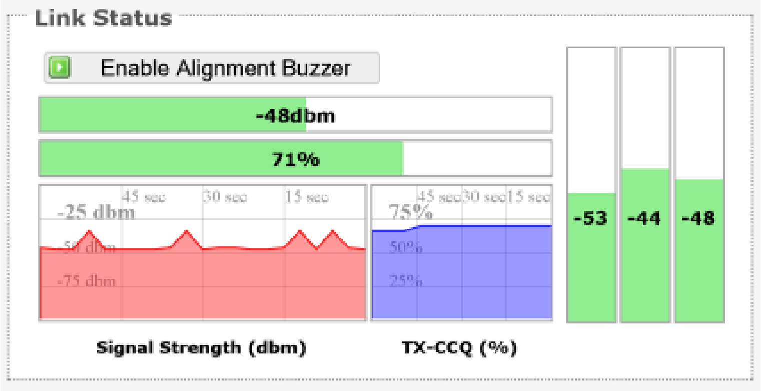


Figure 11: The *Link Status* section

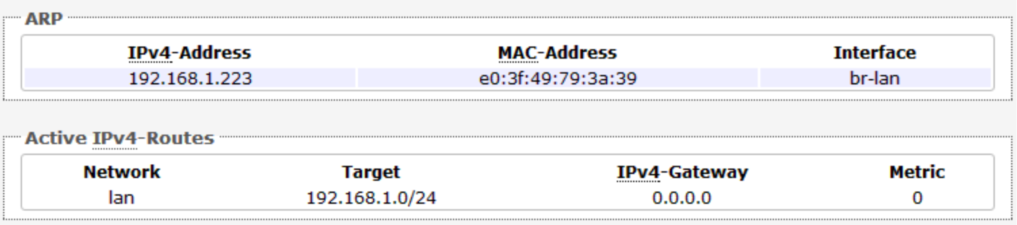
In the *Link Status* section on the *Status → Overview* Web page, the value in the top left box denotes the urrent received signal strength e.g. -48 dBm. The ox directly below it shows the current TX-CCQ (transmission client connection quality) e.g. 71 %. The bottom left box shows a realtime graph of the received signal strength over the last 60 seconds. The box directly to its right shows a realtime graph of the TX-CCQ over the past 60 seconds.

On the right of this section, there are 3 vertical bars. Each bar shows the current received signal strength of each antenna e.g. -53 dBm, -44 dBm, and -48 dBm. If the radio has only 2 antennas, the third vertical bar is given a default value of -95 dBm.

Enable Alignment Buzzer: When enabled, the board would continually emit beeping sounds to indicate the received signal strength. This is currently available on the HWRD boards with a buzzer. Every 3 seconds, the board would emit a number of beeps (1 to 4) in quick succession. The number of beeps is the same as the number of lighted *Signal strength indicator* LEDs. See Section 3.6 on *LED Configuration*. Just like for the LEDs, more beeps indicate a higher received signal strength. This is useful for a person aligning directional antennas at a height, in an outdoor scenario, if the LEDs are not visible. Another person on the ground could adjust the threshold values for the LEDs. There is some delay before the received signal strength gets reported by the alignment buzzer. To turn off the beeping sounds, click the button “Disable Alignment Buzzer”.

2.2 Routes

When you click on the *Status → Routes* tab, you would see the page that shows the routing rules that are currently active on the device.



ARP

IPv4-Address	MAC-Address	Interface
192.168.1.223	e0:3f:49:79:3a:39	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
lan	192.168.1.0/24	0.0.0.0	0

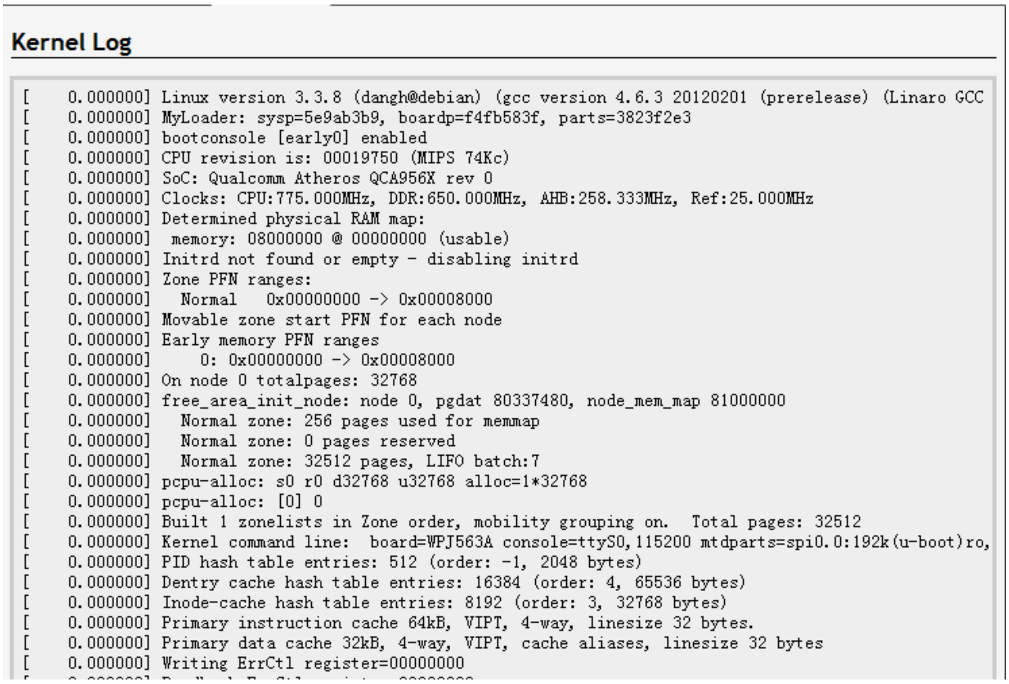
Figure 12: The *Status → Routes* page.

ARP: This address resolution protocol (ARP) table shows the IP address and corresponding MACaddress of each device on the network.

Active IPv4-Routes: This table shows the IPv4 gateway and network ID (Target) for each subnet.

2.3 System Log

When you click on this tab, you can see the log of system messages.



Kernel Log

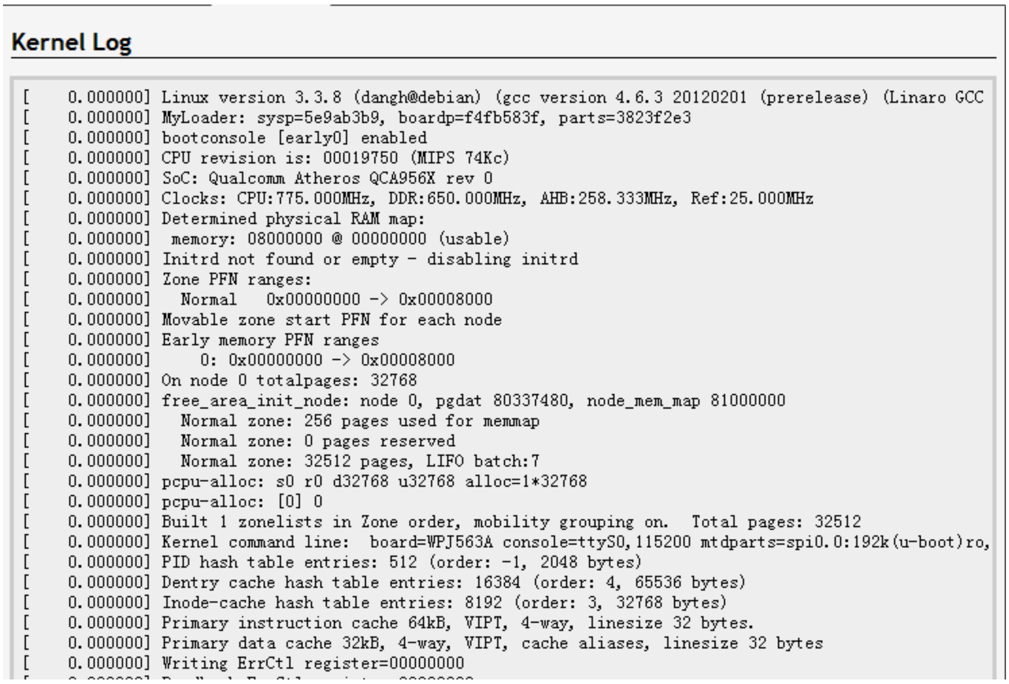
```
[    0.000000] Linux version 3.3.8 (dangh@debian) (gcc version 4.6.3 20120201 (prerelease) (Linaro GCC
[    0.000000] MyLoader: sysp=5e9ab3b9, boardp=f4fb583f, parts=3823f2e3
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU revision is: 00019750 (MIPS 74Kc)
[    0.000000] SoC: Qualcomm Atheros QCA956X rev 0
[    0.000000] Clocks: CPU:775.000MHz, DDR:650.000MHz, AHB:258.333MHz, Ref:25.000MHz
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 08000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Zone PFN ranges:
[    0.000000]   Normal   0x00000000 -> 0x00008000
[    0.000000] Movable zone start PFN for each node
[    0.000000] Early memory PFN ranges
[    0.000000]     0: 0x00000000 -> 0x00008000
[    0.000000] On node 0 totalpages: 32768
[    0.000000] free_area_init_node: node 0, pgdat 80337480, node_mem_map 81000000
[    0.000000]   Normal zone: 256 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 32512 pages, LIFO batch:7
[    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=WPJ563A console=ttyS0,115200 mtdparts=spi0.0:192k(u-boot)ro,
[    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] 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] Writing ErrCtl register=00000000
```

Figure 13: The *Status* → *System Log* page

2.4 Kernel Log

This page shows the kernel debugging messages.

This kernel log can also be obtained by typing “dmesg” in a serial console such as *Tera* Term if a suitable serial connector is used.



Kernel Log

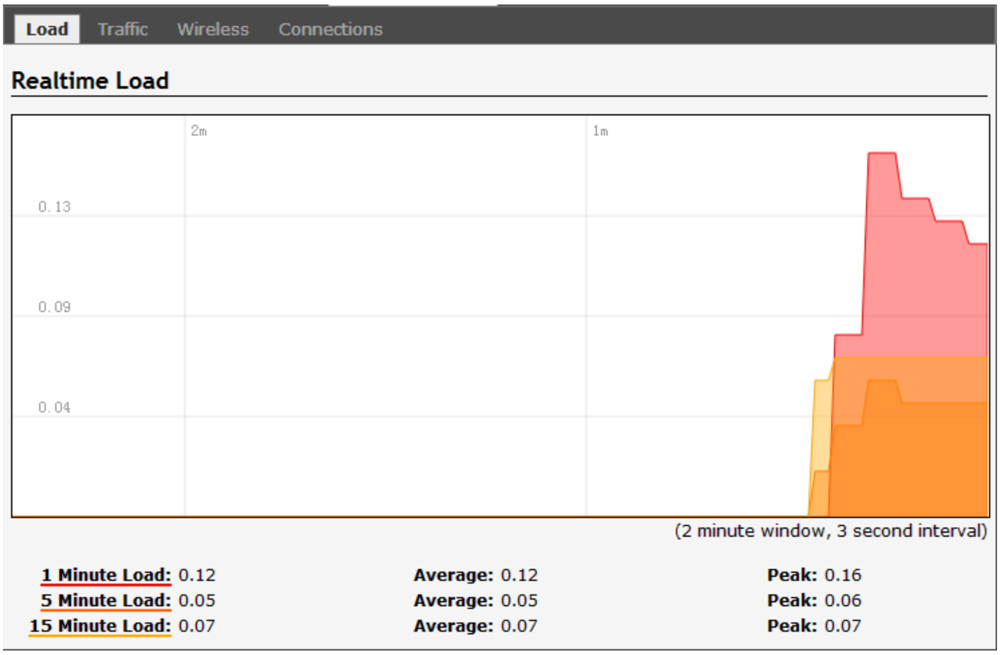
```
[    0.000000] Linux version 3.3.8 (dangh@debian) (gcc version 4.6.3 20120201 (prerelease) (Linaro GCC
[    0.000000] MyLoader: sysp=5e9ab3b9, boardp=f4fb583f, parts=3823f2e3
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU revision is: 00019750 (MIPS 74Kc)
[    0.000000] SoC: Qualcomm Atheros QCA956X rev 0
[    0.000000] Clocks: CPU:775.000MHz, DDR:650.000MHz, AHB:258.333MHz, Ref:25.000MHz
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 08000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Zone PFN ranges:
[    0.000000]   Normal   0x00000000 -> 0x00008000
[    0.000000] Movable zone start PFN for each node
[    0.000000] Early memory PFN ranges
[    0.000000]     0: 0x00000000 -> 0x00008000
[    0.000000] On node 0 totalpages: 32768
[    0.000000] free_area_init_node: node 0, pgdat 80337480, node_mem_map 81000000
[    0.000000]   Normal zone: 256 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 32512 pages, LIFO batch:7
[    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=WPJ563A console=ttyS0,115200 mtdparts=spi0.0:192k(u-boot)ro,
[    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] 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] Writing ErrCtl register=00000000
```

Figure 14: The *Status* → *Kernel Log* page

2.5 Realtime Graphs

Under the tab for *Realtime Graphs,* there are four tabs titled *Load, Traffic, Wireless,* and *Connection*.

2.5.1 Load



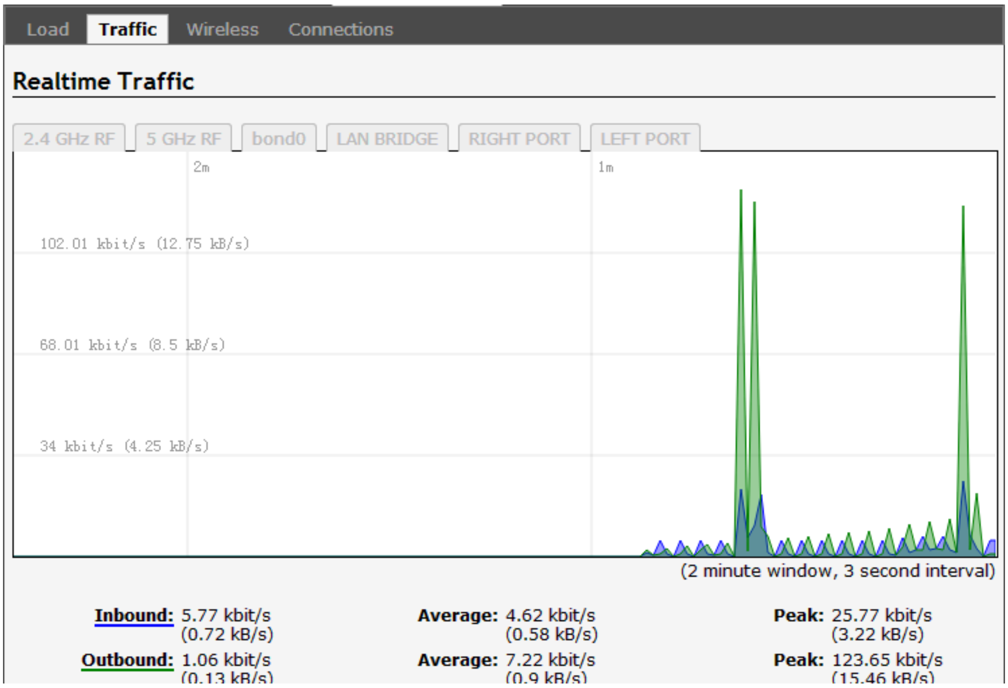
Realtime Load

(2 minute window, 3 second interval)

1 Minute Load: 0.12	**Average:** 0.12	**Peak:** 0.16
5 Minute Load: 0.05	**Average:** 0.05	**Peak:** 0.06
15 Minute Load: 0.07	**Average:** 0.07	**Peak:** 0.07

Figure 15: The graph for *Realtime Load*

2.5.2 Traffic



Realtime Traffic

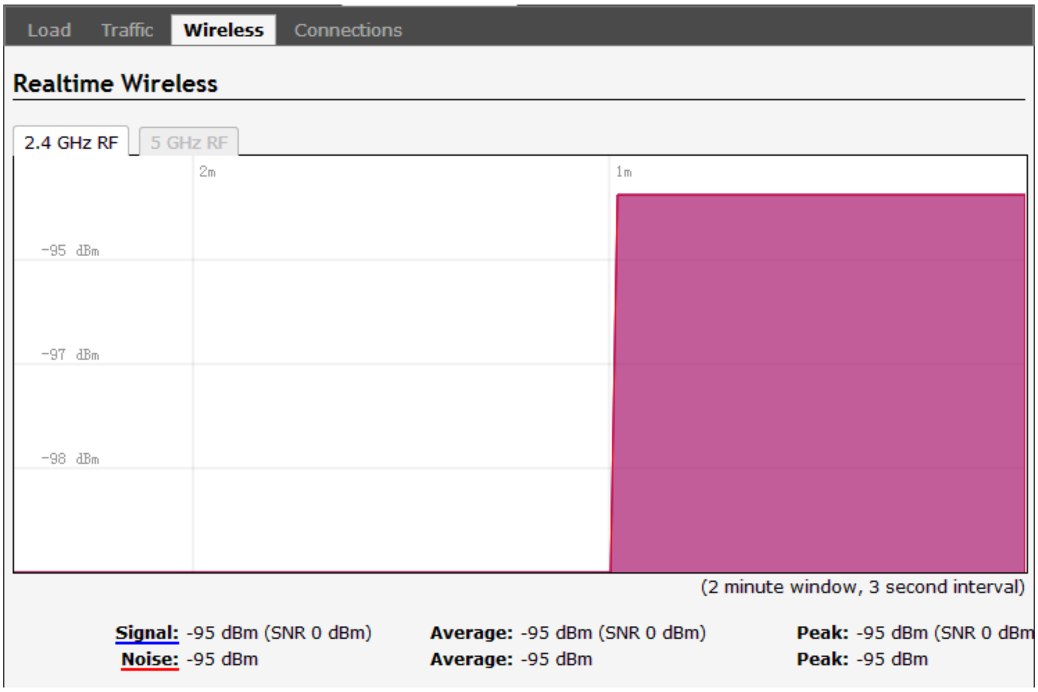
(2 minute window, 3 second interval)

Inbound: 5.77 kbit/s (0.72 kB/s) **Average:** 4.62 kbit/s (0.58 kB/s) **Peak:** 25.77 kbit/s (3.22 kB/s)

Outbound: 1.06 kbit/s (0.13 kB/s) **Average:** 7.22 kbit/s (0.9 kB/s) **Peak:** 123.65 kbit/s (15.46 kB/s)

Figure 16: The graph for *Realtime Traffic*

2.5.3 Wireless



Realtime Wireless

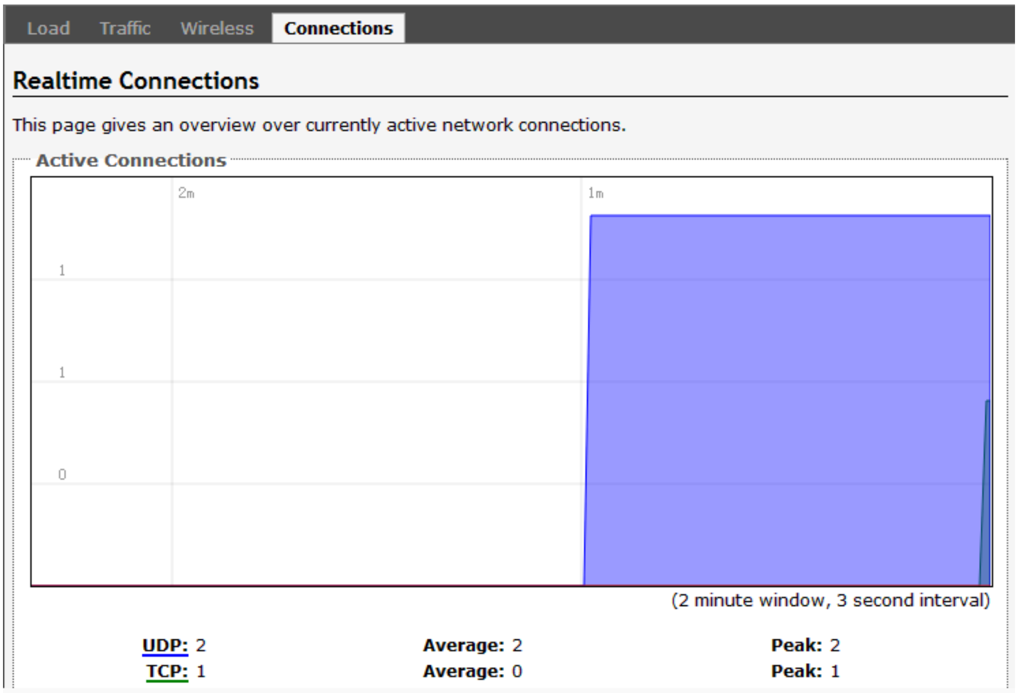
(2 minute window, 3 second interval)

Signal: -95 dBm (SNR 0 dBm) **Average:** -95 dBm (SNR 0 dBm) **Peak:** -95 dBm (SNR 0 dBm

Noise: -95 dBm **Average:** -95 dBm **Peak:** -95 dBm

Figure 17: The graph for *Realtime Wireless*

2.5.4 Connection



Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(2 minute window, 3 second interval)

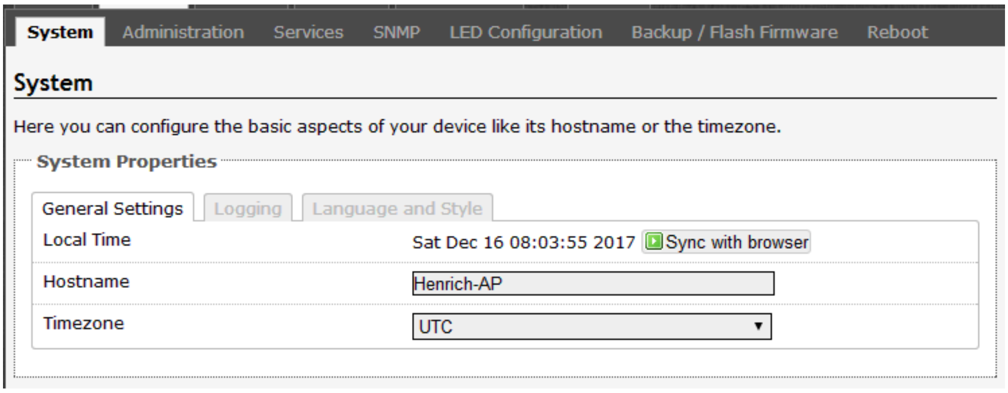
UDP: 2	**Average:** 2	**Peak:** 2
TCP: 1	**Average:** 0	**Peak:** 1

Figure 18: The graph for *Realtime Connections*

Chapter 3: System Tab

This section is about the *System* top-level tab.

Under this tab, there is a row of tabs for *Administration, Services, SNMP, LED Configuration, Backup/Flash Firmware*, and *Reboot*. This can be seen in Figure 19.



System

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

System Properties

Local Time: Sat Dec 16 08:03:55 2017 Sync with browser

Hostname: Henrich-AP

Timezone: UTC

Figure 19: The *System* top-level tab

3.1 System

Within the *System* page, you can configure the device parameters such as the hostname and timezone.

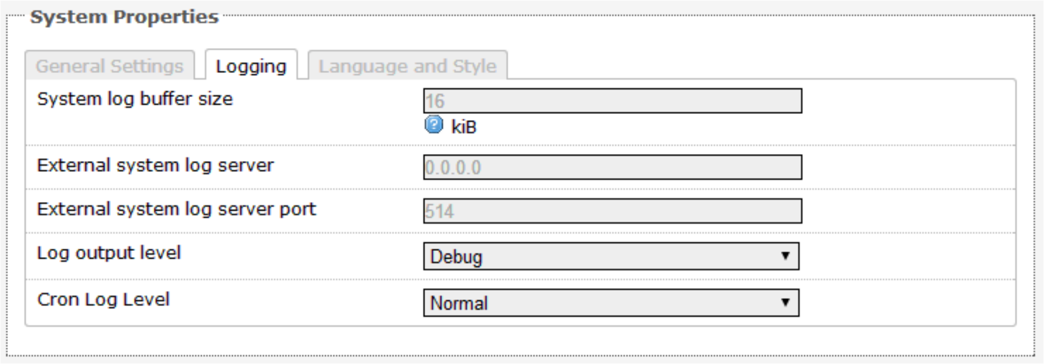
3.1.1 System Properties

Within the section on *System Properties*, there are tabs corresponding to *General Settings, Logging, and Language* and *Style*.

General Settings

Local Time: Displays the local time according to the Timezone.
Hostname: Configures the name of the device.
Timezone: Sets the timezone.

