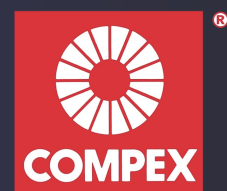




CompexWRT

User Manual



Copyright

This document contains information, which is protected by copyright. Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

© Copyright 2014 Compex Systems Pte Ltd.

All Rights Reserved.

Feedback

Please direct any comments or suggestions about this document to: feedback@compex.com.sg

Trademark Information

Compex® is a registered trademark of Compex Systems Pte Ltd. Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Compex provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Compex may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Compex will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Publication date and software version

Published 14 January 2014. Software version v1.30_b140102.

Contents

Copyright.....	3
Chapter 1: Overview.....	6
1.1 Introduction.....	6
1.2 Language.....	6
1.3 Supported Products.....	6
1.4 System Requirements.....	6
1.5 Getting Started.....	6
1.6 Operating Modes.....	6
1.7 Buttons and Changes.....	7
Chapter 2: Status Tab.....	7
2.1 Overview.....	7
2.1.1 Wireless.....	7
2.1.2 Wireless (for AP Mode).....	7
2.1.3 Wireless (for Station Mode).....	8
2.1.4 Associated Stations (for AP Mode).....	8
2.1.5 System.....	8
2.1.6 Memory.....	8
2.1.7 Network.....	9
2.1.8 DHCP Leases.....	9
2.1.9 Link Status (for Station Mode).....	9
2.2 Routes.....	9
2.3 System Log.....	9
2.4 Kernel Log.....	10
2.5 Realtime Graphs.....	10
2.5.1 Load.....	10
2.5.2 Traffic.....	10
2.5.3 Wireless.....	10
2.5.4 Connection.....	11
Chapter 3: System Tab.....	11
3.1.1 System Properties.....	11
3.1.2 Time Synchronization.....	12
3.2 Administration.....	12
3.2.1 Router Password.....	12
3.2.2 SSH.....	12
3.2.3 Telnet.....	12
3.2.4 Web.....	13
3.2.5 FTP.....	13
3.3 Services.....	13
3.3.1 Ping Watchdog.....	13

3.3.2 Auto Reboot.....	13
3.4 SNMP.....	13
3.4.1 SNMP Information.....	13
3.4.2 SNMP Configuration.....	14
3.5 LED Configuration.....	14
3.6 Backup/Flash Firmware.....	14
3.6.1 Backup/Restore.....	14
3.6.2 Flash new firmware.....	14
3.7 Reboot.....	15
Chapter 4: Services Tab.....	15
4.1 Dynamic DNS.....	15
4.2 Discovery.....	16
Chapter 5: Network Tab.....	16
5.1 Interfaces - WAN.....	17
5.1.1 Common Configuration.....	17
5.2 Interfaces - LAN.....	19
5.2.1 Common Configuration.....	19
5.2.2 DHCP Server.....	19
5.2.3 Static Leases.....	20
5.3 Wifi - Overview.....	20
5.4 Wifi - Wireless Network.....	21
5.4.1 Device Configuration.....	21
5.4.2 Interface Configuration.....	22
5.5 VLANs.....	25
5.5.1 VLAN Management.....	25
5.5.2 VLAN Ethernet Trunk.....	26
5.6 Hostnames.....	26
5.7 Static Routes.....	26
5.8 Firewall.....	26
5.8.1 General Settings.....	26
5.8.2 Port Forwards.....	27
5.8.3 Traffic Rules.....	27
5.9 Diagnostics.....	27
5.9.1 Network Utilities.....	27
5.10 Quality of Service.....	28
Chapter 6: Final Notes.....	28
6.1 Resetting to factory default.....	28

Chapter 1: Overview

1.1 Introduction

This user manual is a guide to the *CompexWRT* firmware on a wireless router. *CompexWRT* combines *OpenWRT* with the most advanced *Qualcomm Atheros 10.1.x* wireless drivers. *CompexWRT* 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 *CompexWRT*.

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 drop-down list for *Language*. You can change the language from *English* to another language e.g. Chinese (中文).