Logging


System Properties

System log buffer size: 16 kiB

External system log server: 0.0.0.0

External system log server port: 514

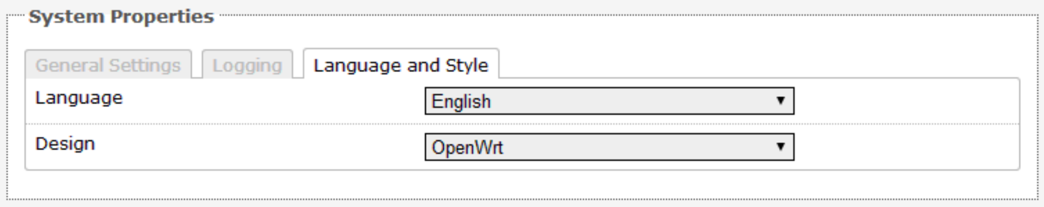
Log output level: Debug

Cron Log Level: Normal

Figure 20: Changing the system properties for *Logging*

Logging: Specifies parameters used for the system log, such as *System log buffer size*, *External system log server, External system log server port, Log output level,* and *Cron Log Level.*

Language and Style



Language: English

Design: OpenWrt

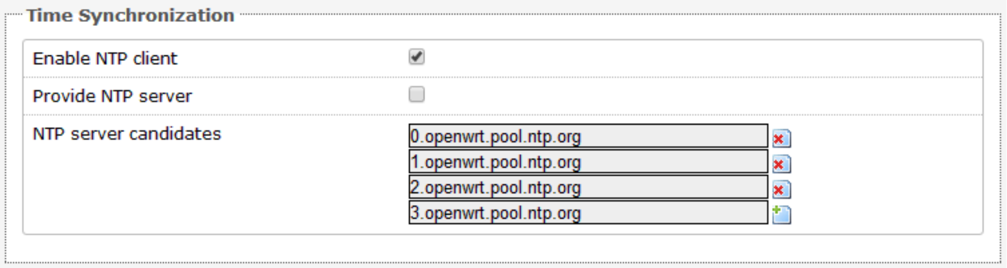
Figure 21: Modifying the *Language and Style*

Language and Style: Lets you choose the language and design of the router's web pages.

3.1.2 Time Synchronization

Enable NTP client: Obtains the date and time from specified Network Time Protocol (NTP) servers.

NTP server candidates: These are the sources of the time information. At least three are recommended for accurate time synchronization.



Enable NTP client ☑

Provide NTP server ☐

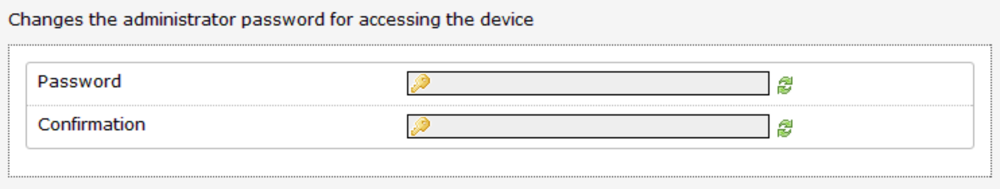
NTP server candidates:
0.openwrt.pool.ntp.org
1.openwrt.pool.ntp.org
2.openwrt.pool.ntp.org
3.openwrt.pool.ntp.org

Figure 22: Time *Synchronization* settings

3.2 Administration

Within the *System → Administration* page, you can configure the *Router Password*, *SSH*, *Telnet*, *Web*, and *FTP* settings.

3.2.1 Router Password


Changes the administrator password for accessing the device

Password

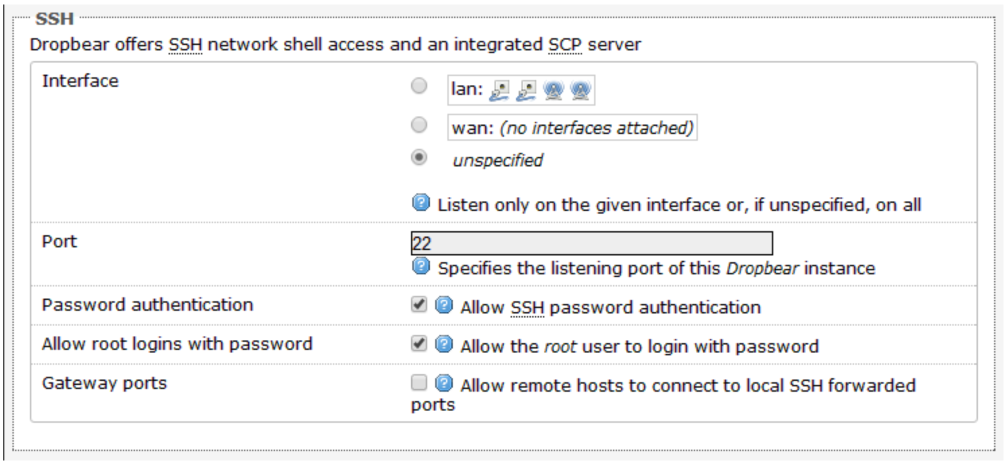
Confirmation

Figure 23: Setting the router password

Password: Allows you to set the router password, the default being *password*.

Confirmation: Requires you to re-enter the password.

3.2.2 SSH



SSH

Dropbear offers SSH network shell access and an integrated SCP server

Interface	○ lan: ○ wan: *(no interfaces attached)* ● *unspecified* Listen only on the given interface or, if unspecified, on all
Port	22 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

Figure 24: *SSH* settings in the *System → Administration* page

SSH: Allows you to access the router's Linux shell and file system using the *Secure Shell* protocol. For example, the programs *PuTTY* and *WinSCP* can be used.

Interface: Lets the device listen on a given interface or all interfaces.

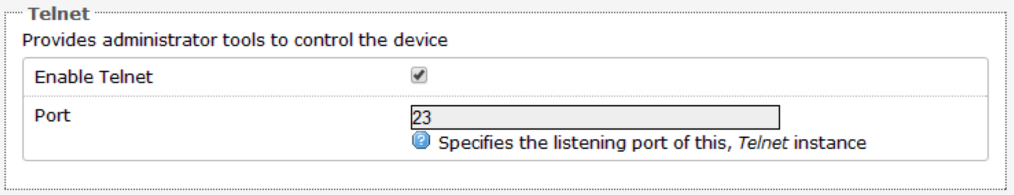
Port: Specifies the listening port, the default being *22*.

Password authentication: Allows *SSH* password authentication.

Allow root logins with password: This is enabled by default.

Gateway ports: Allow remote hosts to connect to local *SSH* forwarded ports.

3.2.3 Telnet



Telnet

Provides administrator tools to control the device

Enable Telnet	☑
Port	23 Specifies the listening port of this, *Telnet* instance

Figure 25: *Telnet* settings in the *System → Administration* page

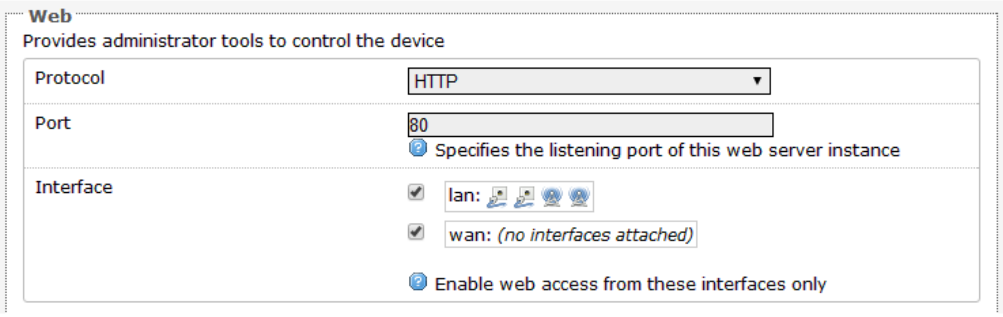
Telnet: Provides administrator tools for controlling the device or network debugging, over an unencrypted connection.

Port: Specifies the listening port, the default being 23.

To start using Telnet, enter the command "telnet 192.168.1.1" or "telnet 192.168.1.1 23" into a Command Prompt if using Windows, or into a Terminal if using Linux or Mac OS X. This is assuming that 192.168.1.1 is the IP address of your router.

The splash page of OpenWRT appears after login. Commands can then be entered into the Linux shell of the router, e.g. ifconfig, iwconfig, iwpriv, uci show, ls /bin, ls /sbin, ls /usr/bin, or ls /usr/sbin.

3.2.4 Web



Web

Provides administrator tools to control the device

Protocol	HTTP ▾
Port	80 Specifies the listening port of this web server instance
Interface	☑ lan: ☑ wan: *(no interfaces attached)* Enable web access from these interfaces only

Figure 26: The router's web server mode and port.

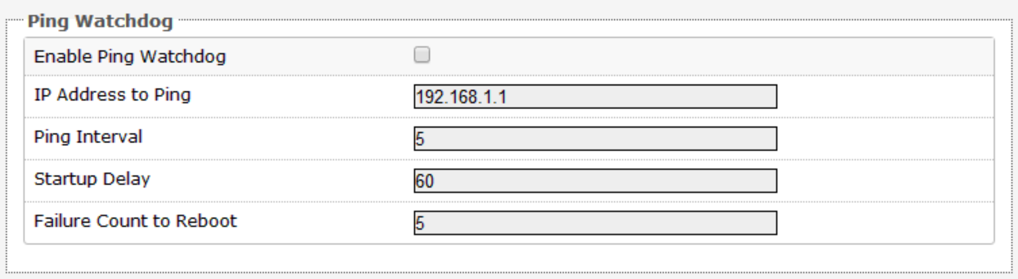
Web Server Mode: This can be set to Hypertext Transfer Protocol (*HTTP*) or Hypertext Transfer Protocol Secure (*HTTPS*). For *HTTPS*, if you see the warning, "The certificate is not trusted because it is self-signed. The certificate is only valid for OpenWRT," click "Add Exception", "Confirm Security Exception" and proceed.

Port: Specifies the listening port, the default being *80* for *HTTP* and *443* for *HTTPS*.

3.3 Services

In the *System → Services* page, you can configure the *Ping Watchdog* and the *Auto Reboot*.

3.3.1 Ping Watchdog



Ping Watchdog

Enable Ping Watchdog	□
IP Address to Ping	192.168.1.1
Ping Interval	5
Startup Delay	60
Failure Count to Reboot	5

Figure 27: *Ping Watchdog* settings in the *System → Services* page

Ping Watchdog: Configures the device to ping to a remote IP address and reboot if the connection is lost. It is disabled by default.

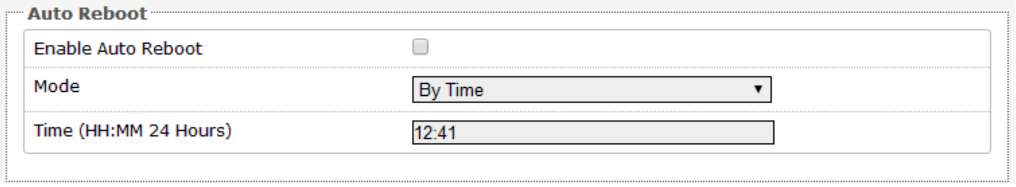
IP Address to Ping: Sets the remote IP address to ping e.g. 192.168.1.10 or 8.8.8.8.

Ping Interval: Specifies the time between successive pings, the default being 5 seconds.

Startup Delay: Sets the time delay after the router finishes rebooting, before running the Ping Watchdog, the default being 60 seconds.

Failure Count to Reboot: Specifies the number of failed pings before the router reboots automatically.

3.3.2 Auto Reboot



Auto Reboot

Enable Auto Reboot	□
Mode	By Time ▾
Time (HH:MM 24 Hours)	12:41

Figure 28: *Auto Reboot* settings in the *System → Services* page

Auto Reboot: Allows the router to reboot itself automatically, disabled by default.

Mode: Chooses the *Auto Reboot* mode *By Time* or *By Number of Hours*.

Time: Sets the time of day to reboot if the *Mode* is *By Time*.

Number of Hours: Sets the delay as an integer number of hours after each reboot, if the *Mode* is *By Number of Hours.*

3.4 SNMP

The Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

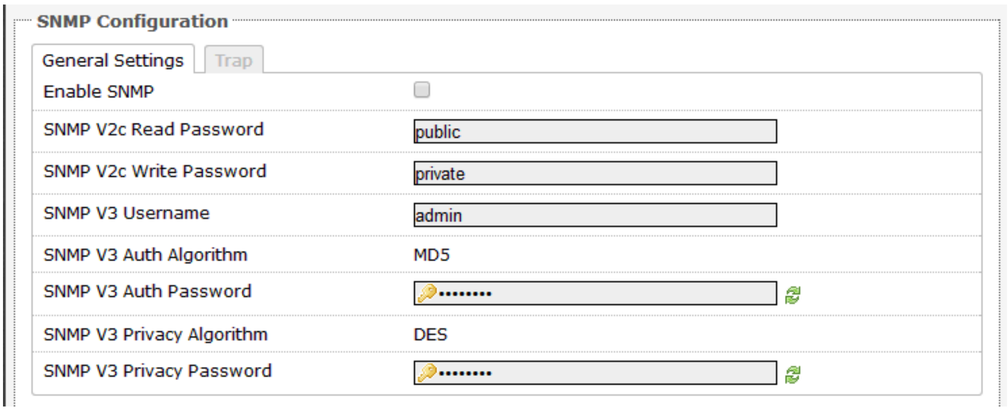
In the *System → SNMP* Page, you can configure SNMP V2c and SNMP V3.

3.4.1 SNMP Information

In the *SNMP Information* section, the text fields for the *SNMP Enterprise ID*, *Contact*, and *Location information* are shown.

3.4.2 SNMP Configuration

General Settings



SNMP Configuration

General Settings | Trap

Enable SNMP	□
SNMP V2c Read Password	public
SNMP V2c Write Password	private
SNMP V3 Username	admin
SNMP V3 Auth Algorithm	MD5
SNMP V3 Auth Password	••••••••
SNMP V3 Privacy Algorithm	DES
SNMP V3 Privacy Password	••••••••

Figure 29: General settings for SNMP

Enable SNMP: Enables SNMP.

SNMP V2c Read Password: Sets the community string for read-only access (to the variables on the SNMP agent) by the network management station (NMS). The NMS is the software which runs on the SNMP manager. (default: public)

SNMP V2c Write Password: Sets the community string for read-write access by the SNMP manager. (default: private) A community string identifies a group of SNMP agents. It is sent in clear text. It should be changed from the default string “public” or “private”. The variables on the SNMP agent can be classified into read-only or read-write variables.

SNMP V3 Username: Sets the username for authentication. (default: admin)

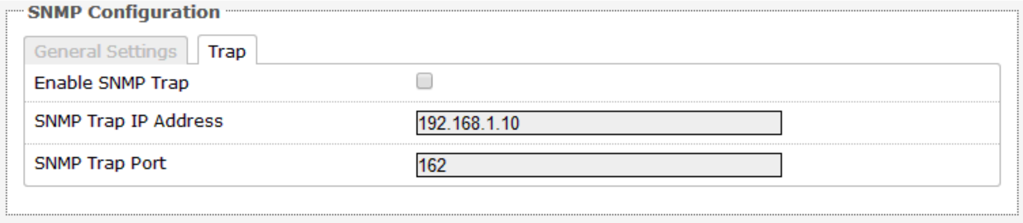
SNMP V3 Auth Algorithm: Shows the authentication algorithm used e.g. MD5.

SNMP V3 Auth Password: Configures the password for user authentication. (default: password)

SNMP V3 Privacy Algorithm: Shows the data encryption algorithm used e.g. DES.

SNMP V3 Privacy Password: Sets the password for data encryption. (default: password)

Trap



SNMP Configuration

Enable SNMP Trap ☐

SNMP Trap IP Address: 192.168.1.10

SNMP Trap Port: 162

Figure 30: SNMP trap configuration

Enable SNMP Trap: Allows the SNMP agent to notify the SNMP manager of events.

SNMP Trap IP Address: Sets the IP address of the SNMP manager which receives the trap messages.

SNMP Trap Port: Sets the port number.

3.5 Reset Button

The reset button is a physical hardware button on the AP hardware board. Depending on how long the button is pressed, you can reboot the board or reset it to factory default. First make sure that the power is on and wait a minute for the board to finish starting up. The following table shows the duration of the button press and the corresponding action.

Duration of button press	Action
0 - 3 seconds	**reboot**
4 - 30 seconds	**reset to factory default**
more than 30 seconds	**do nothing**

3.6 LEDs on the Board

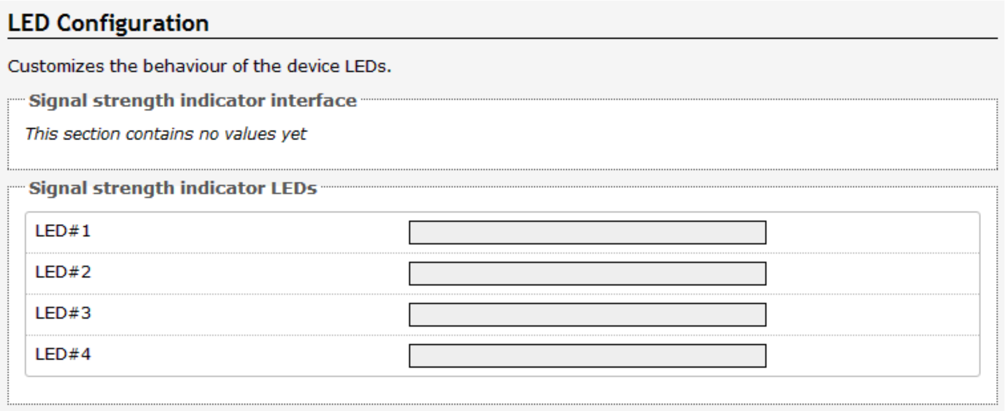
On the HWRD boards, the LEDs starting from the one nearest the corner are: Power, LAN, LED#1, LED#2, LED#3, and LED#4.

3.6.1 LED Configuration for Signal Strength Indicator LEDs #1 to #4

The *System* → *LED Configuration* page customizes how the LEDs indicate the received signal strength.

Signal strength indicator interface: Chooses the Wireless interface, which is the wireless network name.

Signal strength indicator LEDs: Sets the received signal strength thresholds (in dBm) above which LEDs #1 to #4 would light up.



LED Configuration

Customizes the behaviour of the device LEDs.

Signal strength indicator interface

This section contains no values yet

Signal strength indicator LEDs

LED#1	
LED#2	
LED#3	
LED#4	

Figure 31: Signal strength indicator LEDs and their default threshold values in dBm

3.6.2 Loader Mode

The loader mode allows the board to listen to a TFTP server for downloading a new firmware.

To enter the loader mode of the board, power off the board, hold down the reset button, power on the board, and then release the reset button.

The LED farthest from the corner (LED#4) would start blinking steadily. The IP address of the board becomes 192.168.168.1. The program TFTPD32 can be used to create a TFTP server on a computer, by running this program in the same folder as the firmware to be loaded.

3.6.3 Summary of the LED Indicators

The LED indicators are summarized in the following table.

LED	Description
Power (green)	The Power LED emits a steady light when electrical power (normally at 24 V) is supplied to the board
LAN (green)	The LAN/Diagnostic LED is lighted dimly when the LAN ports are not connected. The LAN LED blinks whenever packets are transferred through any of the LAN ports
LED#1 (red)	ED#1 indicates the received signal strength (low).
LED#2 (orange)	LED#2 indicates the received signal strength (medium)
LED#3 (green)	LED#3 indicates the received signal strength (high).
LED#4 (green)	LED#4 indicates the received signal strength (very high). When the board is in the Loader mode, this LED blinks steadily. LEDs #1 to #3 are not lighted up

3.7 Backup/Flash Firmware

The *System → Backup/Flash Firmware* page lets you perform backup and restore, or flash a new firmware.

3.7.1 Backup/Restore

Download backup: Generate archive: Downloads a tar archive of the current configuration files.

Reset to defaults: Perform reset: Resets the firmware to its initial state.

Restore backup: Upload archive: Lets you upload a previously generated backup archive to restore configuration files.

3.7.2 Flash new firmware

You can upload a new firmware to replace the currently running firmware.

Keep settings: Retains the current configuration.

Firmware: Shows the current version of the firmware and allows you to upload a new firmware.

3.8 Reboot

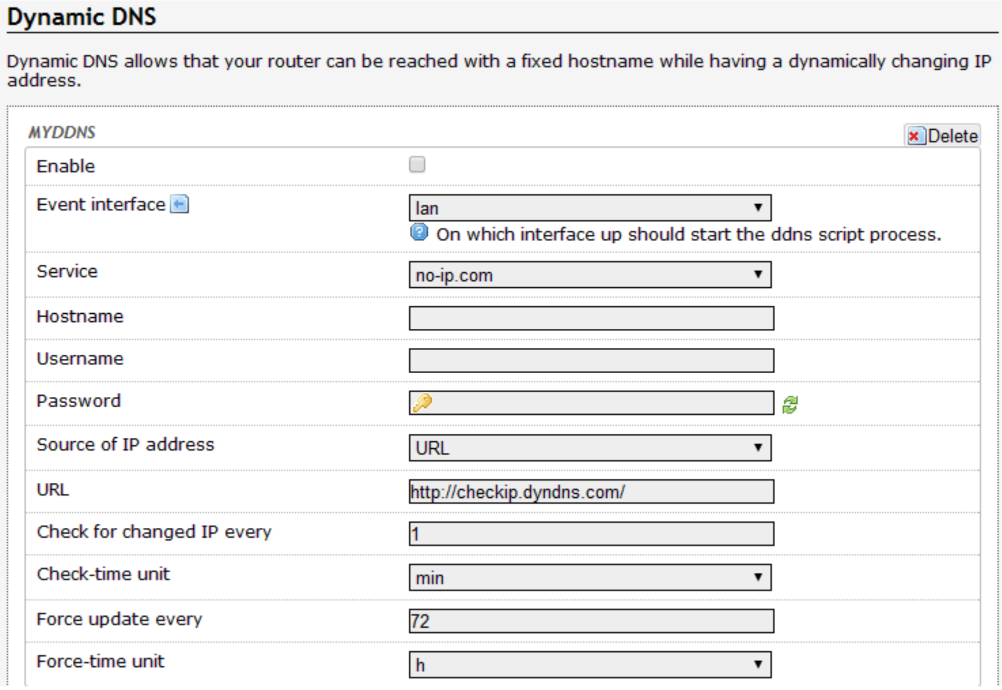
Perform reboot: Reboots the operating system of your device. This is similar to the power-off and power-on cycle. The system configuration remains the same. Any changes that are not applied are lost.

Chapter 4: Services Tab

The *Services* top-level tab contains the configuration pages for *Dynamic DNS*, *Hotspot*, and *Discovery*.

4.1 Dynamic DNS

The domain name system (DNS) translates a URL like www.yahoo.com to an IP address like 206.190.36.45. Dynamic DNS (DDNS) allows the router with the public IP address to be reached from the internet via a URL even if its IP address is dynamically changing.



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

MYDDNS ☒ Delete

Enable	□
Event interface	lan ▾ On which interface up should start the ddns script process.
Service	no-ip.com ▾
Hostname	
Username	
Password	
Source of IP address	URL ▾
URL	http://checkip.dyndns.com/
Check for changed IP every	1
Check-time unit	min ▾
Force update every	72
Force-time unit	h ▾

Figure 32: The *Services* → *Dynamic DNS* page

Enable: Enables the dynamic DNS.

Event interface: Chooses the interface, e.g. LAN or WAN, for which "interface up" would run the DDNS script process.

Service: Chooses the DDNS service provider e.g. noip.com.

Hostname: Specifies the hostname e.g. y0033.noip.biz.

Username: Sets the username registered for the DDNS service.

Password: Sets the password registered for the DDNS service.

Source of IP Address: Configures the source of the IP address information. The default is URL.

URL: Sets the URL of the source of the IP address information

e.g. http://checkip.dyndns.com/.

Check for changed IP every: The default is to check the IP address every 1 minute.

Force update every: The default is to force update every 72 hours.

4.2 Hotspot

The Hotspot service allows you to control the access and usage of the Internet by connected devices.

4.2.1 Setting up the Connections

The following subsections contain advice on configuring the router to implement the hotspot. This router is referred to here as the hotspot router. It is recommended to configure the LAN, Wifi, and WAN, then test it before enabling the hotspot setting.

LAN Interface: DHCP Server

It is recommended to enable the DHCP server, because network address translation (NAT) occurs between the WAN zone and the LAN zone. To do this, you may go to the *Network → Interfaces → LAN (Edit) → Physical Settings → DHCP Server* section, then uncheck the option Ignore interface *(Disable DHCP for this interface)*.

Devices or computers that connect to this hotspot router can then obtain their IP addresses automatically. In addition, the default gateway IP address and the DNS server IP address are automatically configured for these connected devices.

If the DHCP server is left disabled, it is still possible for devices to connect to the hotspot. Each device would need a unique static IP address on the same subnet as this hotspot router. Set the default gateway and DNS server for the device both to be the IP address of this hotspot router.

It is not necessary to set the hotspot router's default gateway and DNS server in the *Network → Interfaces → LAN* page. This information is obtained automatically from the WAN interface.

Wifi Settings

The wireless networks should be set up to allow any user to access the Internet, assuming that the hotspot is not yet enabled.

WAN Interface: Physical Settings

The hotspot has no effect if there is no WAN interface. To use the hotspot, please set the WAN interface in the *Network → Interfaces → WAN (Edit) → Physical Settings.* The WAN interface should be the zone where the Internet access is available. It could be one of the Ethernet adapters or one of the wireless networks. All interfaces other than the WAN interface are considered as in the LAN zone. Any user in the LAN zone would see the hotspot login page after the hotspot is set up.

Test Internet Connection

At this point, before setting up the hotspot, it is good to test the Internet connection by connecting a mobile phone to a wireless network in the LAN zone of the hotspot router

The Internet browser may cache web pages, so to be sure, one may perform an Internet search of a random string of numbers. If the search results are returned, this means that the

Internet connection is working fine.

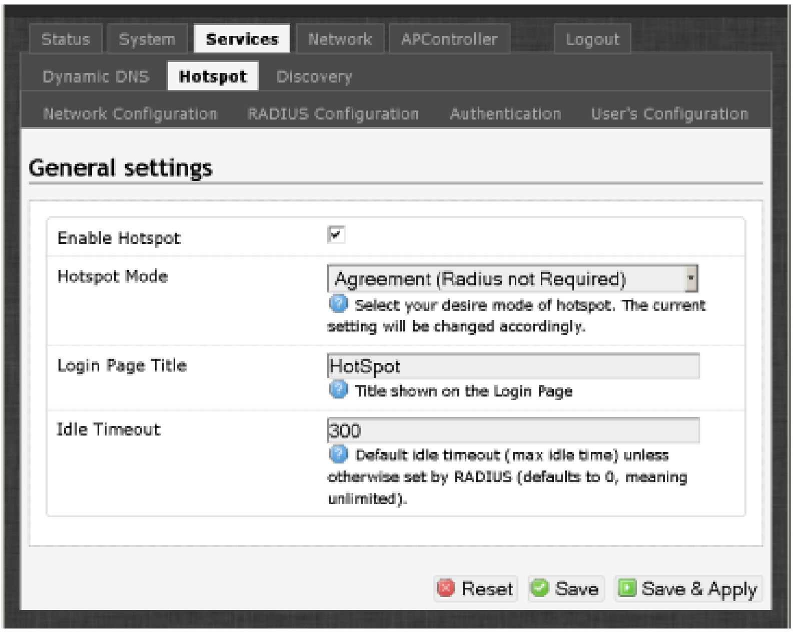
4.2.2 Setting up the Hotspot

The hotspot can then be set up and enabled either by using the AP itself or by using a Henrich Access Point Controller (APc).

The following sections show the Hotspot settings available in the AP's LuCI web page.

4.2.3 General Settings

By clicking on the *Services* → *Hotspot* tab, you can see the general settings.



General settings

Enable Hotspot ☑

Hotspot Mode: Agreement (Radius not Required)
Select your desire mode of hotspot. The current setting will be changed accordingly.

Login Page Title: HotSpot
Title shown on the Login Page

Idle Timeout: 300
Default idle timeout (max idle time) unless otherwise set by RADIUS (defaults to 0, meaning unlimited).

Figure 33: The *Services* → *Hotspot* page

Enable Hotspot: Turns on the hotspot service. You may wish to enable the hotspot after all the settings are completed.

Hotspot Mode: Selects your desired mode of hotspot. You can choose to use the hotspot together with a third party or external RADIUS authentication server.

Login Page Title: Sets the title shown on the Login Page e.g. “HotSpot”.

Idle Timeout: Configures the default idle timeout (max idle time) in seconds unless otherwise set by RADIUS (Set as 0 to mean unlimited time).

4.2.4 Network Configuration

Network Parameters: Auto Config: Automatically configures the network parameters. It is recommended to keep this enabled.

4.2.5 RADIUS Configuration

Here you can set the RADIUS parameters.

Radius Server 1: Sets the IP address of Radius server 1 e.g. 127.0.0.1.

Radius Server 2: Sets the IP address of Radius server 2 e.g. 127.0.0.1.

Radius Secret: Sets the Radius shared secret for both servers. This secret should be changed in order not to compromise security.

4.2.6 Authentication

Here you can set the Universal Access Method (UAM) parameters.

UAM Server: Sets the URL of the web server to use for authenticating clients.

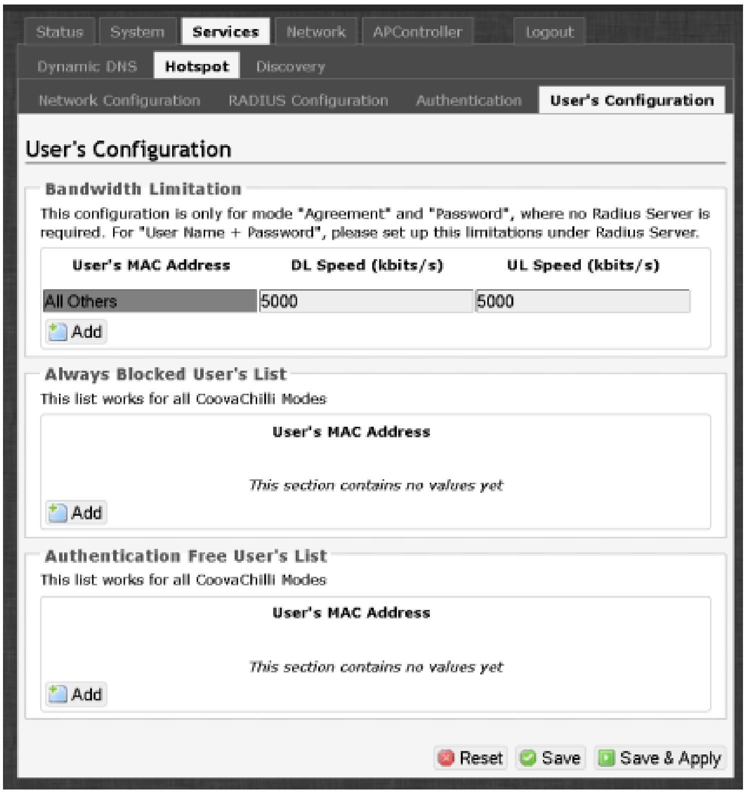
UAM Secret: Configures the shared secret between uamserver and chilli. This secret should be set in order not to compromise security.

Walled Garden (Domain): Shows a comma separated list of resources the client can access without first authenticating. Each entry in the list is a domain name. Do not put www in the domain name. For example, “google.com” is a good domain name, “www.google.com” is not acceptable. The default is “coova.org”.

Walled Garden (IP Address): Shows a comma separated list of resources the client can access without first authenticating. Each entry in the list is a IP Address. The AP's web page is always accessible.

4.2.7 User's Configuration

Here you can configure the users' network access and bandwidth limitations.



User's Configuration

Bandwidth Limitation

This configuration is only for mode "Agreement" and "Password", where no Radius Server is required. For "User Name + Password", please set up this limitations under Radius Server.

User's MAC Address	DL Speed (kbits/s)	UL Speed (kbits/s)
All Others	5000	5000

Always Blocked User's List

This list works for all CoovaChilli Modes

User's MAC Address

This section contains no values yet

Authentication Free User's List

This list works for all CoovaChilli Modes

User's MAC Address

This section contains no values yet

Figure 34: The *Services* → *Hotspot* → *User's Configuration* page

Bandwidth Limitation

This section only applies if the Radius Server is not required. If the Radius Server is required, this section is ignored.

You may add entries consisting of the following three fields:

- User's MAC Address
- Download (DL) Speed (kbits/s)

- Upload (UL) Speed (kbits/s)

By default, there is an entry:

- User's MAC Address: All Others
- Download (DL) Speed (kbits/s): 000
- Upload (UL) Speed (kbits/s): 5000

This means that all hotspot users are subjected to 5000 kbits/s bandwidth limitation. To prevent any limitation, it may be set to a high value like 5000000 kbits/s.

Always Blocked User's List

You may add entries for: User's MAC Address.

These users would be blocked from accessing the network.

This list works for all Hotspot Modes.

Authentication Free User's List

You may add entries for: User's MAC Address.

These users would not need any authentication at all and can get immediate access to the network. For example, the boss of the company could be in the authentication free list.

This list works for all Hotspot Modes

4.2.8 Logging in to the Hotspot

When a hotspot user opens an Internet browser on his/her computer, it would automatically show the hotspot login page. To quickly see the hotspot login page, he/she could enter a simple URL in the Internet browser e.g.

- 1.0.0.1
- 8.8.8.8
- bing.com

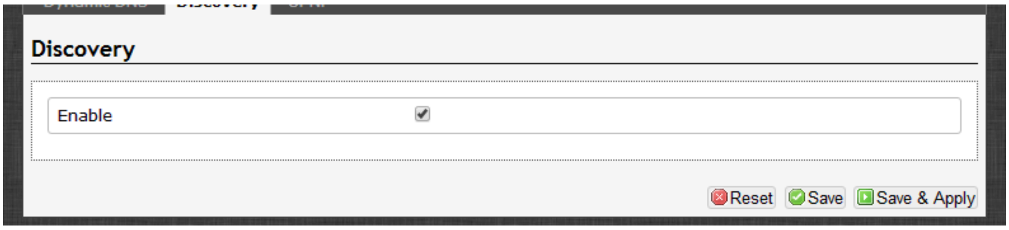
When a user connects his/her mobile/smart phone to the hotspot wireless network, the hotspot login page should automatically appear. Otherwise, he/she could open the default Internet browser app or Chrome app on their mobile phone to see the login page.

4.2.9 Possible Hotspot Scenarios

The WAN interface could be set as one of the Ethernet ports. This means that the wireless networks provided by the hotspot router would be in the LAN zone. Users can connect within the LAN zone to see the hotspot login page.

The wireless distribution system (WDS) can also be used to increase the coverage. More information is found in Section 5.4.2 Interface Configuration.

4.3 Discovery



Discovery

Enable ☑

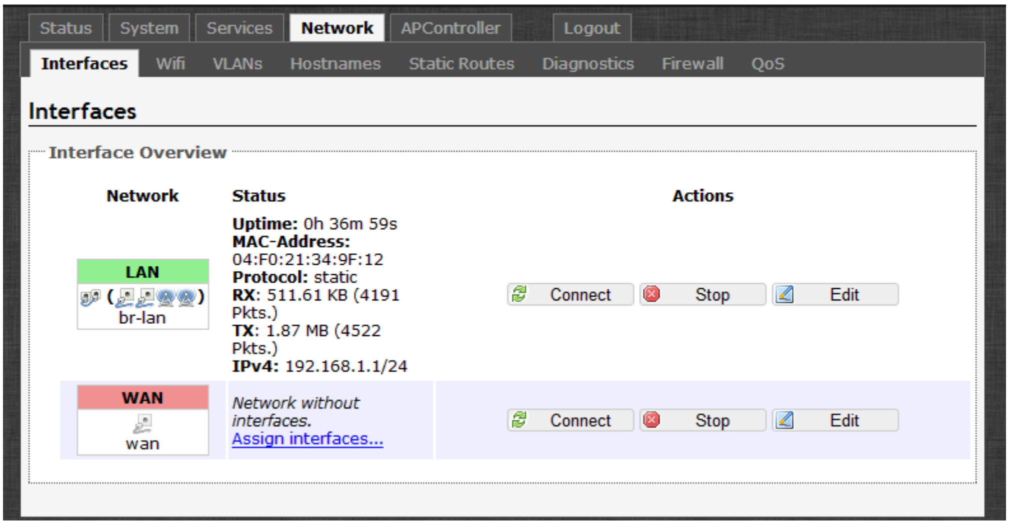
Figure 35: The *Services* → *Discovery* page

Enable: Allows the Device Name and Last IP address of the wireless station to be discovered by the wireless access point. The functionality is similar to the Cisco Discovery Protocol. Discovery is enabled by default.

Chapter 5: Network Tab

The *Network* → *Interfaces* tab shows an overview of the network interfaces. You can view and configure the interfaces of the local area network (LAN) zone as well as the wide area network (WAN) zone.

Network address translation (NAT) occurs between these two network zones. The router that performs the NAT is called a gateway. A gateway is a network point that acts as an entrance to another network.

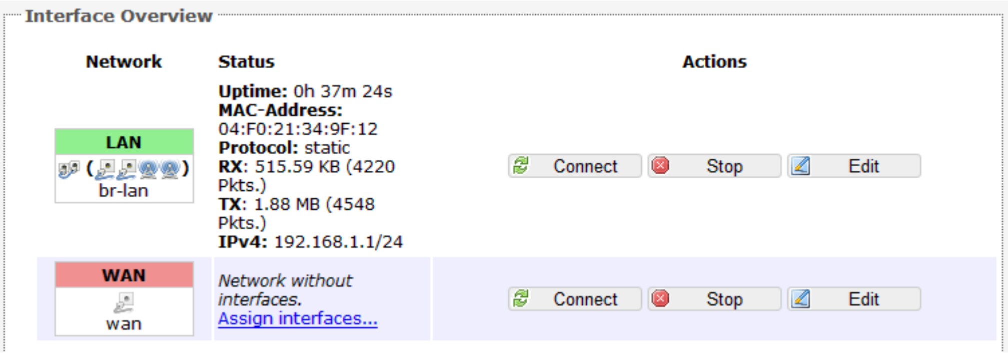


Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	**Uptime:** 0h 36m 59s **MAC-Address:** 04:F0:21:34:9F:12 **Protocol:** static **RX:** 511.61 KB (4191 Pkts.) **TX:** 1.87 MB (4522 Pkts.) **IPv4:** 192.168.1.1/24	Connect Stop Edit
WAN wan	*Network without interfaces.* Assign interfaces...	Connect Stop Edit

Figure 36: The *Network* top-level tab



Interface Overview

Network	Status	Actions
LAN br-lan	**Uptime:** 0h 37m 24s **MAC-Address:** 04:F0:21:34:9F:12 **Protocol:** static **RX:** 515.59 KB (4220 Pkts.) **TX:** 1.88 MB (4548 Pkts.) **IPv4:** 192.168.1.1/24	Connect Stop Edit
WAN wan	*Network without interfaces.* Assign interfaces...	Connect Stop Edit

Figure 37: The *Interface Overview* on the *Network* → *Interfaces* page

The *Network* column shows that the WAN zone has the physical port “eth1” as its interface.

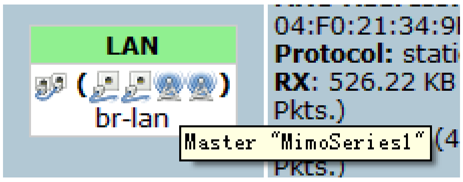


Figure 38: An infotip appears when hovering the mouse over an icon

In Figure 38, the LAN zone (icon with two Ethernet ports) has the bridged interface “br-lan” which consists of one physical port (icon with one Ethernet port) and two wireless networks (each icon looking like a short standing fan) on the device. Hovering the mouse over each icon would give the name of the interface it represents. In this example, the infotip shows that there is a (virtual) access point on the device with “MimoSeries1” as its network name.

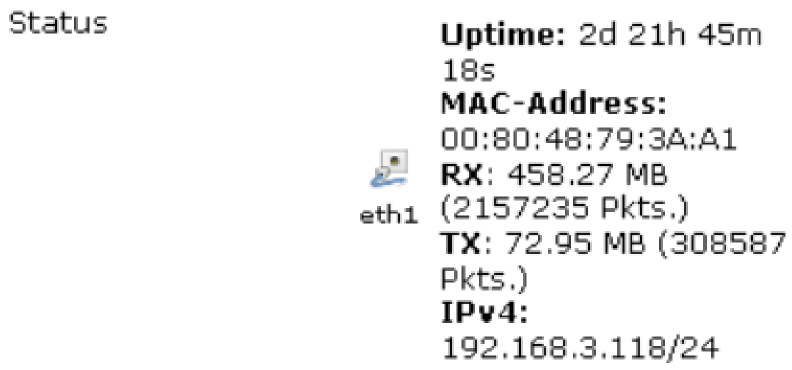
5.1 Interfaces – WAN

The *Network* → *Interfaces* → *WAN* page configures the interface for the WAN zone.

5.1.1 Common Configuration

General Setup

Status: Shows a summary of the interface for the WAN zone. This includes uptime, MAC address, bytes and packets received by the device, bytes and packets transmitted by the device, and its IPv4 address.



Status

eth1

Uptime: 2d 21h 45m 18s
MAC-Address: 00:80:48:79:3A:A1
RX: 458.27 MB (2157235 Pkts.)
TX: 72.95 MB (308587 Pkts.)
IPv4: 192.168.3.118/24

Figure 39: Status of the “eth1” interface of the WAN zone.

Protocol: Chooses between *DHCP client* (default), where the device obtains it IP address automatically, or Static address, where you can specify the device IP address. Other protocols are *PPTP*, *PPPoE*, and *L2TP*.

Protocol – Static address

IPv4 address: Sets the IP address of the device as seen from the WAN zone.

IPv4 netmask: Sets the subnet mask e.g. 255.255.255.0. The IP address and netmask together determine the subnet or network ID e.g.192.168.3.0/24. Two devices must be in the same subnet in order to establish a (Layer 2) link between them.

IPv4 gateway: Specifies the IP address of the remote router that allows the device's shell to gain internet access.

IPv4 broadcast: Specifies the IPv4 broadcast address, optional.

Use custom DNS servers: Configures the IP address of the DNS servers e.g. 165.21.100.88 for the SingNet DNS server in Singapore or 8.8.8.8 for the Google DNS server in the USA. The computers in the same subnet as this device can then set this device's IP address as their preferred DNS server to obtain the same DNS service.

Protocol – DHCP client

The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses automatically to client devices.

Hostname to send when requesting DHCP: Specifies the name of this device as seen by the remote DHCP server

Protocol – PTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over Transmission Control Protocol (TCP) and a Generic Routing Encapsulation (GRE) tunnel operating to encapsulate Point-to-Point Protocol (PPP) packets.

VPN Server: Specifies the IP address of the remote PPTP server for the virtual private network (VPN).

PAP/CHAP username: Sets the username for the Password Authentication Protocol (PAP) or the Challenge-Handshake Authentication Protocol (CHAP).

PAP/CHAP password: Sets the password for the PAP or CHAP.

Configure PPTP IP settings: Upon clicking the “Configure...” button, the PPTP *Common Configuration* page would be displayed. The protocol DHCP client or Static address can be selected. The corresponding options are explained within this section (*5.1.1 Common Configuration*).

Protocol – PPPoE

The Point-to-Point Protocol over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frames. Most DSL providers use PPPoE, which provides authentication, encryption, and compression.

The options *PAP/CHAP* username and *PAP/CHAP* pass*word* have been explained earlier.

Access Concentrator: Identifies the PPPoE server. Leave empty to autodetect.

Service Name: Specifies the PPPoE service name. The server will accept clients which send an initialization message with the service name that matches the server's configuration. Leave empty to autodetect.

Protocol – L2TP

The Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The options *PAP/CHAP* username and *PAP/CHAP* pass*word* have been explained earlier.

L2TP Server: Specifies the IP address of the remote L2TP server.

Configure L2TP IP settings: Upon clicking the “Configure...” button, the L2TP *Common Configuration* page would be displayed. The protocol DHCP client or Static address can be selected. The corresponding options are explained within this section *(5.1.1 Common Configuration)*

Advanced Settings

The following are options in the *Advanced Settings* section tab. Some of these options are shown, depending on the protocol being used.

Override MAC address: Allows you to specify a different MAC address other than the router's original MAC address. This is useful if the ISP uses the MAC address of a router to identify a customer. Suppose that the router needs to be replaced. The new router can take on the MAC address of the previous router in order to continue having internet access.

Override MTU: Sets the maximum transmission unit (MTU), the default being 1500 bytes. Unless, your ISP requires, it is not recommended to change this setting.

Use gateway metric: Allows you to specify a gateway metric. This acts as a cost for choosing the gateway when a connected device has to select between multiple available gateways. The gateway with the smallest metric is chosen.

Use broadcast flag: When sending DHCP requests, a client can indicate if it wants an answer in unicast or broadcast, by setting the broadcast flag. This is required for certain ISPs. Unchecked by default.

Use default gateway: Configures a default route. Checked by default.

Use DNS servers advertised by peer: Uses the DNS settings advertised by the DHCP server. Checked by default.

Client ID to send when requesting DHCP: Sets the identifier that may be required by the ISP or network administrator. If not stated, the MAC address of the client will be sent.

Vendor Class to send when requesting DHCP:Identifies the vendor of a DHCP client for the enhancement of vendor-specific DHCP functionality. The following three options are specific to the PPTP and PPPoE protocols:

LCP echo failure threshold: Sets the number of link control protocol (LCP) echo failures before the peer is presumed to be dead. Use 0 to ignore failures.

LCP echo interval: Specifies the interval in seconds to send LCP echo requests. This is only effective in conjunction with failure threshold.

Inactivity timeout: Sets the number of seconds of inactivity, after which the connection is closed. Use 0 to persist connection.

Physical Settings

Interface: Chooses which physical interface to use for the WAN zone. This can be the *Ethernet Adapter* “eth0” or “eth1” that corresponds to each of the two ports on the device for example. It could also be set as the *Wireless Network*. If there is a physical interface selected for the WAN zone, this can be referred to as the “NAT mode”, because network address translation occurs between the WAN zone and the LAN zone.

If *No Interface* is selected for the WAN zone, all interfaces would be within the LAN zone. This may also be referred to as the “Bridge Mode”

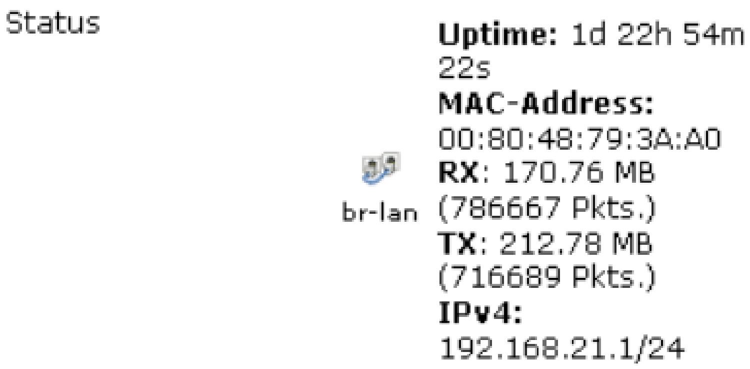
5.2 Interfaces – LAN

The *Network* → *Interfaces* → *WAN* page configures the interface for the WAN zone.

5.2.1 Common Configuration

General Setup

Status: Shows a summary of the current LAN port status, which includes uptime, MAC address, received bytes and packets, transmitted bytes and packets, and IPv4 address.



Status

br-lan

Uptime: 1d 22h 54m 22s
MAC-Address: 00:80:48:79:3A:A0
RX: 170.76 MB (786667 Pkts.)
TX: 212.78 MB (716689 Pkts.)
IPv4: 192.168.21.1/24

Figure 40: Status of the “br-lan” interface of the LAN zone.

Protocol: Chooses between *Static address*, where you can specify the device IP address, or *DHCP client*, where the device obtains it IP address automatically. *Static address* is necessary if other devices obtain internet connection through this device. *Static address* is also recommended if you wish to configure the device via the LuCI web interface.

Protocol – Static address

IPv4 address: Sets the IP address of the device e.g. 192.168.21.1, where you can access the router's configuration web page.

IPv4 netmask: Sets the subnet mask e.g. 255.255.255.0. The IP address and netmask together determine the subnet or network ID e.g. 192.168.21.0/24. Two devices must be in the same subnet in order to establish a (Layer 2) link between them.

IPv4 gateway: Specifies the IP address of the remote router that allows the device's shell to gain internet access.

IPv4 broadcast: Specifies the IPv4 broadcast address, optional.

Use custom DNS servers: Configures the IP address of the DNS servers e.g. 165.21.100.88 for the SingNet DNS server in Singapore or 8.8.8.8 for the Google DNS server in the USA. The computers in the same subnet as this device can then set this device's IP address as their preferred DNS server to obtain the same DNS service.

Protocol – DHCP client

The Dynamic Host Configuration Protocol (DHCP) is a standardized networking protocol used by servers on an IP network to allocate IP addresses automatically to client devices.

Hostname to send when requesting DHCP: Specifies the name of this device as seen by the remote DHCP server.

Advanced Settings

The following are options in the *Advanced Settings* section tab. Some of these options are shown, depending on the protocol being used.

Override MAC address: Allows you to specify a different MAC address other than the router's original MAC address. This is useful if the ISP uses the MAC address of a router to identify a customer. Suppose that the router needs to be replaced. The new router can take on the MAC address of the previous router in order to continue having internet access.

Override MTU: Sets the maximum transmission unit (MTU), the default being 1500 bytes. Unless, your ISP requires, it is not recommended to change this setting.

Use gateway metric: Allows you to specify a gateway metric. This acts as a cost for choosing the gateway when a connected device has to select between multiple available gateways. The gateway with the smallest metric is chosen.

Use broadcast flag: When sending DHCP requests, a client can indicate if it wants an answer in unicast or broadcast, by setting the broadcast flag. This is required for certain ISPs. Unchecked by default.

Use default gateway: Configures a default route. Checked by default.

Use DNS servers advertised by peer: Uses the DNS settings advertised by the DHCP server. Checked by default.

Client ID to send when requesting DHCP: Sets the identifier that may be required by the ISP or network administrator. If not stated, the MAC address of the client will be sent.

Vendor Class to send when requesting DHCP: Identifies the vendor of a DHCP client for the enhancement of vendor-specific DHCP functionality.

Physical Settings

Enable STP: Enables the Spanning Tree Protocol on this bridge. It is unchecked by default.

5.2.2 DHCP Server

This section allows you to configure the device as a DHCP server.

General Setup

Ignore interface: Disables DHCP for this interface. You should uncheck this to enable DHCP.