1.3 Supported Products

The *CompexWRT* software resides in the following models of routers: the WPJ342 Series, the WPJ558 Series, the WPJ344 Series, the WP543 Series, the WP546 Series, and the WPE72 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 *CompexWRT* 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 v1.28_b131217.

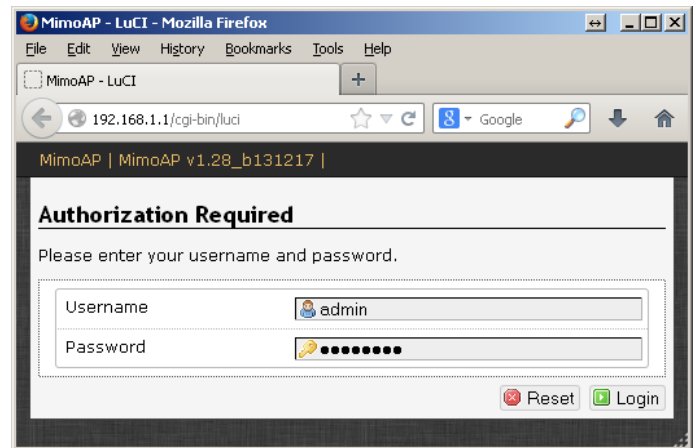


Figure 1: The login page is presented upon requesting the router's IP address.

The default authorization details are:

Username: admin

Password: password

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 page 22.

1.7 Buttons and Changes

The buttons are described here.

Reset: Undo the changes.

Save: Saves the changes.

Save & Apply: Saves and applies the changes. It is recommended to click this button after every change.

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



Note: At the top right corner of the router's configuration web page, there may be either of the following texts displayed.

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*.

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.

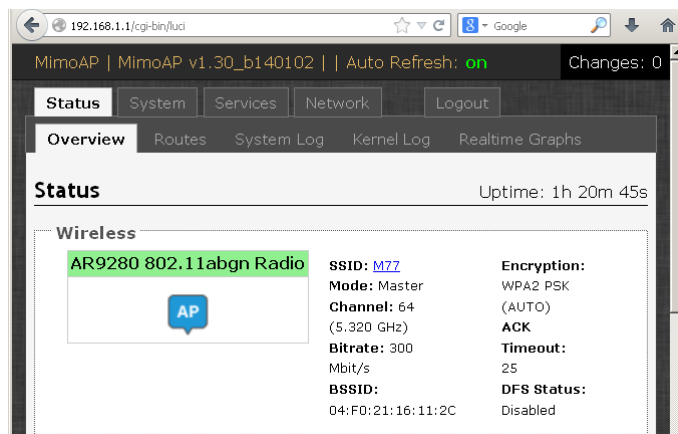


Figure 2: The *Status* → *Overview* page.

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. AR9380 802.11abgn Radio. This box can be removed for OEM customers.

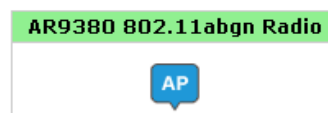


Figure 3: Wireless chipset model

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)

SSID: M7	Encryption: WPA2 PSK (AUTO)
Mode: Master	ACK Timeout: 64
Channel: 1 (2.412 GHz)	DFS Status: Disabled
Bitrate: 300 Mbit/s	
BSSID: 00:80:48:79:3A:A2	

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.

Mode: This is *Master* for 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)

SSID: M7	Encryption: WPA2 PSK (AUTO)
Mode: Client	ACK Timeout: 64
Channel: 1 (2.412 GHz)	DFS Status: Disabled
Bitrate: 300 Mbit/s	TX-CCQ: 88 %
MAC-Address: 04:F0:21:16:11:2C	RX Rate: 177 Mbit/s
BSSID: 00:80:48:79:3A:A2	TX Rate: 241 Mbit/s

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* for Station mode or 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.

MAC-Address	Network	Device Name	Last IP	Signal	Signal/Chains	Noise	TX Rate	RX Rate	TX-CCQ
04:F0:21:16:11:2C	M7	MimoAP	192.168.21.7	-61 dBm	-66,-64,-95 dBm	-95 dBm	229.5 Mbit/s	245.6 Mbit/s	88 %

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. -61 dBm.