Start: Specifies the lowest leased address as offset from the network address, the default being *100.*

Limit: Sets the maximum number of leased addresses, the default being *150*.

Leasetime: States the expiry time of leased addresses, the default being *12h*.

Advanced Settings

Dynamic DHCP: Dynamically allocates DHCP addresses for clients. If disabled, only clients having static leases will be served. Checked by default.

Force: Forces DHCP on this network even if another server is detected, unchecked by default.

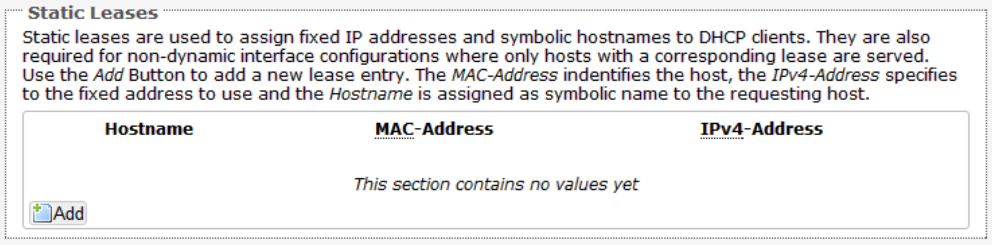
IPv4-Netmask: Overrides the netmask sent to clients. Normally it is calculated from the subnet that is served.

DHCP-Options: Defines additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients. Normally, connected devices would take this board's IP address as the default gateway. To set an alternative default gateway, add the DHCP option "3,192.168.2.3" for example. More information can be found in this link: http://wiki.openwrt.org/doc/uci/dhcp.

5.2.3 Static Leases

In this section, you can specify that a particular DHCP client obtain an IP address that you define. The MAC address of the client is required. Click the Add button to add a static

DHCP lease, then click Save & Apply to apply the changes.



Static Leases

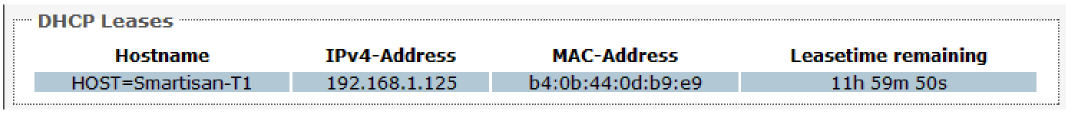
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the *Add* Button to add a new lease entry. The *MAC-Address* indentifies the host, the *IPv4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address

This section contains no values yet

Figure 41: Adding a static DHCP lease

The static DHCP lease shows up on the *Status* → *Overview* page if the client is active.



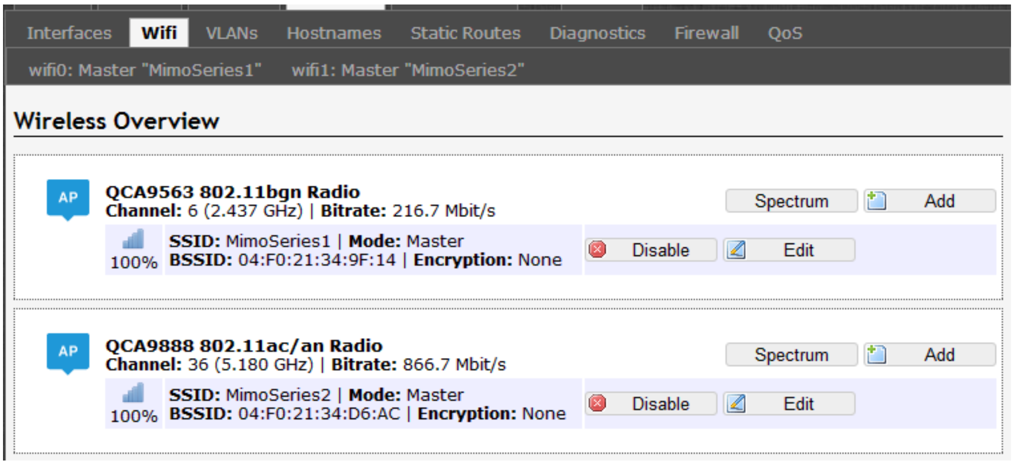
DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
HOST=Smartisan-T1	192.168.1.125	b4:0b:44:0d:b9:e9	11h 59m 50s

Figure 42: The static DHCP leases on the *Status* → *Overview* page

5.3 Wifi – Overview

Clicking on the *Network* → *Wifi* tab would bring you to the *Wireless Overview* page. This page shows the radios present on the device. These may include the on-board radio and the miniPCI/miniPCIe radio card. The wireless local area networks (WLANs) are displayed under each radio.



Wireless Overview

QCA9563 802.11bgn Radio
Channel: 6 (2.437 GHz) | **Bitrate:** 216.7 Mbit/s

100% **SSID:** MimoSeries1 | **Mode:** Master
BSSID: 04:F0:21:34:9F:14 | **Encryption:** None

QCA9888 802.11ac/an Radio
Channel: 36 (5.180 GHz) | **Bitrate:** 866.7 Mbit/s

100% **SSID:** MimoSeries2 | **Mode:** Master
BSSID: 04:F0:21:34:D6:AC | **Encryption:** None

Figure 43: The *Wireless Overview* page showing two radios

In Figure 43, two tabs are shown at the top, wifi0: Master “MimoSeries1” and wifi1: Master “MimoSeries2”. These correspond to the two radios shown below. The buttons are explained as follows.

Spectrum: Shows the Channel Scan Report and allows you to run the Interference Analyzer.

Add: Allows you to add virtual access points (VAPs) to the radio. By default, there is only one VAP on the radio. Each VAP corresponds to one network.

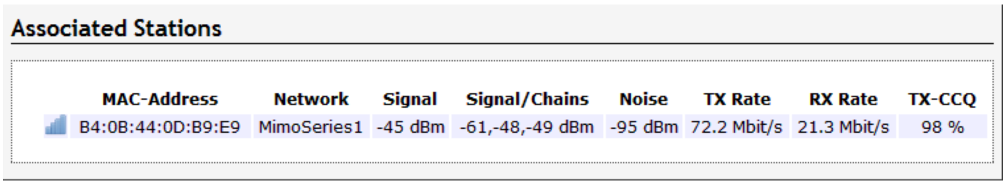
Enable: Enables the radio.

Disable: Disables the radio.

Edit: Brings you to the configuration page of the network. Clicking this button is equivalent to clicking the corresponding tab above e.g. wifi1: Master “MimoSeries1” for the radio with SSID given as “MimoSeries1”

5.3.1 Radio in AP Mode

When a radio is operating as an AP, the section for Associated Stations shows a list of stations connected to this device.



Associated Stations

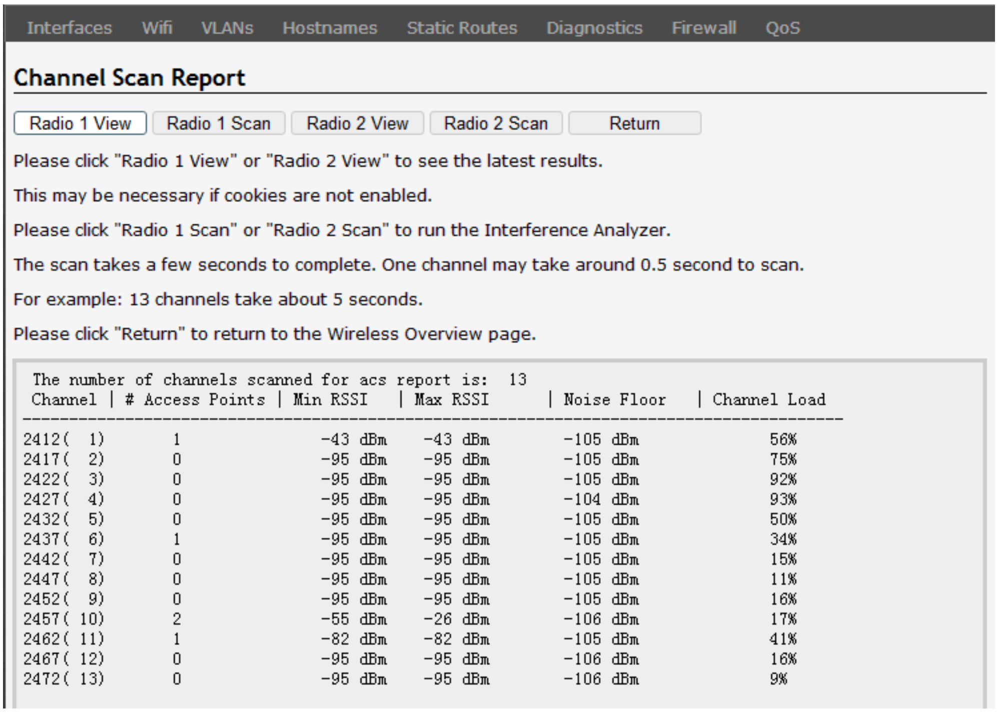
	MAC-Address	Network	Signal	Signal/Chains	Noise	TX Rate	RX Rate	TX-CCQ
📶	B4:0B:44:0D:B9:E9	MimoSeries1	-45 dBm	-61,-48,-49 dBm	-95 dBm	72.2 Mbit/s	21.3 Mbit/s	98 %

Figure 44: The *Associated Stations* are also shown on the *Wireless Overview* page

The MAC address, network name, received signal strength, noise power, transmit rate, receive rate, and transmission quality for each station are displayed.

5.3.2 Spectrum: Interference Analyzer

For a radio in AP mode, clicking the Spectrum button would bring up the Channel Scan Report.



Channel Scan Report

Please click "Radio 1 View" or "Radio 2 View" to see the latest results.

This may be necessary if cookies are not enabled.

Please click "Radio 1 Scan" or "Radio 2 Scan" to run the Interference Analyzer.

The scan takes a few seconds to complete. One channel may take around 0.5 second to scan.

For example: 13 channels take about 5 seconds.

Please click "Return" to return to the Wireless Overview page.

```
 The number of channels scanned for acs report is:  13
 Channel | # Access Points | Min RSSI   | Max RSSI      | Noise Floor   | Channel Load
-------------------------------------------------------------------------------------

2412(  1)      1               -43 dBm   -43 dBm       -105 dBm           56%
2417(  2)      0               -95 dBm   -95 dBm       -105 dBm           75%
2422(  3)      0               -95 dBm   -95 dBm       -105 dBm           92%
2427(  4)      0               -95 dBm   -95 dBm       -104 dBm           93%
2432(  5)      0               -95 dBm   -95 dBm       -105 dBm           50%
2437(  6)      1               -95 dBm   -95 dBm       -105 dBm           34%
2442(  7)      0               -95 dBm   -95 dBm       -105 dBm           15%
2447(  8)      0               -95 dBm   -95 dBm       -105 dBm           11%
2452(  9)      0               -95 dBm   -95 dBm       -105 dBm           16%
2457( 10)      2               -55 dBm   -26 dBm       -106 dBm           17%
2462( 11)      1               -82 dBm   -82 dBm       -105 dBm           41%
2467( 12)      0               -95 dBm   -95 dBm       -106 dBm           16%
2472( 13)      0               -95 dBm   -95 dBm       -106 dBm           9%
```

Figure 45: The Channel Scan Report

The button 'Radio 1 View' shows the number of neighbouring access points for each channel, the Min RSSI, Max RSSI, Noise Floor, and Channel Load.

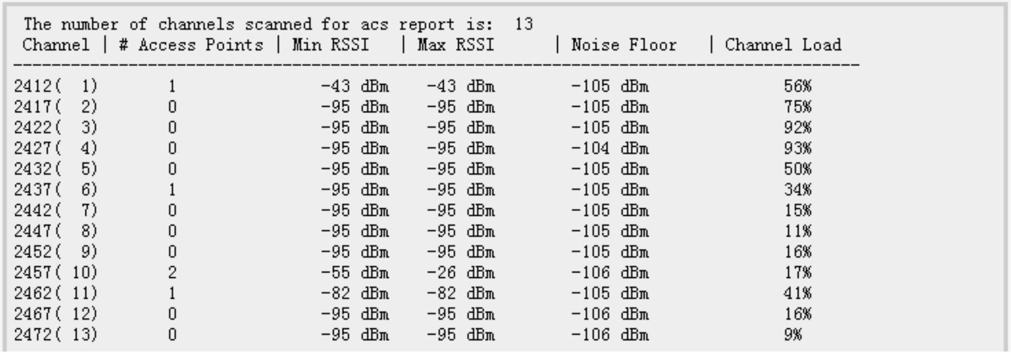
Min RSSI: Shows the minimum received signal strength indicator due to the neighbouring access points.

Max RSSI: Shows the maximum received signal strength indicator due to the neighbouring access points.

Noise Floor: Shows the level of the noise on the channel.

Channel Load: Shows how much the channel is utilized. A lower channel load denotes a channel with less interference. You can click 'Radio 1 Scan' to do the full channel scan again and get the latest results. The buttons for Radio 2 would be shown if Radio 2 is enabled on the device.

Return: Brings you back to the *Wireless Overview* page.

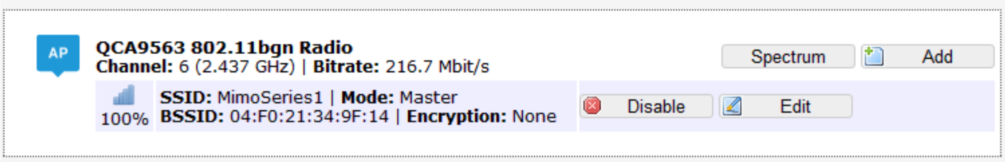


```
 The number of channels scanned for acs report is:  13
 Channel | # Access Points | Min RSSI    | Max RSSI      | Noise Floor   | Channel Load
-----------------------------------------------------------------------------------------
2412(  1)       1              -43 dBm    -43 dBm        -105 dBm              56%
2417(  2)       0              -95 dBm    -95 dBm        -105 dBm              75%
2422(  3)       0              -95 dBm    -95 dBm        -105 dBm              92%
2427(  4)       0              -95 dBm    -95 dBm        -104 dBm              93%
2432(  5)       0              -95 dBm    -95 dBm        -105 dBm              50%
2437(  6)       1              -95 dBm    -95 dBm        -105 dBm              34%
2442(  7)       0              -95 dBm    -95 dBm        -105 dBm              15%
2447(  8)       0              -95 dBm    -95 dBm        -105 dBm              11%
2452(  9)       0              -95 dBm    -95 dBm        -105 dBm              16%
2457( 10)       2              -55 dBm    -26 dBm        -106 dBm              17%
2462( 11)       1              -82 dBm    -82 dBm        -105 dBm              41%
2467( 12)       0              -95 dBm    -95 dBm        -106 dBm              16%
2472( 13)       0              -95 dBm    -95 dBm        -106 dBm              9%
```

Figure 46: A Channel Scan Report for the 5 GHz band.

5.3.3 Radio in Station Mode

A radio can operate as a Station. This can be set in the *Interface Configuration → General Setup → Mode* option, after clicking on the *Edit* button.



QCA9563 802.11bgn Radio
Channel: 6 (2.437 GHz) | **Bitrate:** 216.7 Mbit/s

100%
SSID: MimoSeries1 | **Mode:** Master
BSSID: 04:F0:21:34:9F:14 | **Encryption:** None

Figure 47: The Wireless Overview page showing a radio as a Client (station).

The following buttons are for a radio operating as a station.

Scan: Scans for available wireless networks. This button is available if the device is operating as a Station. You can then select the network to connect to.

Join Network: Associates this device with the selected wireless network

5.4 Wifi – Wireless Network

As mentioned earlier, clicking on the *Edit* button for a network would bring you to the configuration page. This page contains the sections *Device Configuration* and *Interface Configuration*.

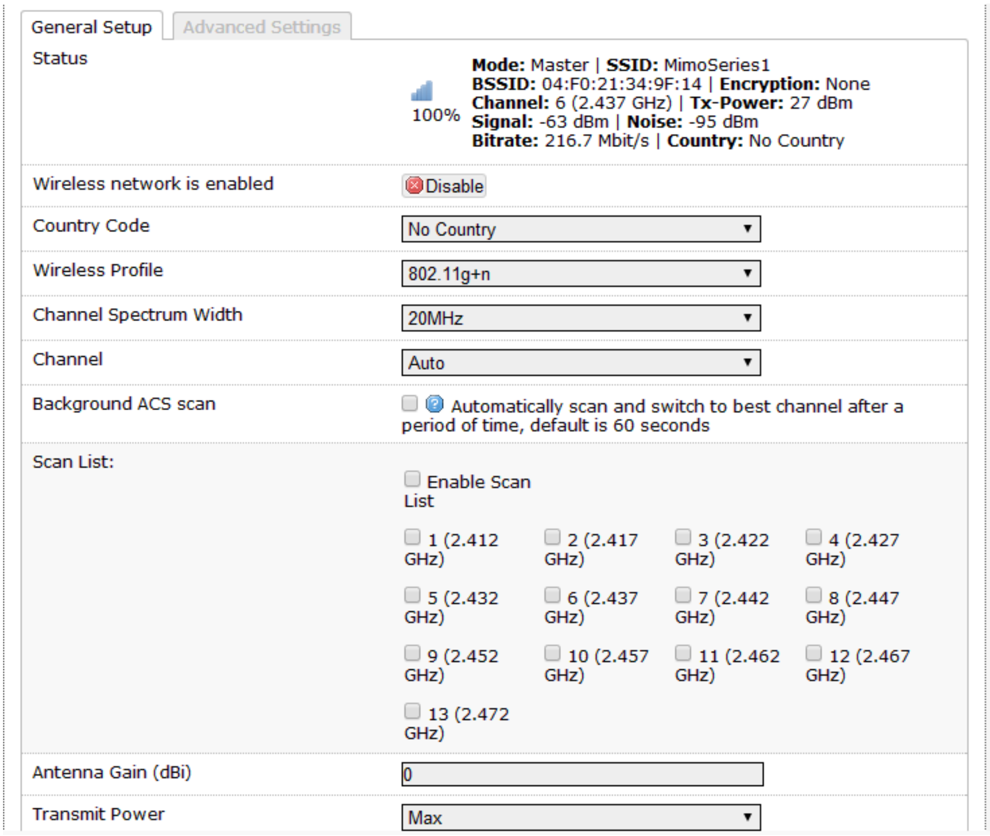
The *Device Configuration* section covers the physical settings of the radio hardware such as channel, transmit power, or antenna selection. These are shared among all defined wireless networks of the radio. Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

5.4.1 Radio in AP Mode

The *Device Configuration* section consists of the section tabs for General Setup and *Advanced Settings*.

General Setup

Status: Shows a summary of the wireless network.



General Setup | Advanced Settings

Status

100%

Mode: Master | **SSID:** MimoSeries1
BSSID: 04:F0:21:34:9F:14 | **Encryption:** None
Channel: 6 (2.437 GHz) | **Tx-Power:** 27 dBm
Signal: -63 dBm | **Noise:** -95 dBm
Bitrate: 216.7 Mbit/s | **Country:** No Country

Wireless network is enabled	Disable
Country Code	No Country ▾
Wireless Profile	802.11g+n ▾
Channel Spectrum Width	20MHz ▾
Channel	Auto ▾
Background ACS scan	□ Automatically scan and switch to best channel after a period of time, default is 60 seconds
Scan List:	□ Enable Scan List
	□ 1 (2.412 GHz) □ 2 (2.417 GHz) □ 3 (2.422 GHz) □ 4 (2.427 GHz) □ 5 (2.432 GHz) □ 6 (2.437 GHz) □ 7 (2.442 GHz) □ 8 (2.447 GHz) □ 9 (2.452 GHz) □ 10 (2.457 GHz) □ 11 (2.462 GHz) □ 12 (2.467 GHz) □ 13 (2.472 GHz)
Antenna Gain (dBi)	0
Transmit Power	Max ▾

Figure 48: The Wifi *Device Configuration* section

Enable: Enables the wireless network.

Disable: Disables the wireless network.

Country Code: Selects the country. Each country has its own transmit power and frequency regulations. To ensure regulatory compliance, you must select the country where the device is operating in. The transmit power levels for each channel are tuned accordingly.

Wireless Profile: Chooses the wireless standard used. 802.11a and 802.11g are older standards while 802.11n is a newer standard that offers higher data rates. The choice of *802.11g+n* is a combination of 802.11g and 802.11n, and operates in the 2.4 GHz frequency band. The choice of *802.11a+n* is a combination of 802.11a and 802.11n, and operates in the 5 GHz frequency band. The *802.11ac* is the latest standard that offers even higher data rates (up to 1300 Mbps) and it also operates in the 5 GHz frequency band.

Channel Spectrum Width: Selects whether *20 MHz* or *20/40 MHz* bands are used. A 40 MHz band has twice the throughput of a 20 MHz band. A smaller bandwidth may allow more devices to be connected. The *20/40 MHz* option allows both 20 and 40 MHz bands to be used. When the *802.11ac* wireless standard is used, the *20/40/80 MHz* band can be selected. An 80 MHz band can carry twice the amount of data of a 40 MHz band.

Channel: Chooses the frequency channel. The default setting of *Auto* is may be used. For an AP, it would select the channel with the least interference from other APs. For a station, it would automatically select the same channel as its AP. The frequency channel may also be manually selected. An AP and its station must have the same channel in order to communicate.

Obey Regulatory Power: Obeys the power regulations specified by each country. This would satisfy the legally permitted maximum for the equivalent isotropically radiated power

(EIRP) limits of the selected country, based on the specified *Antenna Gain (dBi)*. The result is that the maximum transmit power may be less than the capability of the radio. Once activated, a refresh of the webpage may be needed to show the settings correctly. If “No Country” is selected, this is not in use.

Antenna Gain (dBi): Represents the gain relative to an isotropic antenna. A higher antenna gain results in the transmit power more focused towards a certain direction. When *Obey Regulatory Power* is checked, the value of the antenna gain would be taken into account to limit the selectable transmit power, such that the EIRP limits of the country are satisfied.

Transmit Power (dBm): Limits the maximum transmit power of the card at that particular frequency, e.g. 4 dBm, 5 dBm, …, 22 dBm or “Max”. This is the power supplied to the antennas of the radio. The minimum transmit power values for the radios are:

- For 1-Chain: 1 dBm
- For 2-Chain: 4 dBm
- For 3-Chain: 6 dBm

The “Max” power depends on both the country and the frequency channel used.

Outdoor Channels: Limits the available channel frequency selections to 5500-5700 MHz if the country is in the European Union (EU). Based on the EU-Rule 2005/513/EC regulation, only this frequency band is allowed for outdoor use.

For non-EU countries, this is not in use.

Understanding the Maximum Transmit Power Calculation

The maximum transmit power calculation is illustrated with the following examples.

Example 1

- Country Code: US, Channel = 36
- Obey Regulatory Power is enabled
- Antenna Gain is 5dBi
- Transmit Power is 15dBm
- Outdoor Channels is disabled

In the US, Channel = 36 would mean the maximum power is 17dBm for EIRP. Transmit Power is 15dBm, so when adding Antenna Gain of 5dBi, it would be 20dBi, which would EXCEED the EIRP. Thus the “Max” transmit power of the card has to be 12dBm, so that when added with 5dBi, it would be 17dBm.

Example 2

- Country Code: US, Channel = 149
- Obey Regulatory Power is enabled
- Antenna Gain is 5dBi
- Transmit Power is 15dBm
- Outdoor Channels is disabled

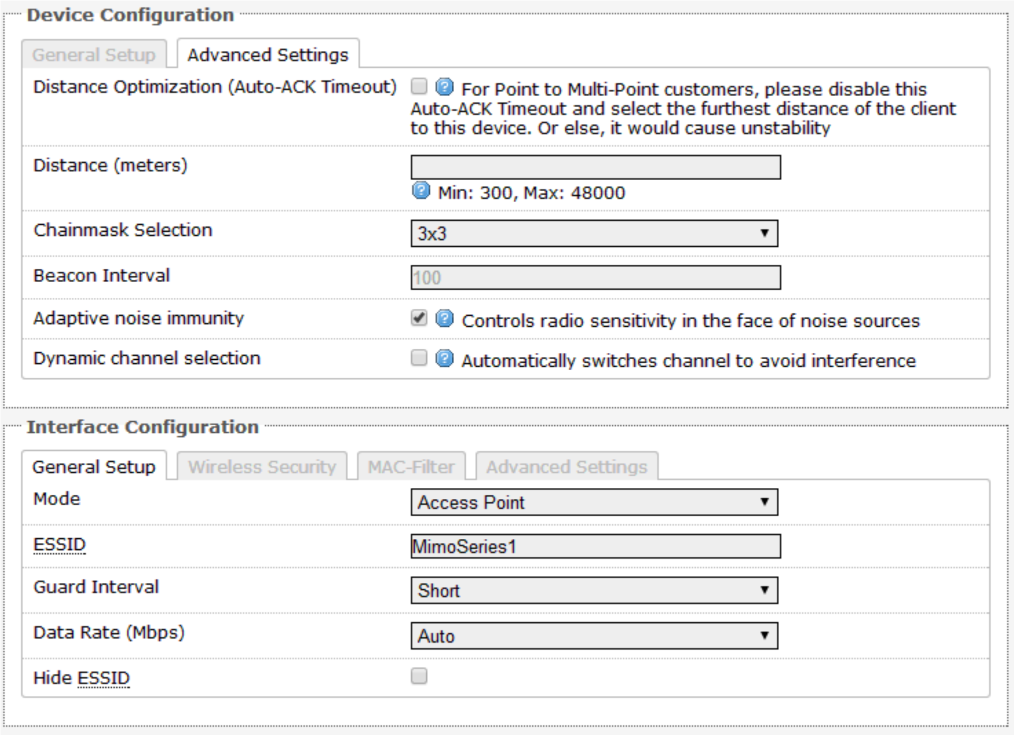
In the US, Channel = 149 would mean the maximum power is 30dBm for EIRP. Transmit Power is 15dBm, so when adding Antenna Gain of 5dBi, it would be 20dBm, which would NOT EXCEED the EIRP. Thus the “Max” transmit power of the card is 15dBm, as Antenna Gain has no effect.