Signal/Chains: Shows the received signal strengths from the station on each antenna e.g. -66 dBm and -64 dBm. The value of -95 dBm is taken to mean “no antenna” because the radio here 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	MimoAP
Router Model	WPJ344
Firmware Version	MimoAP v1.28_b131217
Kernel Version	3.3.8
Local Time	Mon Dec 23 07:24:12 2013

Figure 7: System parameters.

2.1.6 Memory

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

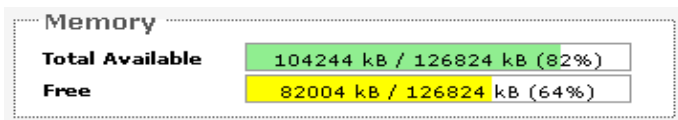


Figure 8: Total Available and Free Memory.

2.1.7 Network

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

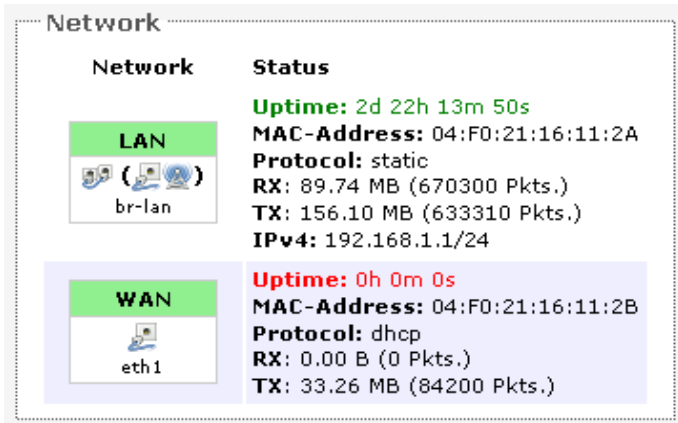


Figure 9: Network summary.

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 page 20.

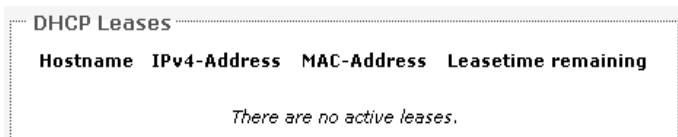


Figure 10: Currently active static DHCP leases.

2.1.9 Link Status (for Station Mode)

This section only applies if the device operates as an 802.11 station.

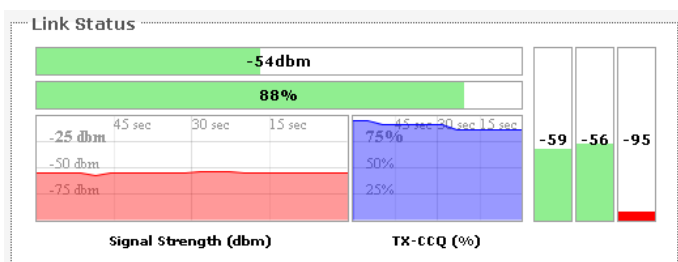


Figure 11: The *Link Status* section.

In the *Link Status* section on the *Status* → *Overview* web page, the value in the top left box denotes the current received signal strength e.g. -54 dBm. The box directly below it shows the current TX-CCQ (transmission client connection quality) in %. 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. -59 dBm and -56 dBm. For this example, the radio has only 2 antennas, so the third vertical bar is given a default value of -95 dBm and shown with a red horizontal line at the base.

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.

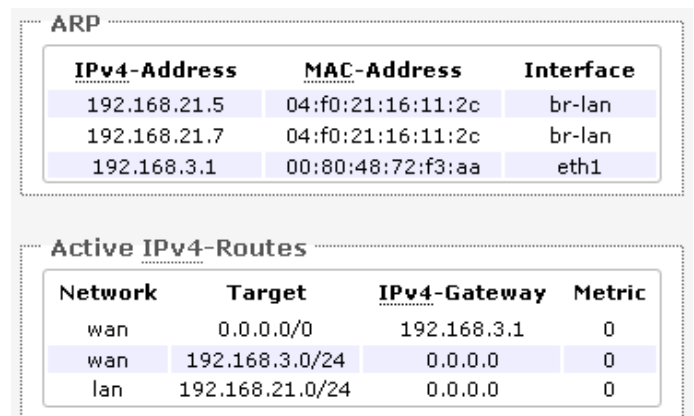


Figure 12: The *Status* → *Routes* page.

ARP: This table shows the IP address and corresponding MAC address 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.

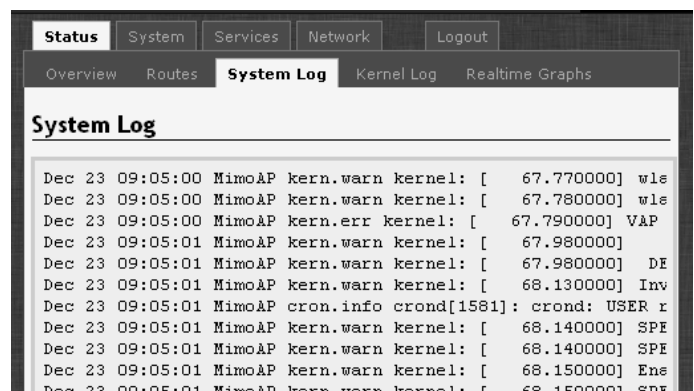


Figure 13: The *Status* → *System Log* page.

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.

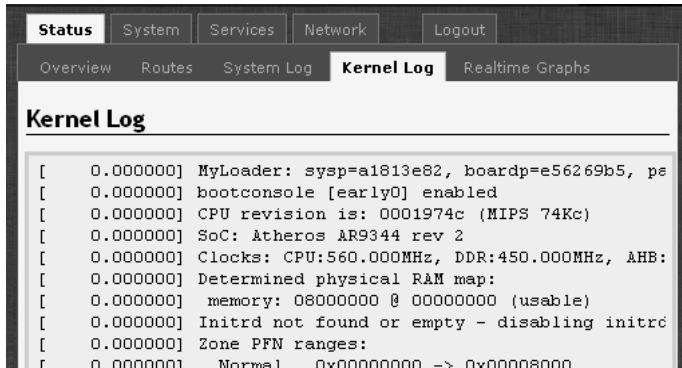


Figure 14: The Status → Kernel Log page.

2.5 Realtime Graphs

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

2.5.1 Load

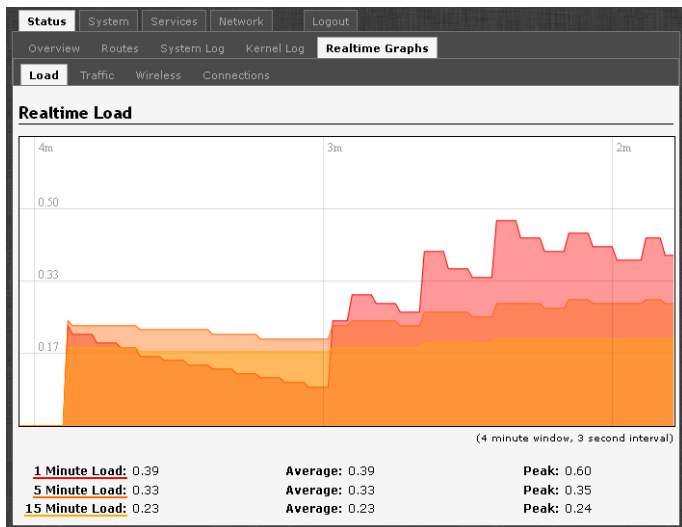


Figure 15: The graph for Realtime Load.