Example 3

- Country Code: CZ, Channel = 100
- Obey Regulatory Power is enabled
- Antenna Gain is 5dBi
- Transmit Power is 15dBm
- Outdoor Channels is enabled

In the Czech Republic, Channel = 100 would mean the maximum power is 30dBm for EIRP. Transmit Power is 15dBm, when adding Antenna Gain of 5dBi, it would be 20dBi, which would NOT EXCEED the EIRP. Thus the “Max” transmit power of the card is 15dBm, as Antenna Gain has no effect.

Advanced Settings



Device Configuration

Distance Optimization (Auto-ACK Timeout)	□ For Point to Multi-Point customers, please disable this Auto-ACK Timeout and select the furthest distance of the client to this device. Or else, it would cause unstability
Distance (meters)	Min: 300, Max: 48000
Chainmask Selection	3x3
Beacon Interval	100
Adaptive noise immunity	☑ Controls radio sensitivity in the face of noise sources
Dynamic channel selection	□ Automatically switches channel to avoid interference

Interface Configuration

Mode	Access Point
ESSID	MimoSeries1
Guard Interval	Short
Data Rate (Mbps)	Auto
Hide ESSID	□

Figure 49: *Advanced Settings* for the Wifi *Device Configuration*

Distance Optimization (Auto-ACK Timeout): Determines the distance of the connected station from the AP and automatically adjusts the ACK timeout. This is disabled by default. If the stations are positioned over a wide area at different distances from the AP, it is recommended to disable this option to prevent the ACK timeout from fluctuating widely.

Distance (meters): Specifies the distance between the AP and the station, if the previous option is unchecked. Min: 300, Max: 12000 (80MHz), 24000 (40MHz), 48000 (20MHz). This value may be set to slightly more than the physical distance between the AP and the farthest station.

Chainmask Selection: Sets the antenna port selection on the radio. For example, 2x2 means that 2 antennas are being used.

Beacon Interval: Specifies the interval between beacon transmissions by the AP, in ms. A beacon is a frame broadcast by the AP to synchronize the wireless network. For the multiple VAP case, the beacons are transmitted evenly within this interval. Thus, if four VAPs are created and the beacon interval is 200 ms, a beacon will be transmitted from the radio portion every 50 ms, from each VAP in a round-robin fashion. The default value of the interval is 100 ms.

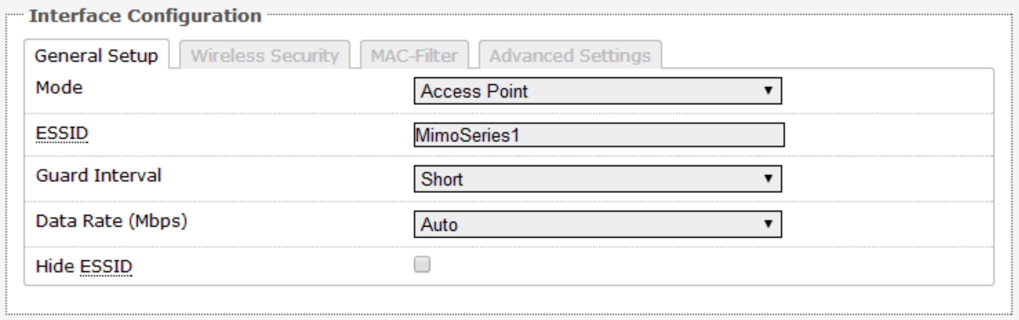
Adaptive noise immunity: Controls radio sensitivity in the face of noise sources. Adaptive noise immunity allows the AP to reject spurs and nonWLAN noise. An advantage is that the AP would have to spend less time decoding the signal, resulting in lower packet loss rate.

Dynamic channel selection: Automatically switches channel to avoid interference. Dynamic channel selection is feature to detect and avoid continuous wave (CW) interference. CW interference or spurs cause the noise floor to be high. This stops transmissions as well as causes receives to fail frequently. The noise floor is monitored by the calibration logic. When the noise floor is above a threshold, the AP is performs an automatic channel selection. It would disconnect from the stations (it would already have due to the interference) and move to a new channel. The stations are expected to re-associate with the AP on their own.

5.4.2 Interface Configuration

The *Interface Configuration* section contains the section tabs for *General Setup, Wireless Security, MAC-Filter,* and *Advanced Settings*.

General Setup



Mode	Access Point ▾
ESSID	MimoSeries1
Guard Interval	Short ▾
Data Rate (Mbps)	Auto ▾
Hide ESSID	☐

Figure 50: The Wifi *Interface Configuration* section

Mode: Selects whether the device is operating as an *Access Point* (AP) or a Station. Other options are *Access Point WDS* and *Station WDS.*

ESSID: Specifies the name or extended service set identifier (ESSID) of the wireless network as it is provided in the beacon message. The network name can be up to 32 characters in length and can contain spaces. When running in AP mode, it is the name of the network as advertised in the beacon message. In Station mode, it is the network name that the station associates with.

BSSID: Sets the MAC address of the AP. This option is available for a device operating as a station. This is useful because there can be multiple APs with the same ESSID. Setting the MAC address would prevent the station from roaming to other APs.

Guard Interval: Chooses between *Short* and *Long* guard intervals. Guard intervals are used to ensure that distinct transmissions do not interfere with one another. Data rate is improved in downlink and uplink if both AP and station use the Short Guard Interval.

Data Rate (Mbps): Selects the data rate or the modulation and coding scheme (MCS).

The default setting of *Auto* is recommended. The MCS and data rates are adjusted automatically depending on the wireless channel conditions.

Hide ESSID: Hides the network name (ESSID) from being broadcast publicly. (This option is for a device operating as an AP.)

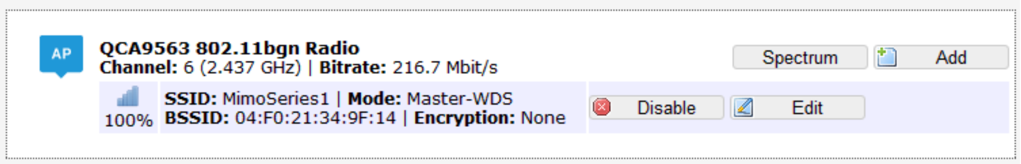
WDS

A Wireless Distribution System (WDS) is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them. The notable advantage of WDS over other solutions is it preserves the MAC addresses of client frames across links between access points.

WDS may also be considered a repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). However, with this method, throughput is halved for all clients connected wirelessly.

Setup for the WDS Modes

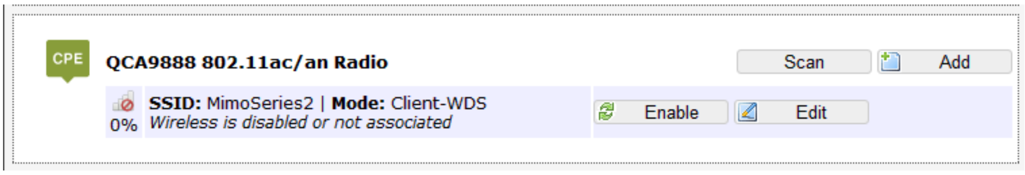
The wireless distribution system (WDS) allows the *Station WDS* to bridge wireless traffic transparently, providing the functionality of a repeater. The *Station WDS* is a transparent client and would need to associate with an *AP WDS.* The WDS protocol is not defined as a standard so there may be compatibility issues between devices from different vendors. The following figures show an example of a setup.



QCA9563 802.11bgn Radio
Channel: 6 (2.437 GHz) | **Bitrate:** 216.7 Mbit/s

100% **SSID:** MimoSeries1 | **Mode:** Master-WDS
BSSID: 04:F0:21:34:9F:14 | **Encryption:** None

Figure 51: The first router is set to the *AP WDS* mode



QCA9888 802.11ac/an Radio

0% **SSID:** MimoSeries2 | **Mode:** Client-WDS
Wireless is disabled or not associated

Figure 52: The second router is set to the *Station WDS* mode

Multiple stations or *Stations WDS* can connect to an *AP WDS*. In Figure 52, the *Add* button creates a virtual access point (VAP) on the second router. You should choose *AP WDS* mode for the VAP's wireless network e.g. "MimoSeries2" so that devices in *Station WDS* mode can connect to this network. The pair of *Station WDS* and *AP WDS* on the same board extends the wireless coverage. If the board has two radios, one onboard and one card radio, one radio can be the *Station WDS* and the other radio can be the *AP WDS*. Therefore the *Station WDS* with *AP WDS* on the same board functions as a repeater.

In the non-WDS mode, the *Station* translates all the packets that pass through it to its own MAC address, thus resulting in a lack of transparency. A consequence is that the ARP table of the access point would show the MAC address of the Station assigned to IP addresses of both the Station and the computer connected to it.

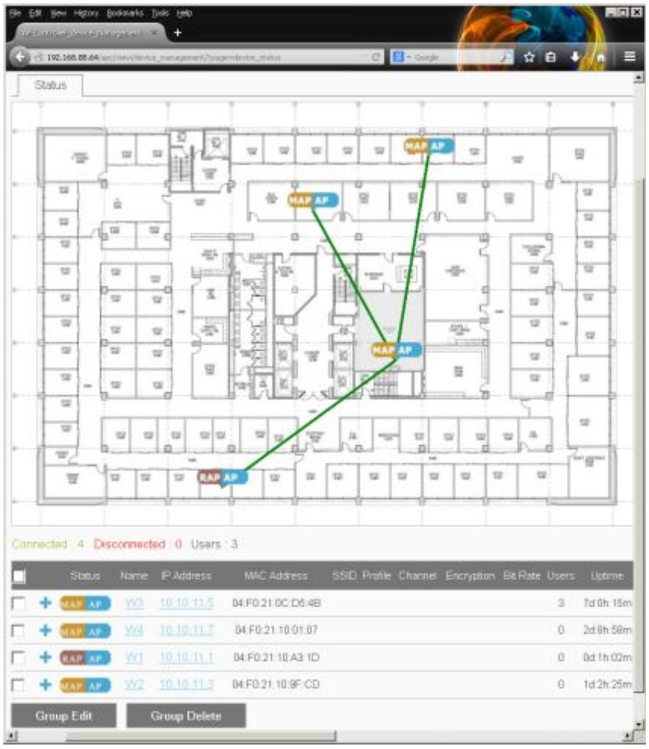
Mesh

A mesh network can be set up using HenrichWRT APs. Redundancy is achieved because if one AP dies, the other APs would automatically link up and calculate the most efficient path.

For the WDS described earlier, the topology is fixed, while for the mesh network, the topology is determined automatically in real-time.

A HenrichWRT AP can be configured as one of the following three mesh modes:

- Root AP (RAP)
- Mesh AP (MAP)
- Root AP + Router Client (RRC)



Connected : 4 Disconnected : 0 Users : 3

☐		Status	Name	IP Address	MAC Address	SSID	Profile	Channel	Encryption	Bit Rate	Users	Uptime
☐	+	MAP AP	W3	10.10.11.5	04:F0:21:0C:D6:4B						3	7d:0h:15m
☐	+	MAP AP	W4	10.10.11.7	04:F0:21:10:01:07						0	2d:8h:58m
☐	+	RAP AP	W1	10.10.11.1	04:F0:21:10:A3:1D						0	0d:1h:02m
☐	+	MAP AP	W2	10.10.11.3	04:F0:21:10:9F:CD						0	1d:2h:25m

Figure 53: APc web page showing an RAP connected to 3 MAPs in a mesh network

RAP

An RAP is connected to the Internet or main network by a wired LAN connection and broadcasts a wireless mesh signal.

MAP

MAPs connect wirelessly in a mesh configuration and at least one MAP connects to an RAP.

This RAP functions like a gateway for the MAPs to connect to the Internet network.

A mesh network can have multiple RAPs.

RRC

Suppose that you already have an existing wireless router without the mesh capability, and already broadcasting on the same channel that you would use for the mesh. An RAP just beside this router would introduce an unnecessary wireless network. In this case, you can use an RRC placed some distance away.

An RRC functions as a station associated with the wireless network of the existing router. It then broadcasts the wireless mesh signal just like an RAP.

A mesh network can be set up using the AP Controller (APc). Please refer to the APc user manual for the instructions. Otherwise, the steps to configure the mesh APs using the APs' LuCI web page are explained in the following sections.

Steps to Set Up a Mesh Network

In a mesh network, all the APs have to use the same wireless profile (e.g. 802.11a+n), channel (e.g. 149), spectrum width (e.g. 20/40 MHz), and encryption (e.g. WPA/WPA2-PSK).

RAP Configuration

The LAN/WAN Settings and the Wireless Settings are described in the following subsections.

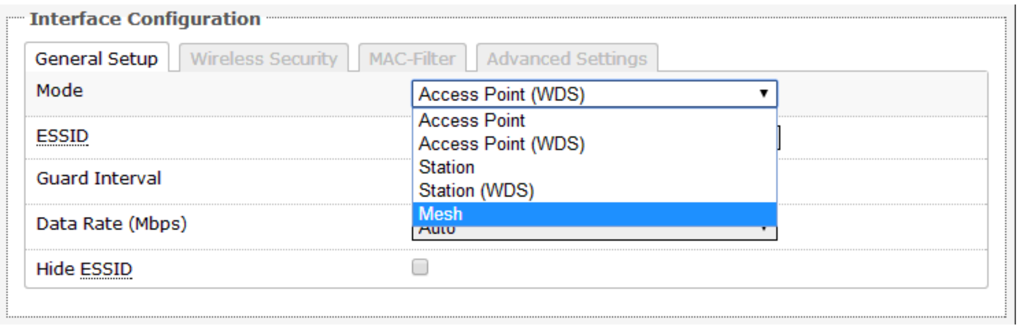
LAN/WAN Settings

For this RAP to act as a router (NAT mode), add in a WAN interface. (Refer to Section 5.1.1 Common Configuration > Physical Settings). If this RAP is to act as a bridge to the network, just leave the network settings as it is.

Wireless Settings

Click on Network > Wifi and click the "Edit" button for the radio to be used for the mesh. Alternatively, click on the SSID name on the Status page to go straight to the wireless settings.

In the Interface Configuration > General Setup tab, please select "Mesh" for the "Mode" option.



Interface Configuration

Mode: Access Point (WDS)

ESSID

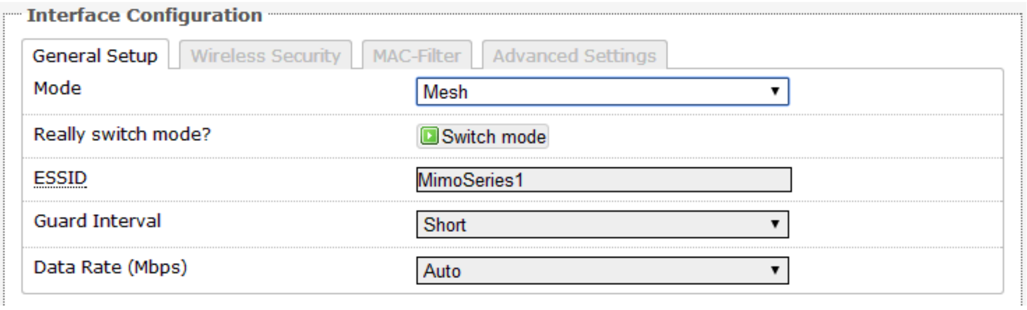
Guard Interval

Data Rate (Mbps)

Hide ESSID ☐

Figure 54: Please select "Mesh" for the "Mode" option.

You would be prompted with the "Really switch mode?" option. Please click "Switch mode".



Interface Configuration

Mode: Mesh

Really switch mode? Switch mode

ESSID: MimoSeries1

Guard Interval: Short

Data Rate (Mbps): Auto

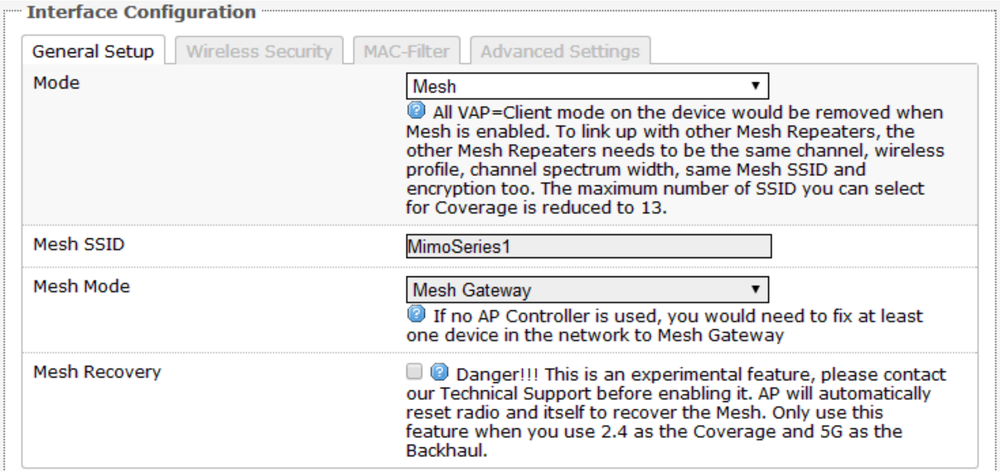
Figure 55: Please click "Switch mode".

You would then see the following options.

Mesh ID: The default Mesh ID created is "meshid". Key in the Mesh ID that would identify this mesh. All the mesh APs would be linked by this common Mesh ID.

Mesh Mode: The default Mesh Mode is "Mesh AP". The available options are

- Mesh AP (MAP)
- Root AP (RAP)
- Root AP + Router Client (RRC)



Mode: Mesh
All VAP=Client mode on the device would be removed when Mesh is enabled. To link up with other Mesh Repeaters, the other Mesh Repeaters needs to be the same channel, wireless profile, channel spectrum width, same Mesh SSID and encryption too. The maximum number of SSID you can select for Coverage is reduced to 13.

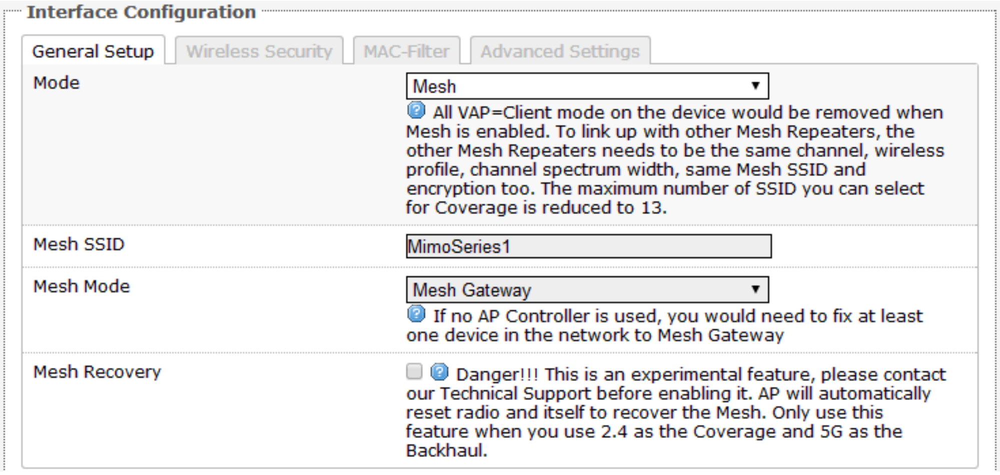
Mesh SSID: MimoSeries1

Mesh Mode: Mesh Gateway
If no AP Controller is used, you would need to fix at least one device in the network to Mesh Gateway

Mesh Recovery: □ Danger!!! This is an experimental feature, please contact our Technical Support before enabling it. AP will automatically reset radio and itself to recover the Mesh. Only use this feature when you use 2.4 as the Coverage and 5G as the Backhaul.

Figure 56: The default Mesh ID and Mesh Mode options.

For this AP, you would set it as an RAP. Following that, please click “Save & Apply”.



Mode: Mesh
All VAP=Client mode on the device would be removed when Mesh is enabled. To link up with other Mesh Repeaters, the other Mesh Repeaters needs to be the same channel, wireless profile, channel spectrum width, same Mesh SSID and encryption too. The maximum number of SSID you can select for Coverage is reduced to 13.

Mesh SSID: MimoSeries1

Mesh Mode: Mesh Gateway
If no AP Controller is used, you would need to fix at least one device in the network to Mesh Gateway

Mesh Recovery: □ Danger!!! This is an experimental feature, please contact our Technical Support before enabling it. AP will automatically reset radio and itself to recover the Mesh. Only use this feature when you use 2.4 as the Coverage and 5G as the Backhaul.

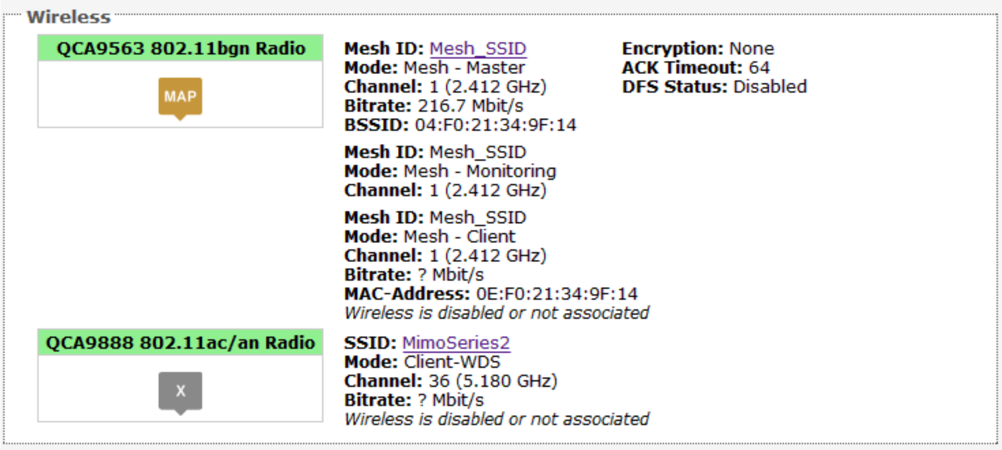
Figure 57: Setting the Mesh ID and the Mesh Mode options.

Next, please go to the “Wireless Security” tab to set the wireless encryption (e.g. WPA/WPA2-PSK).

After that, you may set up additional wireless networks to provide coverage.

You could create an additional wireless network on the same radio as the mesh network by adding a virtual AP (VAP).

You could also have a wireless network on the other radio to provide coverage for a different wireless profile (e.g. 802.11g+n).



Wireless

QCA9563 802.11bgn Radio

Mesh ID: Mesh_SSID
Mode: Mesh - Master
Channel: 1 (2.412 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Mesh ID: Mesh_SSID
Mode: Mesh - Monitoring
Channel: 1 (2.412 GHz)

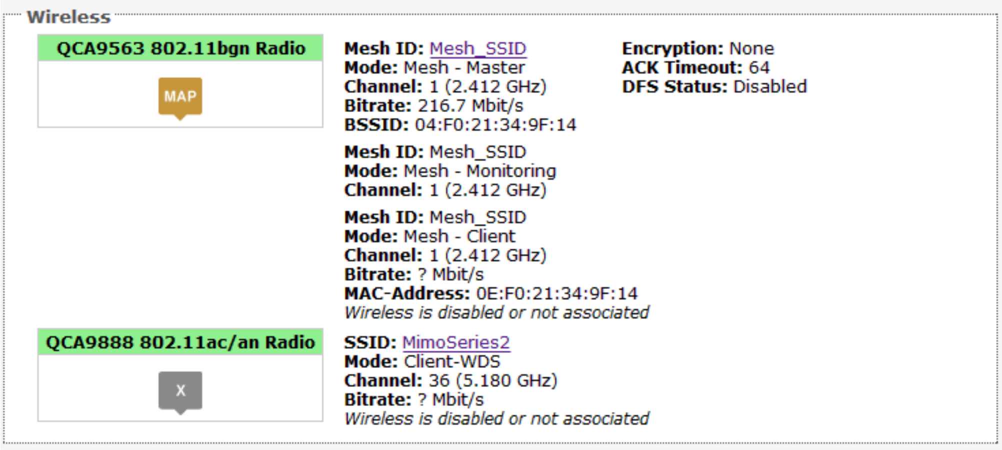
Mesh ID: Mesh_SSID
Mode: Mesh - Client
Channel: 1 (2.412 GHz)
Bitrate: ? Mbit/s
MAC-Address: 0E:F0:21:34:9F:14
Wireless is disabled or not associated

QCA9888 802.11ac/an Radio

SSID: MimoSeries2
Mode: Client-WDS
Channel: 36 (5.180 GHz)
Bitrate: ? Mbit/s
Wireless is disabled or not associated

Figure 58: The Status > Overview page of an RAP

The VAPs can be seen in the Network > Wifi page.



Wireless

QCA9563 802.11bgn Radio

Mesh ID: Mesh_SSID
Mode: Mesh - Master
Channel: 1 (2.412 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Mesh ID: Mesh_SSID
Mode: Mesh - Monitoring
Channel: 1 (2.412 GHz)

Mesh ID: Mesh_SSID
Mode: Mesh - Client
Channel: 1 (2.412 GHz)
Bitrate: ? Mbit/s
MAC-Address: 0E:F0:21:34:9F:14
Wireless is disabled or not associated

QCA9888 802.11ac/an Radio

SSID: MimoSeries2
Mode: Client-WDS
Channel: 36 (5.180 GHz)
Bitrate: ? Mbit/s
Wireless is disabled or not associated

Figure 59: The Network > Wifi page of an RAP

The RAP is now configured.

RRC Configuration

The "Router Client" is to connect to another router that has wireless connectivity. Mesh networks can then expand the connectivity using wireless instead of using cables.

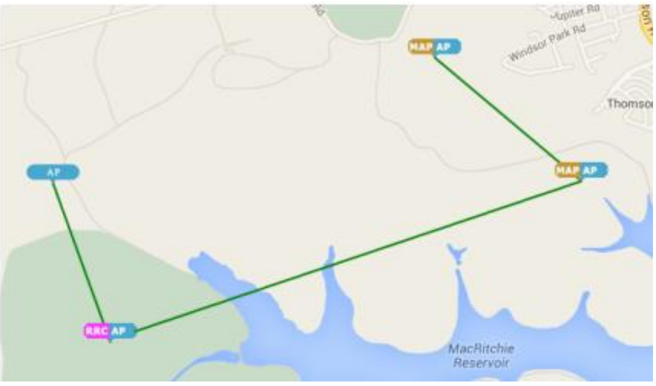


Figure 60: An existing AP is connected to an RRC
which is in turn connected to 2 MAPs

This AP should not have any WAN interfaces. That is, it is operating in bridge mode.

In the Network > Wifi > Interface Configuration > General Setup tab, please select

"Mesh" for the "Mode" option.

You would be prompted with the "Really switch mode?" option. Please click "Switch mode".

You should set the following options.

Mesh ID: The default Mesh ID created is "meshid". Key in the Mesh ID that would identify this mesh. All the mesh APs would be linked by this common Mesh ID.

Mesh Mode: This should be Root AP + Router Client (RRC).

Please click "Save & Apply".

Next, please go to the "Wireless Security" tab to set the wireless encryption (e.g. WPA/WPA2-PSK).

After that, you may set up additional wireless networks to provide coverage.

The steps are the same as described in the previous section for the RAP.

This RRC is now configured.

MAP Configuration

Now, disconnect your PC's LAN cable from the RAP (or RRC) and connect it to an AP that would function as an MAP.

This AP should not have any WAN interfaces. That is, it is operating in bridge mode.

Based on the wireless profile, channel, and spectrum width you had decided earlier, apply these settings to the radio that you would use for the mesh.

In the Network > Wifi > Interface Configuration > General Setup tab, please select "Mesh" for the "Mode" option.

You would be prompted with the "Really switch mode?" option. Please click "Switch mode".

You should set the following options.

Mesh ID: Please use the same Mesh ID as the RAP.

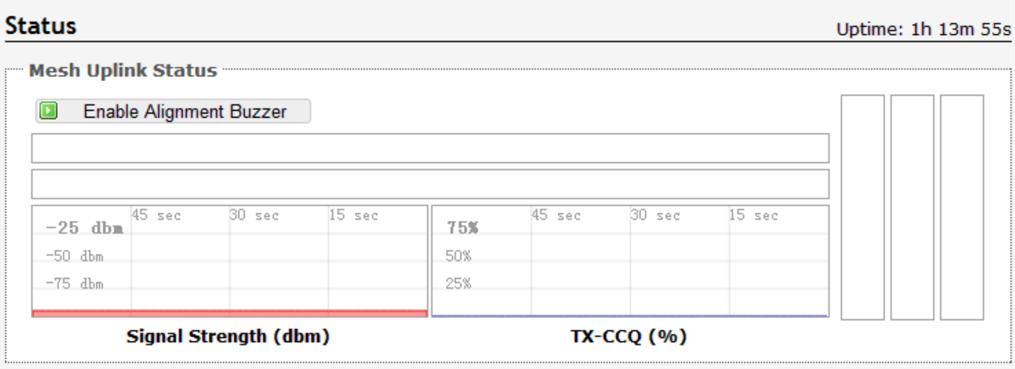
Mesh Mode: This should be Mesh AP (MAP).

Please click "Save & Apply".

Next, please go to the "Wireless Security" tab to set the wireless encryption (e.g. WPA/WPA2-PSK).

After that, you may set up additional wireless networks to provide coverage.

The steps are the same as for the RAP.



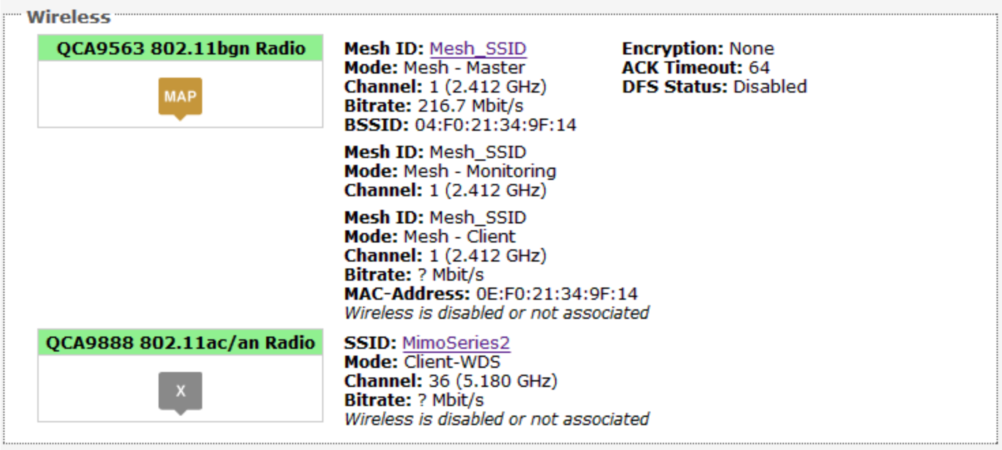
Status

Uptime: 1h 13m 55s

Mesh Uplink Status

Figure 61: The Status > Overview page of an MAP

The VAPs can be seen in the Network > Wifi page.



Mesh ID: Mesh_SSID
Mode: Mesh - Master
Channel: 1 (2.412 GHz)
Bitrate: 216.7 Mbit/s
BSSID: 04:F0:21:34:9F:14

Encryption: None
ACK Timeout: 64
DFS Status: Disabled

Mesh ID: Mesh_SSID
Mode: Mesh - Monitoring
Channel: 1 (2.412 GHz)

Mesh ID: Mesh_SSID
Mode: Mesh - Client
Channel: 1 (2.412 GHz)
Bitrate: ? Mbit/s
MAC-Address: 0E:F0:21:34:9F:14
Wireless is disabled or not associated

SSID: MimoSeries2
Mode: Client-WDS
Channel: 36 (5.180 GHz)
Bitrate: ? Mbit/s
Wireless is disabled or not associated

Figure 62: The Network > Wifi page of an MAP

This MAP is now configured.

You would then repeat the same process to configure all the MAPs.

Potential Network Looping and Solution

If there are network loops, you may see the error message on the serial console of the root AP: `br-lan: received packet on ath1 withown address as source address`

Also, you would also not be able to ping to the RAP from your PC.

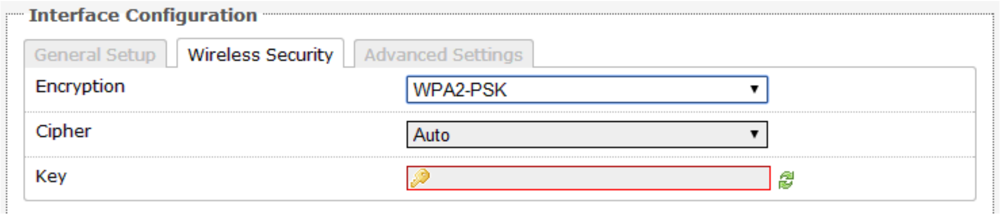
This could happen if the AP was connected by a LAN cable to the network and then the mesh was enabled on the AP.

Once you see this, please disconnect the MAPs from the wired LAN network.

Connecting to the Mesh Network

Once the RAP and MAPs have been configured, devices can now connect to the wireless networks that provide coverage. The APs in the mesh network can also be monitored and managed with an AP Controller (APc).

Wireless Security



Encryption	WPA2-PSK
Cipher	Auto
Key	

Figure 63: Setting the *Wireless Security* for the Wifi Interface.

Encryption: Chooses between No Encryption (open) and the following encryptions: WEP Open System, WEP Shared Key, WPA-PSK, WPA2-PSK, WPAPSK/WPA2-PSK Mixed Mode, WPA-EAP, and WPA2- EAP

WEP

Wired Equivalent Privacy (WEP) is the oldest and least secure encryption algorithm. Stronger encryption using WPA or WPA2 should be used where possible. The WEP option may be removed from the future releases of the firmware.

For the WEP Open System and WEP Shared Key encryptions, you can specify up to 4 keys and only 1 would be used at a time. We have the following options:

Used Key Slot: Chooses between Key #1 to Key #4.

Key #1: Specifies a string of characters to be used as the password. It may consist of 5 ASCII characters or 10 HEX characters, implying a 64-bit WEP key length. Otherwise, it may consist of 13 ASCII or 26 HEX characters, implying a 128-bit key length.

Key #2, #3, and #4: Similar to Key #1.

WPA or WPA2 with PSK

Wifi protected access (WPA) is a stronger encryption than WEP.

Furthermore, WPA2 was developed to strengthen the security of WPA and is stronger than WPA and WEP.

For *WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK* Mixed Mode encryptions, we have the following options.

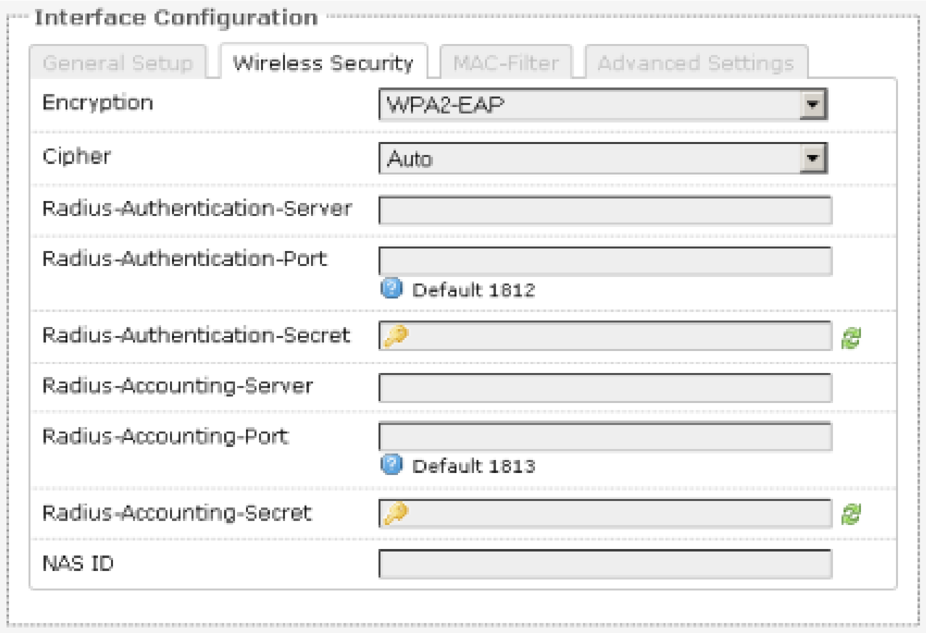
Cipher: Can be set to *Auto, CCMP (AES),* or *TKIP* and *CCMP (AES).* The Temporal Key Integrity Protocol (TKIP) was developed as a temporary replacement for WEP. The Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) is based on the Advanced Encryption Standard (AES) and is the most secure protocol.

Key: The pre-shared key (PSK) is the password for the wireless network. This may consist of 8 to 63 ASCII characters.

WPA or WPA2 with EAP

The Extensible Authentication Protocol (EAP) is encapsulated by the IEEE 802.1X authentication method. IEEE 802.1X is equivalent to EAP over LAN or WLAN. Enterprise networks commonly use this authentication method.

WPA or WPA2 with EAP (AP Mode)



Encryption	WPA2-EAP
Cipher	Auto
Radius-Authentication-Server	
Radius-Authentication-Port	Default 1812
Radius-Authentication-Secret	
Radius-Accounting-Server	
Radius-Accounting-Port	Default 1813
Radius-Accounting-Secret	
NAS ID	

Figure 64: Encryption options for WPA-EAP or WPA2-EAP in AP mode.

Cipher: Can be set to *Auto, CCMP (AES),* or *TKIP* and *CCMP (AES).*

Radius-Authentication-Server: Specifies the IP address of the RADIUS authentication server.

Radius-Authentication-Port: Sets the port number for the RADIUS authentication server. Normally, the port number is 1812.

Radius-Authentication-Secret: Configures the password for the authentication transaction.

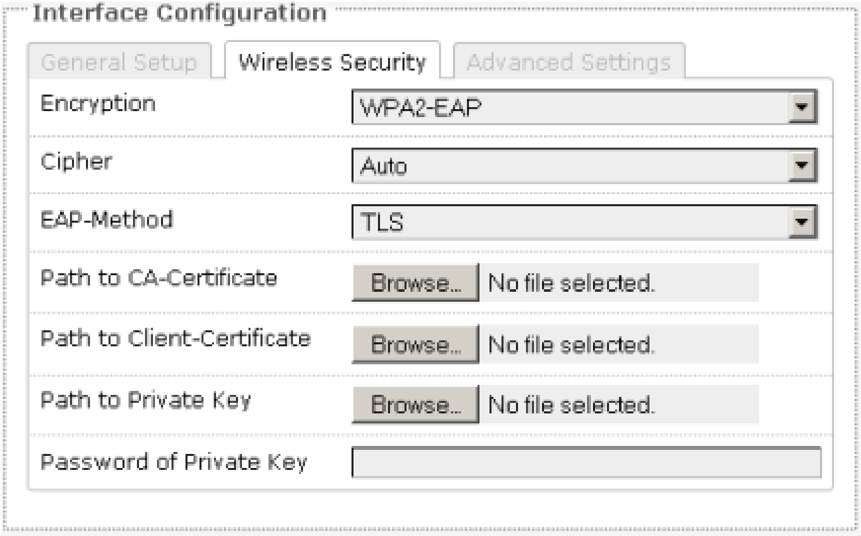
Radius-Accounting-Server: Specifies the IP address of the RADIUS accounting server.

Radius-Accounting-Port: Sets the port number for the RADIUS accounting server. Normally, the port number is 1813.

Radius-Accounting-Secret: Configures the password for the accounting transaction.

NAS ID: Specifies the identity of the network access server (NAS).

WPA or WPA2 with EAP (Station Mode)



Encryption: WPA2-EAP

Cipher: Auto

EAP-Method: TLS

Path to CA-Certificate: No file selected.

Path to Client-Certificate: No file selected.

Path to Private Key: No file selected.

Password of Private Key:

Figure 65: Encryption options for WPA-EAP or WPA2-EAP in Station mode

Cipher: Can be set to *Auto, CCMP (AES),* or *TKIP* and *CCMP (AES).*

EAP-Method: The authentication protocol can be set to Transport Layer Security *(TLS),* Tunneled TLS *(TTLS),* or Protected EAP *(PEAP).*

Path to CA-Certificate: Selects the file for the CA certificate.

Path to Client-Certificate: Selects the file for the client certificate.

Options for TLS as the EAP method

Path to Private Key: Selects the file for the private key.

Password of Private Key: Configures the password for the private key.

Options for TTLS or PEAP as the EAP method

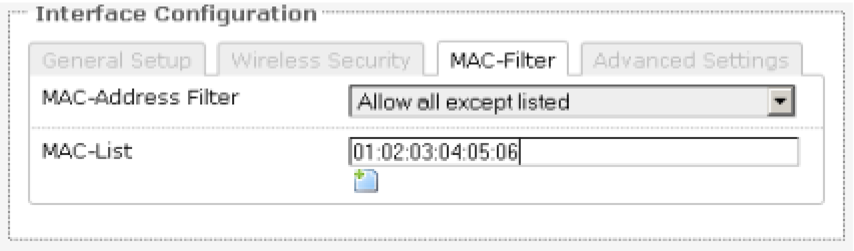
Authentication: Selects the authentication method used by the AP, e.g. PAP, CHAP, MSCHAP, or MSCHAPV2.

Identity: Sets the identity used by the supplicant for EAP authentication

Password: Sets the password used by the supplicant for EAP authentication.

MAC-Filter

This section tab is only available for a device operating as an AP



Interface Configuration

MAC-Address Filter: Allow all except listed

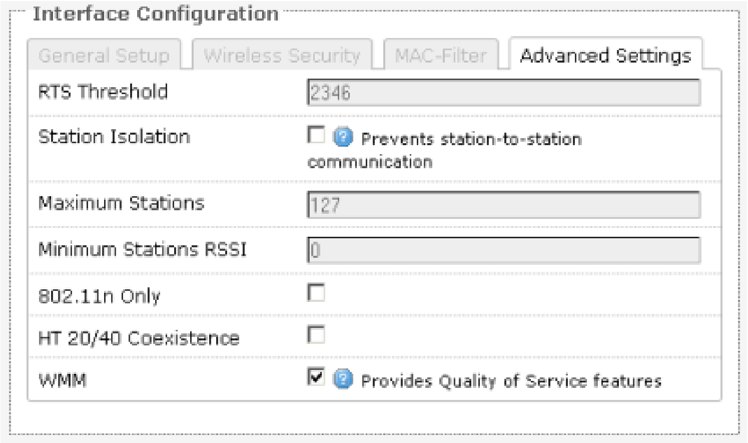
MAC-List: 01:02:03:04:05:06

Figure 66: Configuring the *MAC-Filter* for a Wifi AP

MAC-Address Filter: Lets you allow only devices with the listed MAC address to associate with this AP, or lets you block devices with the listed MAC address.

MAC-List: Adds the MAC address of the remote device to either block or allow

Advanced Settings



Interface Configuration

RTS Threshold: 2346

Station Isolation: □ Prevents station-to-station communication

Maximum Stations: 127

Minimum Stations RSSI: 0

802.11n Only: □

HT 20/40 Coexistence: □

WMM: ☑ Provides Quality of Service features

Figure 67: *Advanced Settings* for the Wifi Interface

RTS Threshold: Sets the threshold for the packet size above which the request to send (RTS) mechanism is used. The default is 2346 octets. There is a trade-off to consider when setting this parameter. On the one hand, using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth, and therefore reducing the throughput of the network packet. On the other hand, when more RTS packets are sent, the system recovers faster from interference or collisions. This is useful in a heavily loaded network, or a wireless network with high electromagnetic interference.

Station Isolation: Prevents station-to-station communication, unchecked by default. When Station Isolation is disabled, wireless clients can communicate with one another normally by sending traffic through the AP. When Station Isolation is enabled, the AP blocks communication between wireless clients on the same AP.

Maximum Stations: Specifies the maximum number of associated stations, the default being 127.

Minimum Stations RSSI: Sets the minimum received signal strength indicator for a station to be associated. The default value of 0 means that the AP would allow a station to associate independent of its RSSI.

802.11n Only: Forces the device to use only the IEEE802.11n standard, unchecked by default.

HT 20/40 Coexistence: Allows the network to use both 20 MHz and 40 MHz bands. Required on AP side primarily to support co-existence. The station can also send intolerant bit status to AP to signal use of 20 MHz channel. The station will follow the AP's channel bonding and channel switching HT 20/40 mechanism. Disabling this setting forces the use of 40 MHz bandwidth/channel bonding, and results in high data rate.

WMM: Provides Quality of Service (QoS) features, checked by default. Wireless multimedia enables the classification of the network traffic into 4 main types, voice, video, best effort, and background, in decreasing order of priority. Higher priority traffic has a higher transmission opportunity and would have to wait less time to transmit. As a result, an existing video stream would not be interrupted by additional background processes.

5.5 VLANs

A local area network (LAN) can be divided into multiple distinct virtual LANs (VLANs) with the use of VLAN switches. This improves the management and security of the network. The broadcast domain of a device on a VLAN is confined to all devices on
the same VLAN.

The next section describes the options available on the web page.

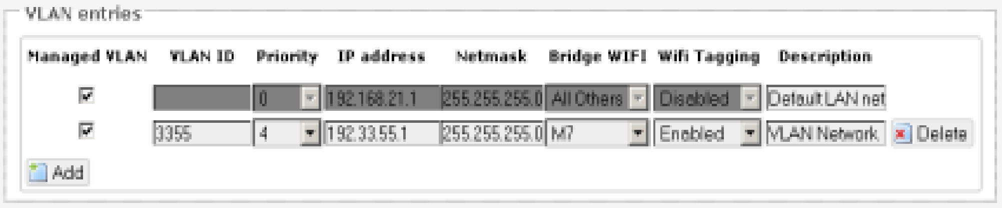
Following that, some scenarios that use the HenrichWRT VLAN Management and VLAN Ethernet Trunk are explained in detail.

5.5.1 Options

The *Network* → *VLAN* page contains the sections for VLAN Management and *VLAN Ethernet Trunk.*

VLAN Management

The *VLAN Management* section controls individual VLANs according to the IEEE802.1Q standards. Within the subsection for VLAN entries, each row represents one VLAN ID



VLAN entries

Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIFI	Wifi Tagging	Description	
☑		0	192.168.21.1	255.255.255.0	All Others	Disabled	Default LAN net	
☑	3355	4	192.33.55.1	255.255.255.0	M7	Enabled	VLAN Network	Delete

Figure 68: *VLAN* entries in the *VLAN Management* section

The first row is given by default. It is the native or untagged VLAN.

Add: Inserts a new row corresponding to a new VLAN. The *IP* address field should be distinct for different devices.

Managed VLAN: Allows computers on this VLAN to access the device's configuration web page.

VLAN ID: Specifies the identifier for the VLAN. It is an integer from 2 to 4094.

Priority: Chooses the priority for transmitting packets, which is IEEE802.1D compatible. This is a number from 0 to 7. The number 7 represents the highest priority.

IP address: Sets the IP address of the router as seen by other devices on this VLAN.

Netmask: States the netmask of the subnet defined by this VLAN.

Bridge WIFI: Selects the wireless network for which its interface would be bridged to the tagged VLAN Ethernet interface. The choice *All Others* would select all other wireless networks that are currently not selected.

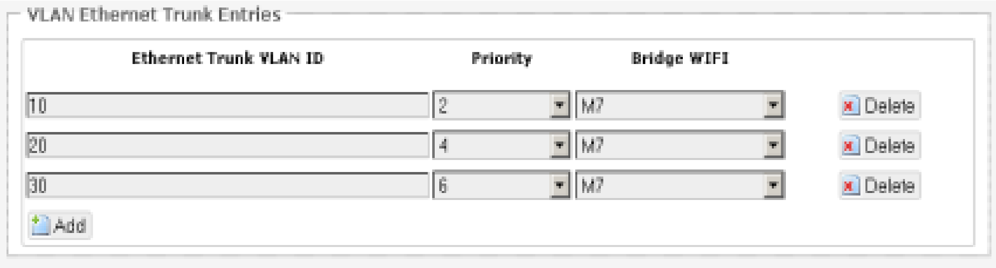
Wifi Tagging: This tags the Ethernet frames sent over Wifi.

Description: Provides a short description of the VLAN.

VLAN Ethernet Trunk

The VLAN Ethernet Trunk links the tagged Ethernet interfaces to the untagged wireless interfaces.

Within the subsection for the VLAN Ethernet Trunk Entries, each row represents one VLAN ID.



VLAN Ethernet Trunk Entries

Ethernet Trunk VLAN ID	Priority	Bridge WIFI	
10	2	M7	Delete
20	4	M7	Delete
30	6	M7	Delete

Add

Figure 69: *VLAN* entries in the *VLAN Ethernet Trunk* section.

Ethernet Trunk VLAN ID: Sets the VLAN ID of the separate VLANs to connect.

Priority: Chooses the priority for transmitting packets. This is a number from 0 to 7. The number 7 represents the highest priority.

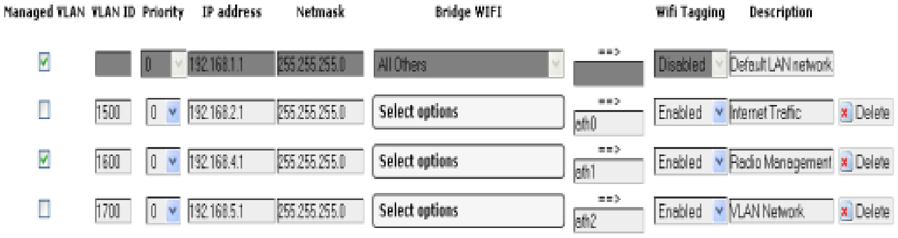
Bridge WIFI: Selects the wireless network (untagged) that would be linked to the Ethernet interface (tagged).