2.5.2 Traffic

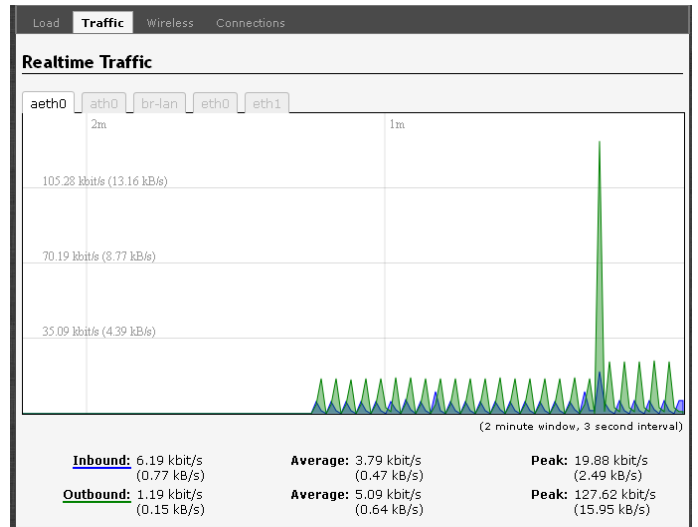


Figure 16: The graph for Realtime Traffic.

2.5.3 Wireless

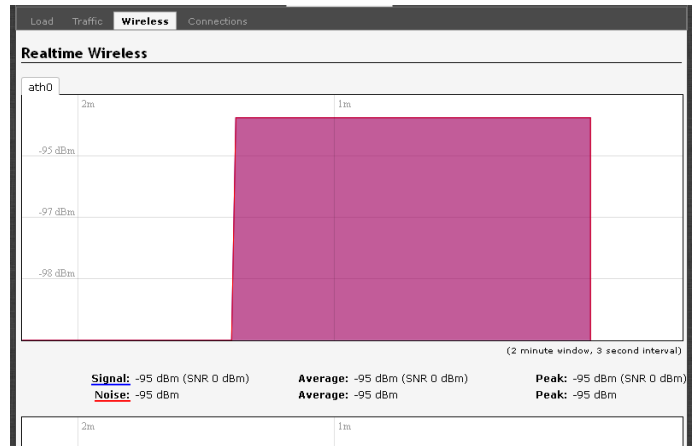


Figure 17: The graph for Realtime Wireless.

2.5.4 Connection

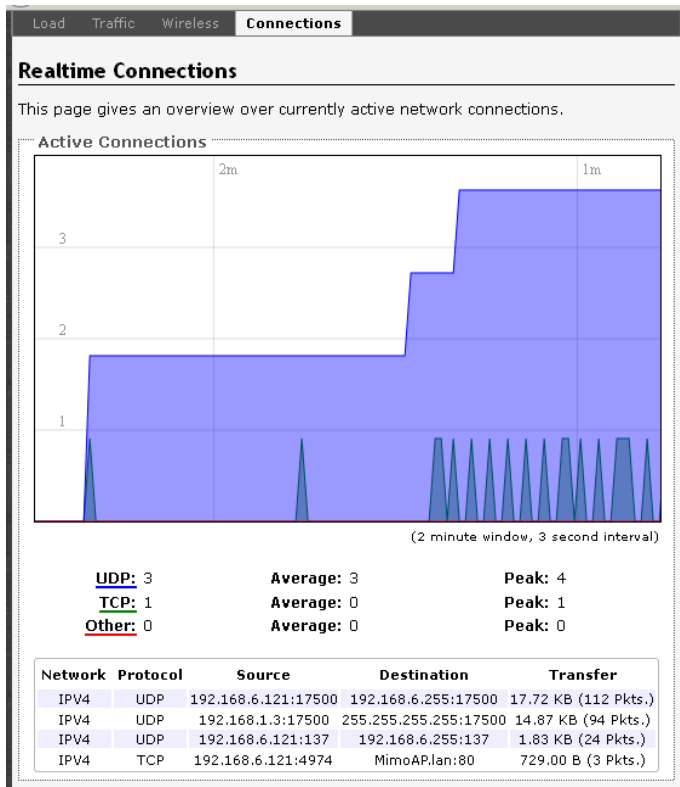


Figure 18: The graph for *Realtime Connections*.

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.