5.5.2 Scenarios

VLAN Management Scenario 1: 3 SSIDs with different VLAN IDs

Examples of usage:

SSID1 (ath0) with VLAN1500 – Internet Traffic
SSID2 (ath1) with VLAN1600 – Wireless Radio Management
SSID3 (ath2) with VLAN1700 – Intranet Traffic



Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIFI		Wifi Tagging	Description	
☑		0	192.168.1.1	255.255.255.0	All Others	==>	Disabled	Default LAN network	
□	1500	0	192.168.2.1	255.255.255.0	Select options	==> ath0	Enabled	Internet Traffic	Delete
☑	1600	0	192.168.4.1	255.255.255.0	Select options	==> ath1	Enabled	Radio Management	Delete
□	1700	0	192.168.5.1	255.255.255.0	Select options	==> ath2	Enabled	VLAN Network	Delete

SSID2 (ath1) has Managed VLAN ticked, and 192.168.4.0/24 is able to use webpage to manage the devices.

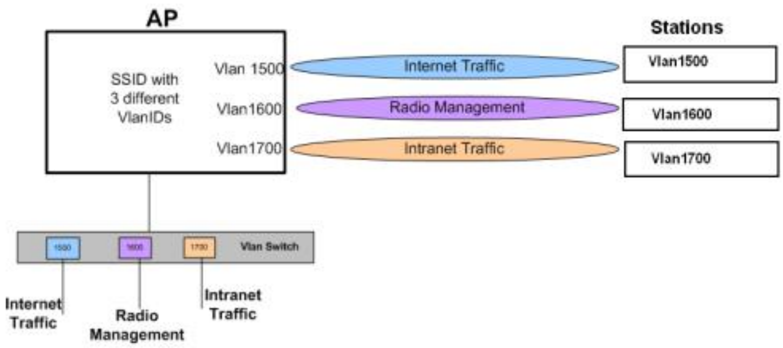
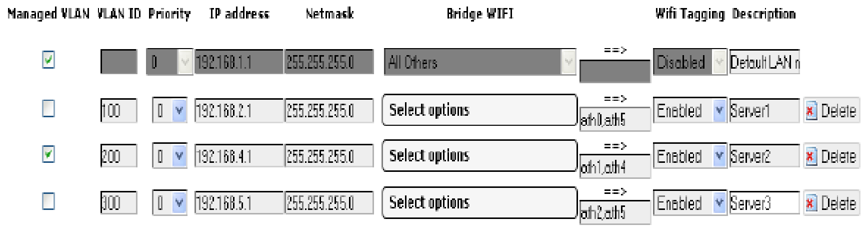


Figure 70: AP connected to 3 stations with different VLAN IDs

VLAN Management Scenario 2: Multiple VAPs in same interface

Add multiple VAPs in same interface with VLAN ID.



Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIFI		Wifi Tagging	Description	
☑		0	192.168.1.1	255.255.255.0	All Others	==>	Disabled	Default LAN n	
□	100	0	192.168.2.1	255.255.255.0	Select options	==> ath0,ath5	Enabled	Server1	Delete
☑	200	0	192.168.4.1	255.255.255.0	Select options	==> ath1,ath4	Enabled	Server2	Delete
□	300	0	192.168.5.1	255.255.255.0	Select options	==> ath2,ath5	Enabled	Server3	Delete

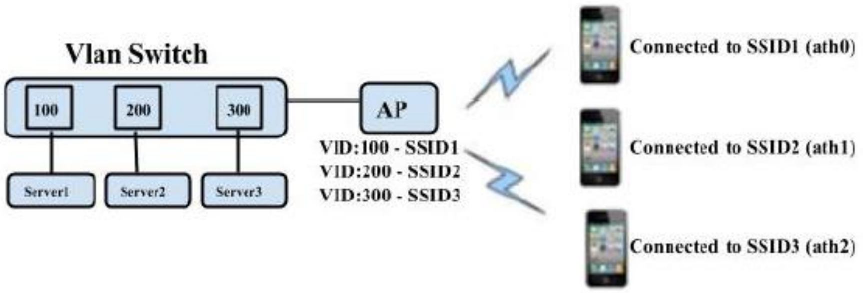
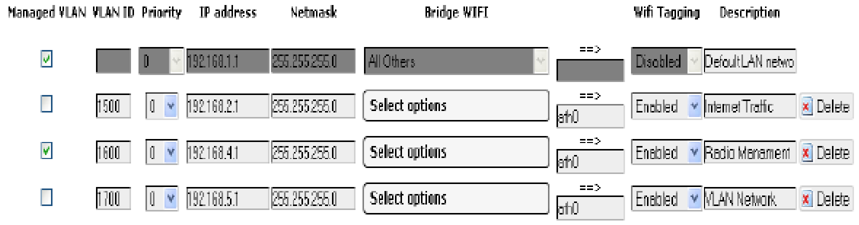


Figure 71: Clients with different SSIDs to connect
different servers.

VLAN Management Scenario 3: SSID with different VLAN IDs



Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIFI		Wifi Tagging	Description	
☑		0	192.168.1.1	255.255.255.0	All Others	==>	Disabled	Default LAN netwo	
□	1500	0	192.168.2.1	255.255.255.0	Select options	==> ath0	Enabled	Internet Traffic	Delete
☑	1600	0	192.168.4.1	255.255.255.0	Select options	==> ath0	Enabled	Radio Menament	Delete
□	1700	0	192.168.5.1	255.255.255.0	Select options	==> ath0	Enabled	VLAN Network	Delete

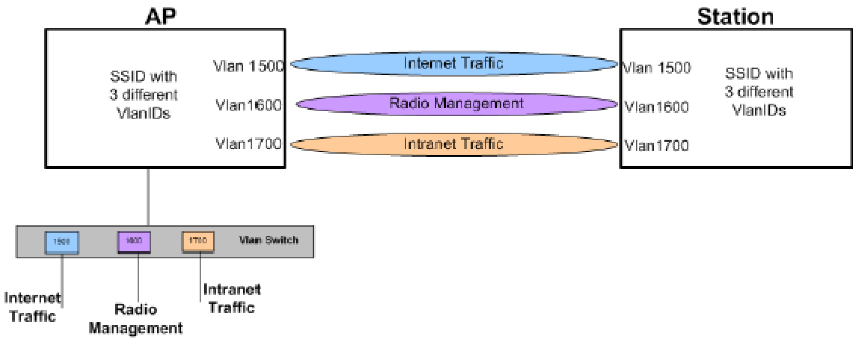


Figure 72: AP connected to Station with 3 different VLAN IDs on same SSID.

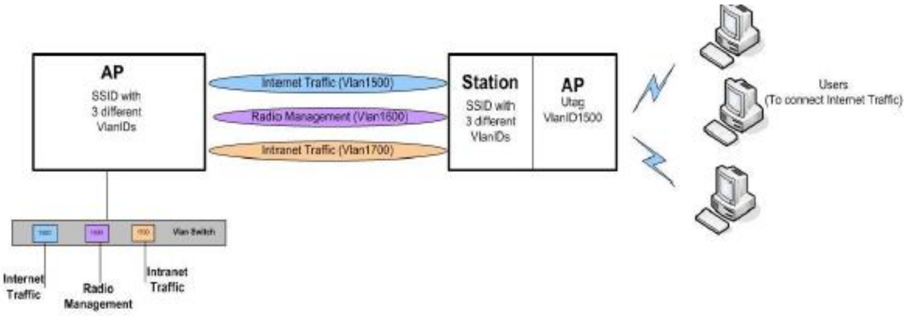
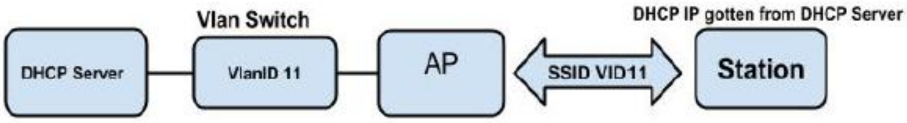
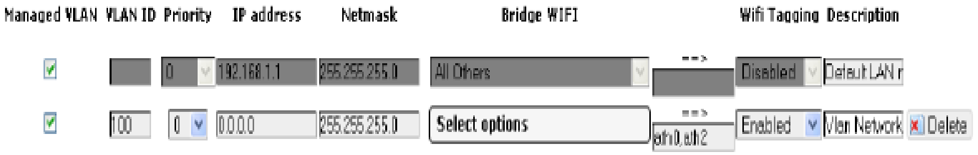

AP
SSID with 3 different VlanIDs
Internet Traffic (Vlan1500)
Radio Management (Vlan1600)
Intranet Traffic (Vlan1700)
Station
SSID with 3 different VlanIDs
AP
Utag VlanID1500
Users
(To connect Internet Traffic)
Vlan Switch
Internet Traffic
Radio Management
Intranet Traffic

Figure 73: Virtual AP (VAP) on the same Station with VLAN ID 1500 (Untagged).

In Figure 73, the VAP would be connected with the Station with VLAN ID 1500, and forward Internet Traffic to the users who are connected to the VAP.

VLAN Management Scenario 4: DHCP client at VLAN Management





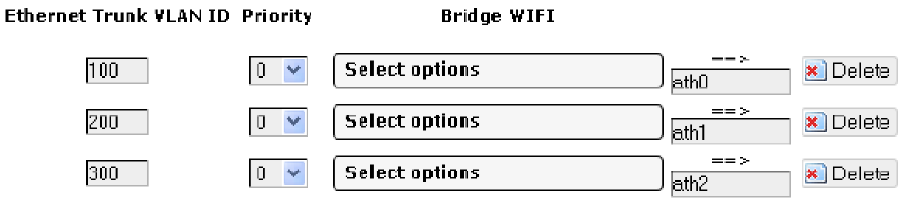
Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIFI		Wifi Tagging	Description	
☑		0	192.168.1.1	255.255.255.0	All Others	==>	Disabled	Default LAN r	
☑	100	0	0.0.0.0	255.255.255.0	Select options	==> ath0,ath2	Enabled	Vlan Network	☒ Delete

Device enabled DHCP client with VlanID at Ethernet port, set IP at Vlan Management as 0.0.0.0. If you ticked at the box, you can access the web page with DHCP client IP after device gotten IP from DHCP server. Please check the IP status at network status page

VLAN Ethernet Trunk Scenario: VLAN IDs at Ethernet port and

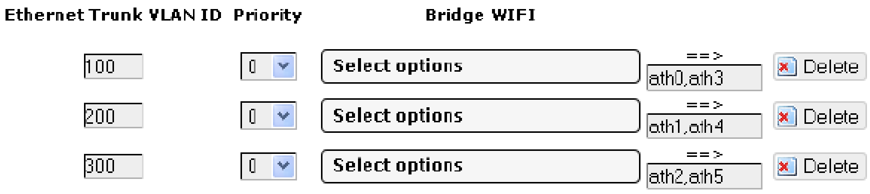
untagged VLAN IDs at SSIDs

Example of usage:
SSID1 (ath0) with VLAN100 – Network Service Provider
SSID2 (ath1) with VLAN200 – Telco Server
SSID3 (ath2) with VLAN300 – Application Service Provide (ASP)

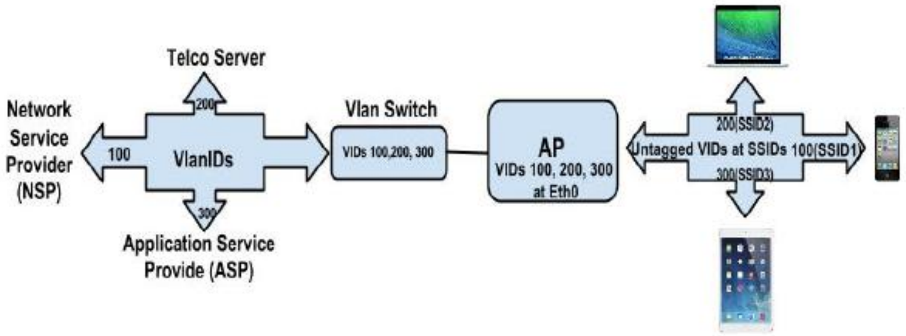


Ethernet Trunk VLAN ID	Priority	Bridge WIFI		
100	0	Select options	==> ath0	Delete
200	0	Select options	==> ath1	Delete
300	0	Select options	==> ath2	Delete

If you want to add more VAPs in same interface that allow you to add it in as below figure. SSID4 (ath3), SSID5 (ath4) and SSID6 (ath5)



Ethernet Trunk VLAN ID	Priority	Bridge WIFI		
100	0	Select options	==> ath0,ath3	Delete
200	0	Select options	==> ath1,ath4	Delete
300	0	Select options	==> ath2,ath5	Delete

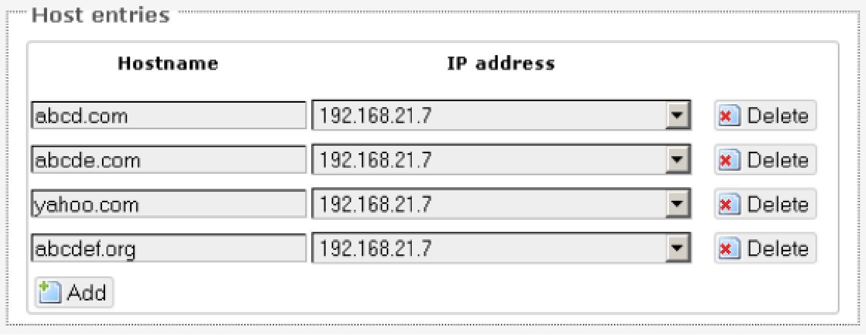

Telco Server
200
Network Service Provider (NSP)
100
VlanIDs
300
Application Service Provide (ASP)
Vlan Switch
VIDs 100,200, 300
AP
VIDs 100, 200, 300 at Eth0
200(SSID2)
Untagged VIDs at SSIDs 100(SSID1)
300(SSID3)

Examples of Applications:
Broadband Remote Access Servers (BRAS)

The BRAS makes use of VLAN ID to differentiate the services to the end-users. It would then provide the different services to different end-users connected with different SSIDs.

5.6 Hostnames

In the *Network* → *Hostnames* page, you can specify custom hostnames (URLs) with their respective IP addresses. This is an additional local DNS.



Host entries

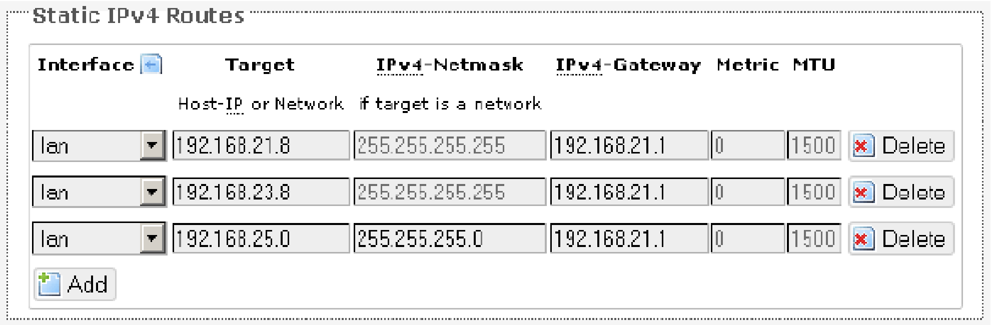
Hostname	IP address	
abcd.com	192.168.21.7	Delete
abcde.com	192.168.21.7	Delete
yahoo.com	192.168.21.7	Delete
abcdef.org	192.168.21.7	Delete

Add

Figure 74: Custom hostname entries.

5.7 Static Routes

The *Network* → *Static Routes* page shows the static IPv4 routes.



Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	
lan	192.168.21.8	255.255.255.255	192.168.21.1	0	1500	Delete
lan	192.168.23.8	255.255.255.255	192.168.21.1	0	1500	Delete
lan	192.168.25.0	255.255.255.0	192.168.21.1	0	1500	Delete

Add

Figure 75: *Static IPv4 Routes*.

Each row shows the interface and gateway over which a certain host or network can be reached.

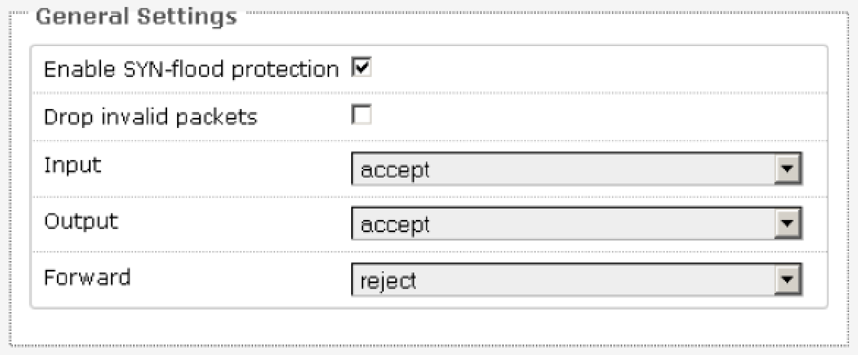
5.8 Firewall

The *Network* → *Firewall* page contains the subpages for *General Settings, Port Forwards,* and *Traffic Rules*.

5.8.1 General Settings

The firewall creates zones over the network interfaces to control network traffic flow. The Network → Firewall → General Settings page contains the zone settings.

Zone Settings



General Settings

Enable SYN-flood protection	☑
Drop invalid packets	☐
Input	accept
Output	accept
Forward	reject

Figure 76: *General Settings* for the *Firewall Zones*

Enable SYN-flood protection: Checked by default.

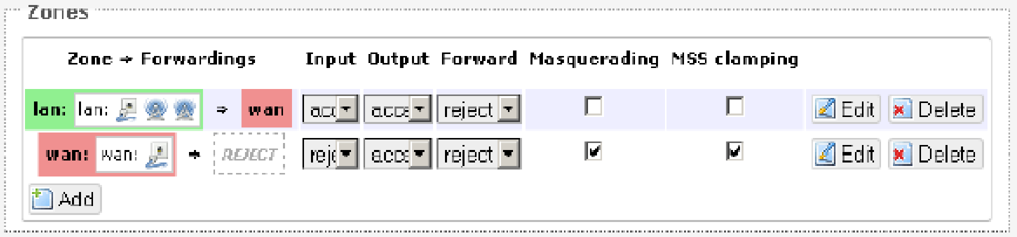
Drop invalid packets: Unchecked by default.

Input: To *accept* by default.

Output: To *accept* by default.

Forward: To *reject* by default.

Zones



Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	acc	acce	reject	☐	☐	Edit Delete
wan: wan: ⇒ REJECT	reje	acce	reject	☑	☑	Edit Delete

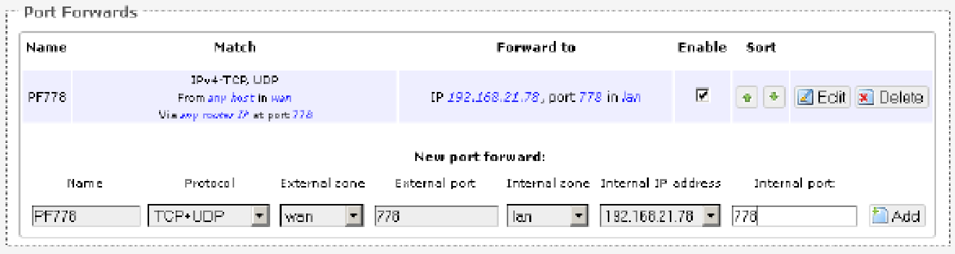
Add

Figure 77: The *Zones* section showing the default settings for the firewall zones.

5.8.2 Port Forwards

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

The *Network* → *Firewall* → *Port Forwards* page lets you define the protocol and port number to access an internal IP address.



Port Forwards

Name	Match	Forward to	Enable	Sort	
PF778	IPv4-TCP, UDP From any host in wan Via any router IP at port 778	IP 192.168.21.78, port 778 in lan	☑		Edit Delete

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
PF778	TCP+UDP	wan	778	lan	192.168.21.78	778	Add

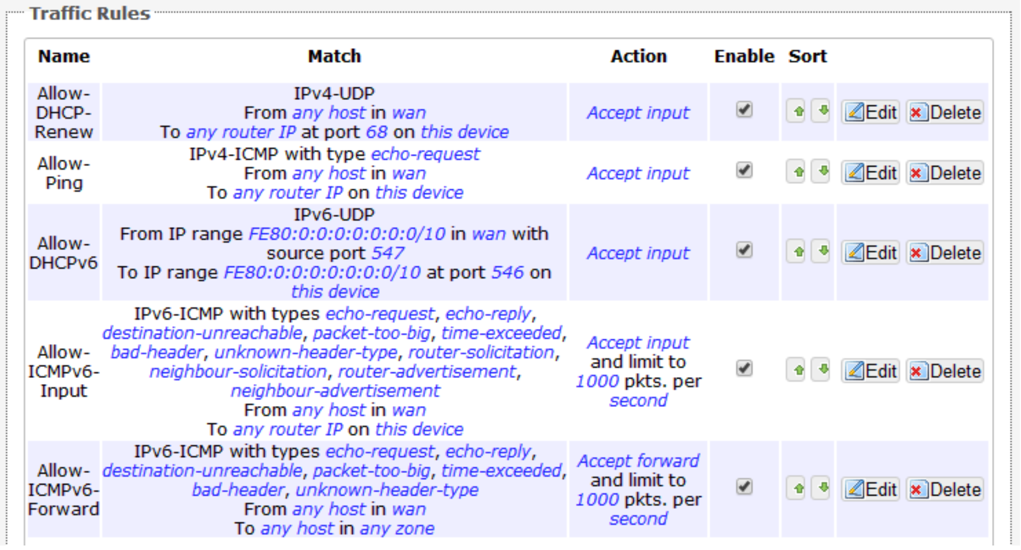
Figure 78: Adding a port forwarding rule

5.8.3 Traffic Rules

The *Network* → *Firewall* → *Traffic Rules* page configures the traffic rules and source NAT.

Traffic Rules

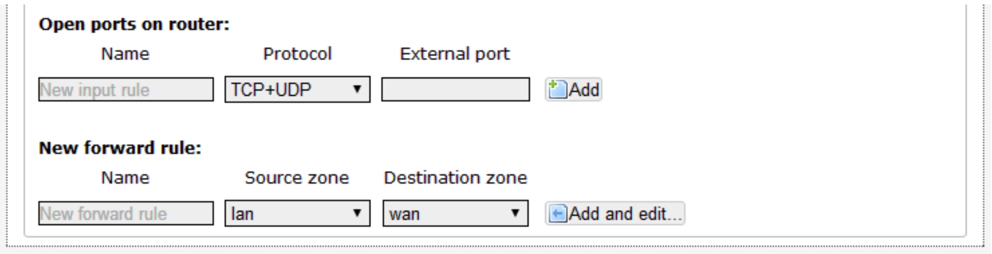
Traffic rules define policies for packets travelling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.



Traffic Rules

Name	Match	Action	Enable	Sort		
Allow-DHCP-Renew	IPv4-UDP From *any host* in *wan* To *any router IP* at port *68* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-Ping	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-DHCPv6	IPv6-UDP From IP range *FE80:0:0:0:0:0:0:0/10* in *wan* with source port *547* To IP range *FE80:0:0:0:0:0:0:0/10* at port *546* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
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*	☑	↑ ↓	Edit	Delete
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*	☑	↑ ↓	Edit	Delete

Figure 79: Firewall Traffic Rules with the default settings



Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP ▾		Add

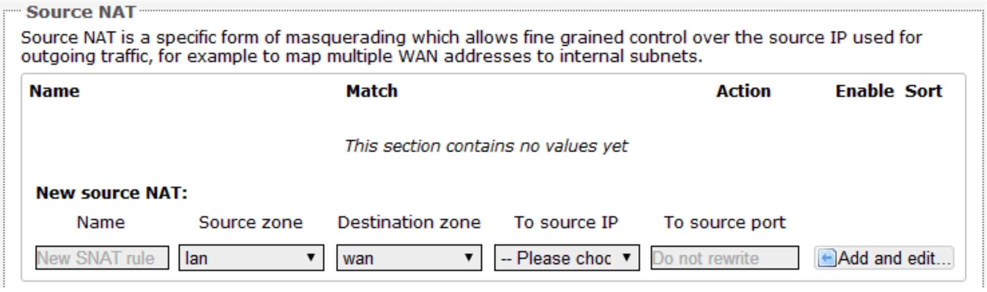
New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan ▾	wan ▾	Add and edit...

Figure 80: You can choose to open ports on the router or add new forwarding rules.

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.



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			

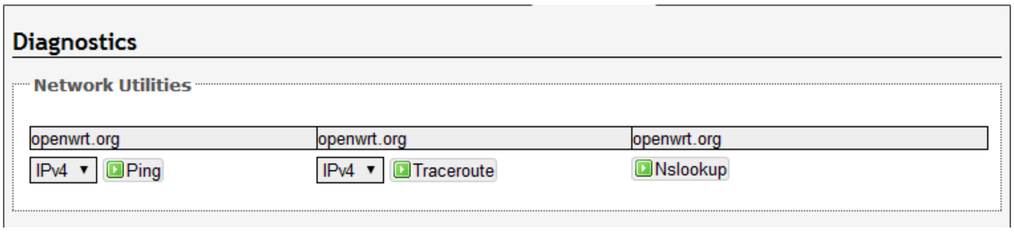
New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	lan ▾	wan ▾	-- Please choc ▾	Do not rewrite	Add and edit...