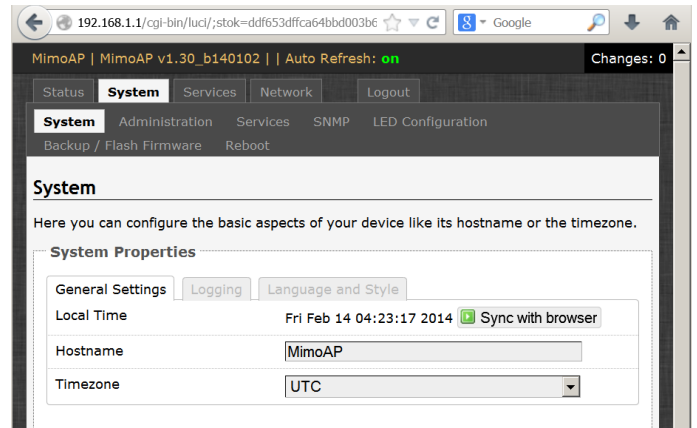


Figure 19: The *System* top-level tab.

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

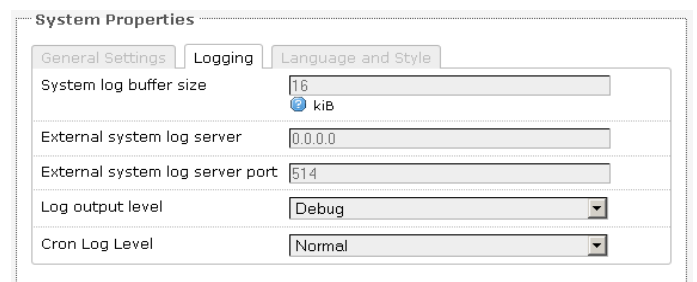


Figure 20: Changing the system properties for *Logging*.

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



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 NTP servers.

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

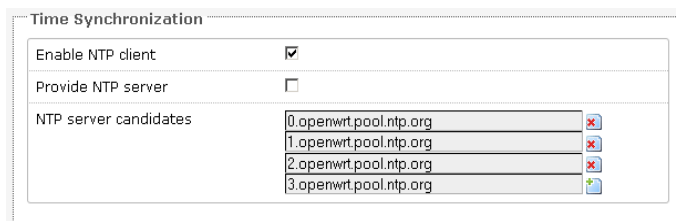


Figure 22: *Time Synchronization* settings.

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

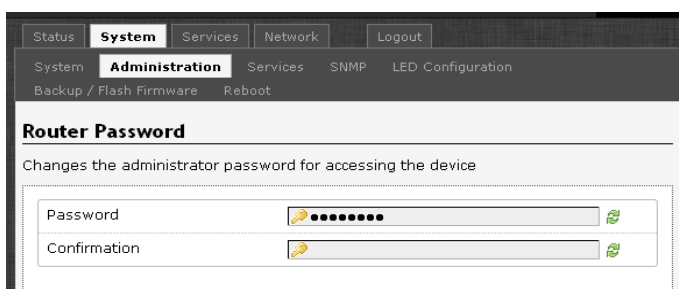


Figure 23: Setting the router password.

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

Confirmation: Requires you to re-enter the password.

3.2.2 SSH

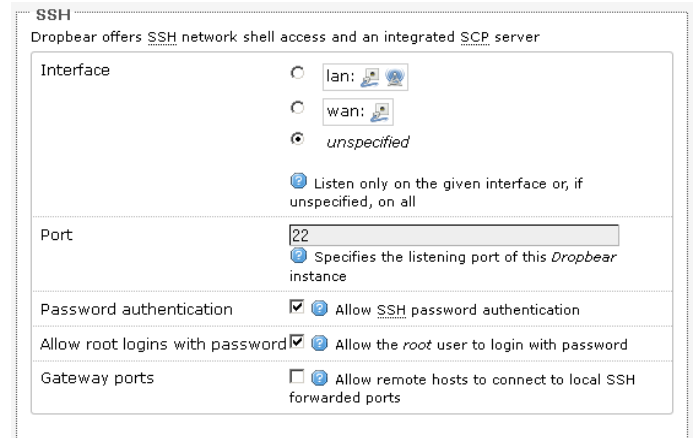


Figure 24: *SSH* settings in the *System* → *Administration* page.