Figure 81: *Source NAT.*

5.9 Diagnostics

5.9.1 Network Utilities



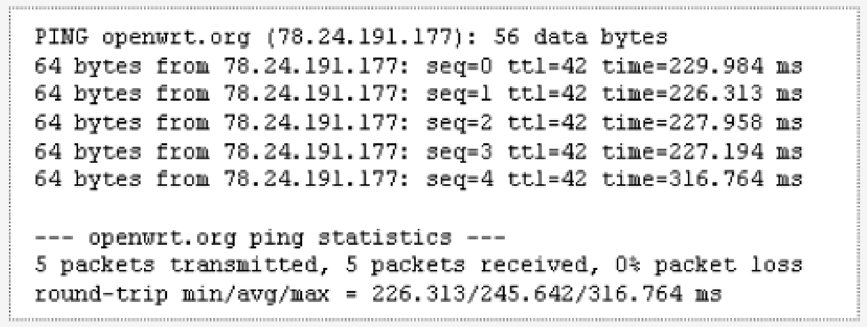
Diagnostics

Network Utilities

openwrt.org | openwrt.org | openwrt.org

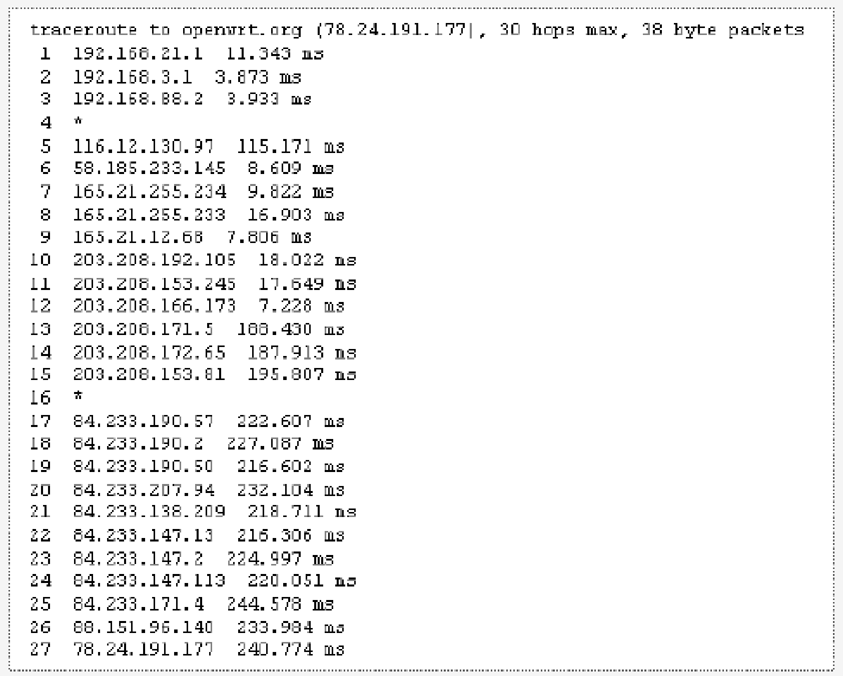
IPv4 ▼ | IPv4 ▼

Figure 82: *Network Utilities* consist of *Ping, Traceroute,* and *Nslookup*.



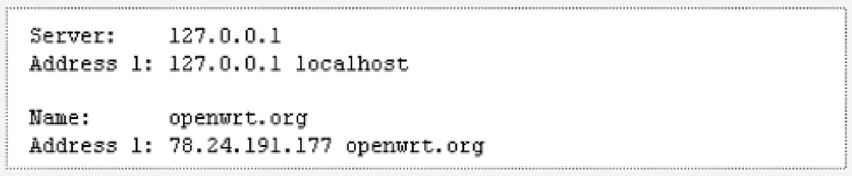
```
PING openwrt.org (78.24.191.177): 56 data bytes
64 bytes from 78.24.191.177: seq=0 ttl=42 time=229.984 ms
64 bytes from 78.24.191.177: seq=1 ttl=42 time=226.313 ms
64 bytes from 78.24.191.177: seq=2 ttl=42 time=227.958 ms
64 bytes from 78.24.191.177: seq=3 ttl=42 time=227.194 ms
64 bytes from 78.24.191.177: seq=4 ttl=42 time=316.764 ms

--- openwrt.org ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 226.313/245.642/316.764 ms
```

Figure 83: Result of *Ping.*



```
traceroute to openwrt.org (78.24.191.177|, 30 hops max, 38 byte packets
 1  192.168.21.1  11.343 ms
 2  192.168.3.1  3.873 ms
 3  192.168.88.2  3.933 ms
 4  *
 5  116.12.130.97  115.171 ms
 6  58.185.233.145  8.609 ms
 7  165.21.255.234  9.822 ms
 8  165.21.255.233  16.903 ms
 9  165.21.12.68  7.806 ms
10  203.208.192.105  18.022 ms
11  203.208.153.245  17.649 ms
12  203.208.166.173  7.228 ms
13  203.208.171.5  188.430 ms
14  203.208.172.65  187.913 ms
15  203.208.153.81  195.807 ms
16  *
17  84.233.190.57  222.607 ms
18  84.233.190.2  227.087 ms
19  84.233.190.50  216.602 ms
20  84.233.207.94  232.104 ms
21  84.233.138.209  218.711 ms
22  84.233.147.13  216.306 ms
23  84.233.147.2  224.997 ms
24  84.233.147.113  220.051 ms
25  84.233.171.4  244.578 ms
26  88.151.96.140  233.984 ms
27  78.24.191.177  240.774 ms
```

Figure 84: Result of *Traceroute*

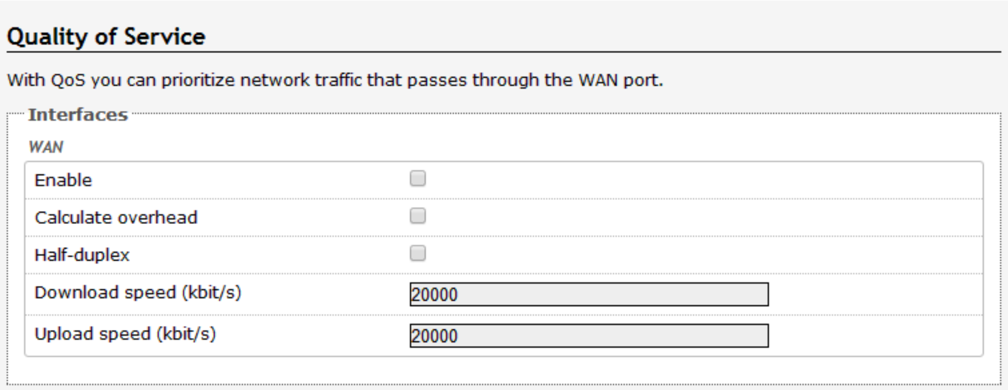


```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      openwrt.org
Address 1: 78.24.191.177 openwrt.org
```

Figure 85: Result of *Nslookup*.

5.10 Quality of Service

The *Network* → *QoS* page configures the quality of service (QoS). With QoS you can prioritize network traffic that passes through the WAN port. You can limit the download and upload speeds. Network QoS is disabled by default.



Quality of Service

With QoS you can prioritize network traffic that passes through the WAN port.

Interfaces

WAN

Enable	□
Calculate overhead	□
Half-duplex	□
Download speed (kbit/s)	20000
Upload speed (kbit/s)	20000

Figure 86: *Network QoS* settings.

Chapter 6: AP Controller Tab

APs running the HenrichWRT firmware can be managed by a Henrich Access Point Controller (APc).

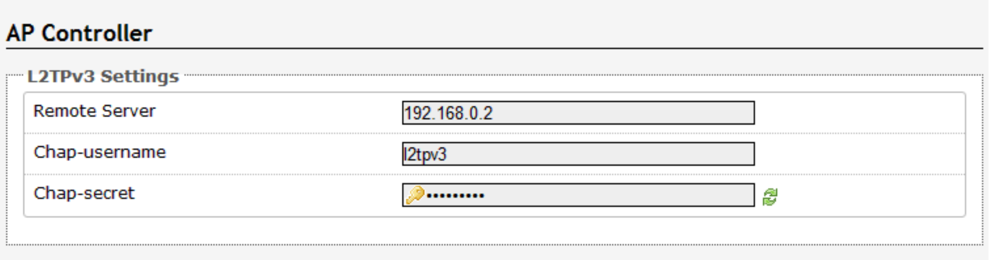
The Henrich APc sends and receives information from HenrichWRT APs using the SNMPv3 protocol.

6.1 Getting Started with Managing APs using the APc

For each AP, please perform the following steps in the AP's web page:

1. Set the APc IP address.
2. Set the AP's IP address, default gateway, and custom DNS server.
   - The web page may not jump automatically to the new IP address if the subnet changed, so please re-enter the new IP address in the browser.
   - Click on the network tab to check that the L2TP is communicating packets with the APc.
3. Set the hostname of the AP to better identify it.

The following describes the “APController” top-level tab.



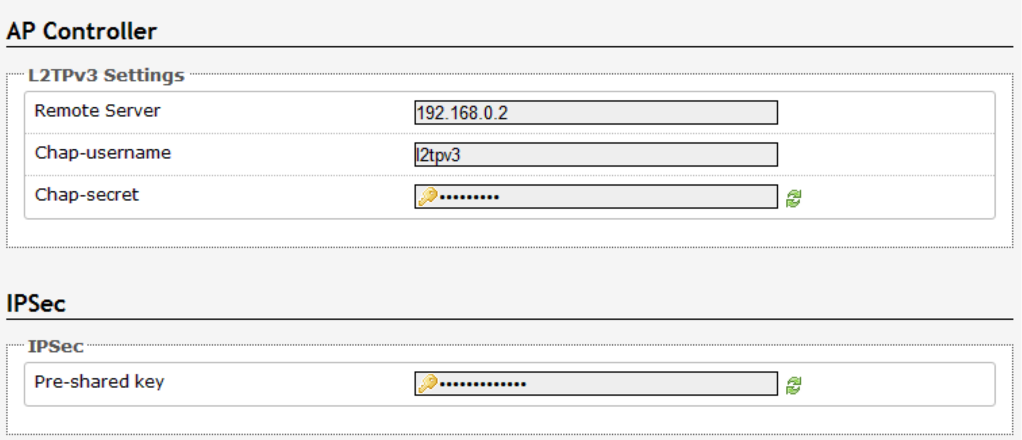
AP Controller

L2TPv3 Settings

Remote Server	192.168.0.2
Chap-username	l2tpv3
Chap-secret	••••••••

Figure 87: The *APController* Tab.

In later versions of HenrichWRT, from b140814 onwards, you would see the following page.



AP Controller

L2TPv3 Settings

Remote Server	192.168.0.2
Chap-username	l2tpv3
Chap-secret	••••••••

IPSec

IPSec

Pre-shared key	••••••••••••

Figure 88: The new AP Controller tab

When using the APc for the first time, you only need to set the IP address of the APc. This has to be done in the AP's configuration web page itself. All other settings should remain as the default values for now.

Please always click “Save & Apply”. Do not click “Save”. This is to apply the settings immediately.

6.2 L2TPv3 Settings

The following are the settings for the Layer 2 Tunneling Protocol Version 3 (L2TPv3).

Remote Server: Configures the IP address of the APc e.g. 192.168.3.178.

Chap-username: Sets the username for the Challenge-Handshake Authentication Protocol (CHAP).

Chap-secret: Sets the password for the Challenge- Handshake Authentication Protocol (CHAP).

6.3 IPSec

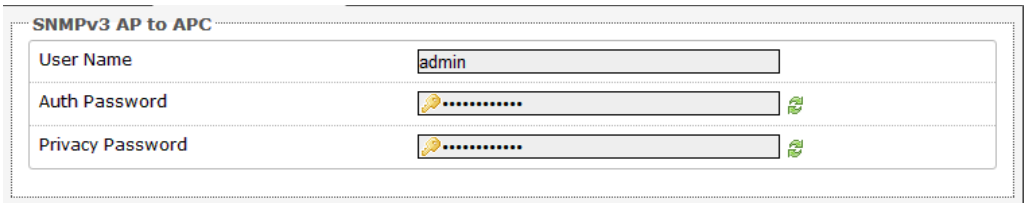
By default, the Internet Protocol Security (IPsec) is disabled for the HenrichWRT HWRD boards to decrease the usage of the CPU resources. It can also be enabled.

The L2TPv3 itself already provides data channel protection against malicious data insertion.

Pre-shared key: Sets the password for the IPsec.

6.4 APc SNMP Settings

The "SNMPv3 AP to APC" section contains the APc SNMP settings.



SNMPv3 AP to APC

User Name	admin
Auth Password	••••••••••••
Privacy Password	••••••••••••

Figure 89: APc SNMP Settings.

Currently, the following default values must be used.

User Name: "admin"

Auth Password: "apc0ntr0ll3r"

Privacy Password: "apc0ntr0ll3r"

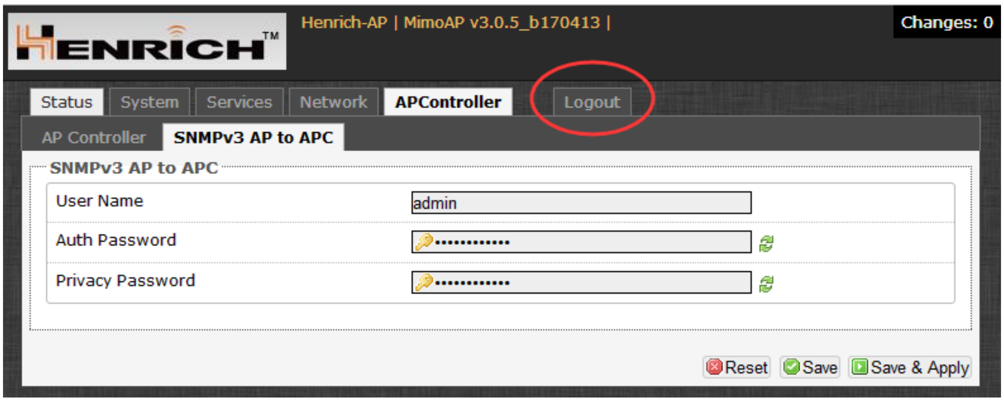
6.5 AP SNMP Settings

For communication from the APc to the AP, the settings in the following section of the LuCI web page is used: *System* → *SNMP* → *SNMP Configuration* → *General Settings*

The description of the SNMP options are mentioned in Section 3.4.2 *SNMP Configuration*.

Chapter 7: Final Notes

Logout: Logs out of the router's web page.



SNMPv3 AP to APC

User Name	admin
Auth Password	••••••••••
Privacy Password	••••••••••

Figure 90: The *Logout* button is circled.

7.1 Troubleshooting steps

7.1.1 PC cannot connect to the router

The configuration web page for the router would not be able to show up if the router and your computer are not connected.

If the PC and the router are joined to the network by LAN cables, they would not be able to connect if any of the network cable connections are loose. A possible indicator is that there is no light at the LAN port of the PC. In Windows, if you click the network icon and click to “View network connections”, the LAN port shows “Disconnected”. Please ensure that all the connections are tight.

Sometimes, disconnecting and reconnecting the LAN cable solves connection problems if DHCP is used, because the DHCP server and DNS server are reset.

(Also, dis-associating and re-associating to the wireless network has a similar benefit as unplugging and re-inserting the LAN cable.)

The router, the computer, and the gateway must have IP addresses on the same network. For example, if you use a subnet mask of 255.255.255.0 and the gateway IP address is 192.168.3.1, all the IP addresses must be unique and be of the form 192.168.3.X.

Check whether the router and your computer are connected on the same network by running the ping command to ping the IP address of the router. Alternatively, type the following in the router's Linux terminal: ping 192.168.3.77 (if your computer's IP address is 192.168.3.77 for example.)

They should be able to give the ping responses.

An IP address conflict would cause unstable pings. Switch to another address and ping the conflicting address to check.

If using a Windows computer, you should run the command arp -d * if the network configuration has changed. This is to delete the address resolution protocol (ARP) table in Windows as it may not update fast enough.

If the ping still cannot get responses, try disabling the firewall on your Windows computer. The Windows Firewall on your computer may prevent it from sending back a ping response. Disabling the firewall may be a security risk, so you should take the precaution of disconnecting the Internet first.

7.1.2 PC Ethernet and Wifi adapters

If your PC has both Ethernet and Wifi adapters, they must not have the same subnet. Otherwise, packets from the PC may not be directed to the correct network.

7.1.3 Mobile phone cannot connect

A mobile phone or any Wifi user would not be able to connect to a wireless router if there does not exist a DHCP server on the network. Please make sure that there is one, and only one, DHCP server to assign IP addresses automatically to users.

You may refer to Section 5.2.2 DHCP Server to enable the DHCP server for a router. The option is found in *Network* → *Interfaces* → *LAN* → *DHCP Server.*

7.1.4 Mobile phone connects but cannot access Internet

A mobile phone or any connected Wifi user would not be able to access the Internet if the default gateway is not set correctly on the router.

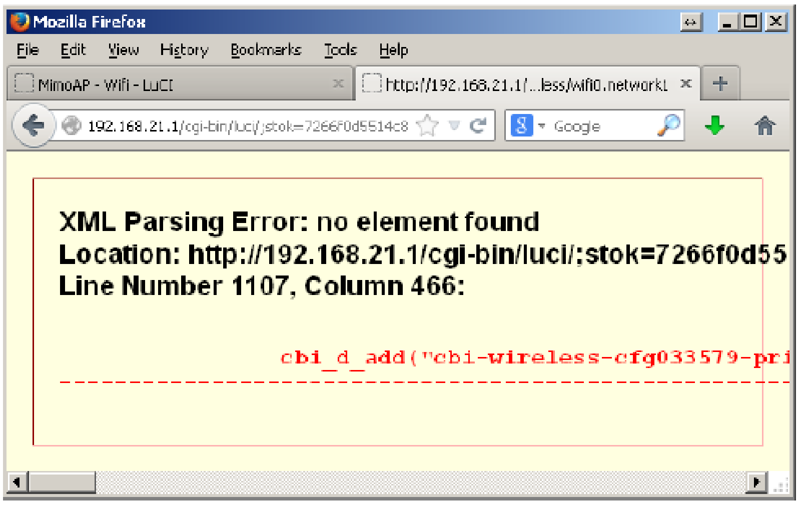
The option for the default gateway is found in *Network* → *Interfaces* → *LAN* → *Common Configuration* → *General Setup* → *IPv4 gateway.*

If this router has enabled a DHCP server but the gateway is at a different IP address please add a DHCP option according to Section 5.2.2 *DHCP Server.*

The DNS server should also be set. This option is found in *Network* → *Interfaces* → *LAN* → *Common Configuration* → *General Setup* → *Use custom DNS servers.*

7.1.5 Unresponsive web page

Symptom: The 'XML Parsing Error' may occur if a certain option was changed and the web page did not update in time.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
MimoAP - Wifi - LuCI
http://192.168.21.1/...less/wifi0.networkL
192.168.21.1/cgi-bin/luci/;stok=7266f0d5514c8
Google

```
XML Parsing Error: no element found
Location: http://192.168.21.1/cgi-bin/luci/;stok=7266f0d55
Line Number 1107, Column 466:

                    cbi_d_add("cbi-wireless-cfg033579-pri
---------------------------------------------------------------
```

Figure 91: XML Parsing Error.

Solution: Re-enter the IP address into the browser. For example, if the current URL is 192.168.21.1/cgibin/ luci/;stok=7266f0d55..., delete the right hand side to leave the IP address of 192.168.21.1 and press Enter. This would bring you back to the login page of the device.

7.1.6 Unresponsive router

Symptom: The router does not respond.
Solution: Turn off the router for 10 seconds and then turn it on again.

7.2 Troubleshooting steps

To reset the router to the factory default settings, while the power is on, hold down the reset button for 8 seconds and then release.

Another method is to enter the following command into the router's Linux terminal: mtd -r erase rootfs_data

After a while, the flash would be erased and the router would reboot into its factory default state. The firmware version remains the same as the latest firmware loaded onto the board.

Glossary

Term	Definition
Access Point (AP)	A device that provides network access to associated stations (connected wireless devices). A wireless router can function as an AP.
ACK	Acknowledgment. This is a response to a transmission to indicate that the data packet was received correctly.
ARP	Address Resolution Protocol. This is a broadcast protocol for mapping IP addresses to MAC addresses.
CHAP	Challenge-Handshake Authentication Protocol. This is a protocol for authenticating users to an ISP.
CPE	Customer-Premises Equipment. This is also known as a station.
Db	Decibels. This is a measure of intensity.
dBm	Decibel-milliwatts. This is a measure of power relative to 1 mW. This is commonly used to measure wireless signal power. A higher power leads to better signal quality.
DDNS	Dynamic DNS. This is a system for updating domain names in real time. It allows a domain name to be assigned to a device with a dynamic IP address.
DHCP	Dynamic Host Configuration Protocol. This is a protocol for allocating IP addresses dynamically so that addresses can be reused when hosts (e.g. computers) no longer need them.
DNS	Domain Name System. This is a distributed and hierarchical naming system for computers, services, or any resource connected to the Internet or a private network.
EIRP	Equivalent Isotropically Radiated Power. Each country sets the legally permitted maximum for the EIRP limits on each channel.
ESSID	Extended Service Set Identifier. This is the name of the wireless network. It is case-sensitive and up to 32 alphanumeric characters in length. The ESSID differentiates one wireless network from another. All access points and devices trying to connect to a specific wireless network should use the same ESSID (and password) to enable effective roaming.
FTP	File Transfer Protocol. This is a protocol for transferring files between network nodes.

HTTP	Hypertext Transfer Protocol. This is a protocol used by web browsers and web servers to transfer files.
IP	Internet Protocol. This is the primary communications protocol used for relaying network packets (also known as datagrams) across an internetwork using the Internet Protocol Suite. IP is responsible for routing packets across network boundaries. It is the principle protocol that establishes the Internet.
ISP	Internet Service Provider.
L2TP	Layer 2 Tunneling Protocol. This is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.
LAN	Local Area Network.
Layer 2	Data link layer of the Open Systems Interconnection (OSI) model. This corresponds to the Link layer of the Internet protocol suite.
MAC Address	Media Access Control Address. This is a globally unique identifier attached to a network adapter. It also identifies the hardware manufacturer.
Mbps	Megabits per second. Also Mbit/s. This is a measure of the data rate.
MiniPCIe	Mini Peripheral Component Interconnect Express. A miniPCIe radio is a radio card that can be inserted into a router's circuit board.
MTU	Maximum transmission unit. This is the size, in bytes, of the largest packet that can be passed on. The MTU for Ethernet is a 1500-byte packet.
NAT	Network Address Translation. This is the process of rewriting IP addresses as a packet passes through a controller or firewall. NAT enables multiple computers (or hosts) on a LAN to access the Internet using the single public IP address of the LAN's gateway controller.
NMS	Network Management Station. This is a software which runs on the SNMP manager. It is sometimes simply referred to as an SNMP manager.
NTP	Network Time Protocol. This is a protocol for synchronizing a controller to a single clock on the network, known as the clock master.
PAP	Password Authentication Protocol. This is a protocol for authenticating users to a remote access server or ISP.
PPPoE	Point-to-Point Protocol over Ethernet. This is a protocol for connecting

	a network of hosts to an ISP without the ISP having to manage the allocation of IP addresses.
PPTP	Point-to-Point Tunneling Protocol. This is a protocol for the creation of VPNs for the secure transfer of data from remote clients to private servers over the Internet.
QoS	Quality of Service. This is the prioritization of network traffic. Voice traffic gets the highest priority, followed by video, best effort, and background traffic, in this order.
RADIUS	Remote Authentication Dial In User Service. This is a networking protocol that provides Authentication, Authorization, and Accounting (AAA) management for remote users. The RADIUS provides centralized management of usernames and passwords.
SNMP	Simple Network Management Protocol. This is an Internet-standard protocol for managing devices on IP networks. It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.
SSID	Service Set Identifier. This is also known as the ESSID or the wireless network name.
Station	A device that connects wirelessly to an access point.
Subnet	A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 192.168.7 belong to the same subnet.
TCP	Transmission Control Protocol. This is a protocol for transmitting data over the Internet with guaranteed reliability and in-order delivery.
UDP	User Datagram Protocol. This is a protocol for transmitting data over the Internet quickly but with no guarantee of reliability or in-order delivery.
VAP	Virtual Access Point. A VAP simulates a physical access point. A VAP is configured on a per-radio basis. By default, only one VAP is enabled. Up to 16 VAPs can be created for each radio, each with its own SSID.
VPN	Virtual Private Network. This is a network that enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. The VPN uses tunneling to encrypt all information at the IP level.

WAN	Wide Area Network. This is a network that covers a broad area. The world's most popular WAN is the Internet.
Web Browser	A software that allows the user to surf the Internet.
WDS	Wireless Distribution System. This is a system enabling the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the traditional requirement for a wired backbone to link them.
WLAN	Wireless Local Area Network. *52*