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

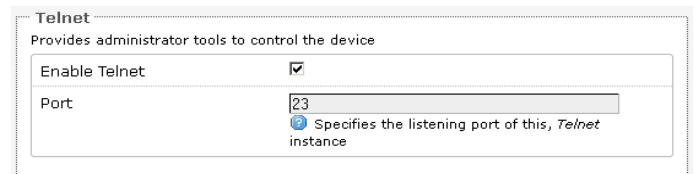


Figure 25: *Telnet* settings in the *System* → *Administration* page.

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

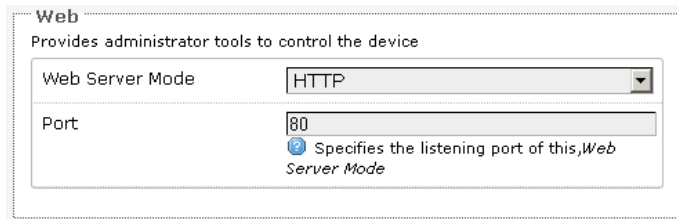


Figure 26: The router's web server mode and port.

Web Server Mode: This can be set to *HTTP* or *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*.

3.2.5 FTP

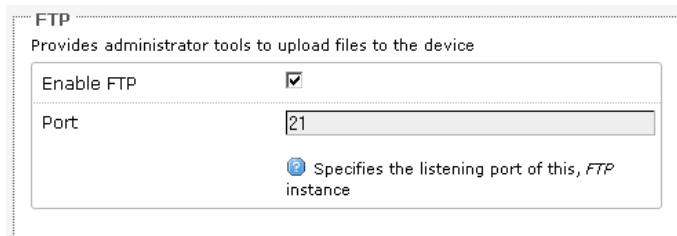


Figure 27: FTP settings in the *System* → *Administration* page.

FTP: Allows you to upload files to the device.

Port: Specifies the listening port, the default being *21*.

3.3 Services

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

3.3.1 Ping Watchdog

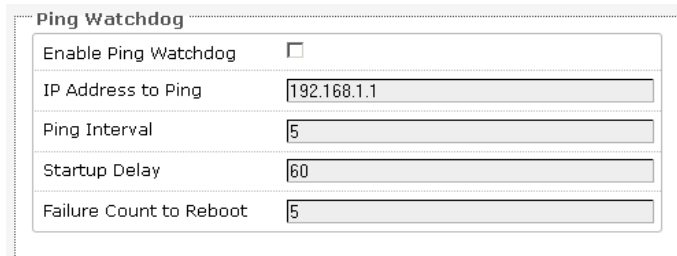


Figure 28: *Ping Watchdog* settings in the *System* → *Services* page.

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

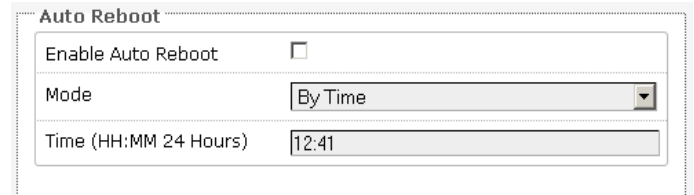


Figure 29: *Auto Reboot* settings in the *System* → *Services* page.

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.

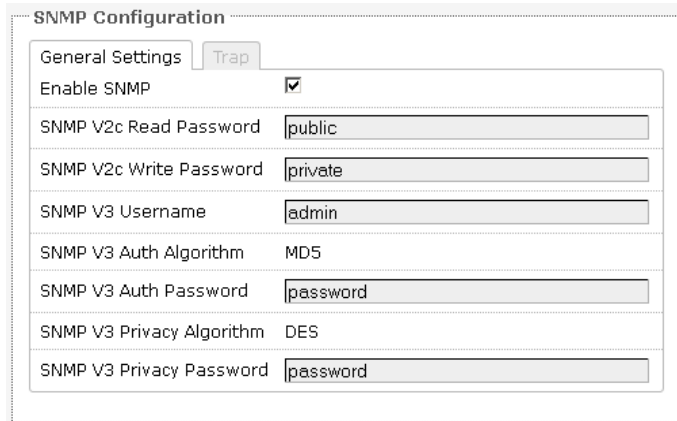
In the *System* → *SNMP* Page, you can configure SNMP V2c and SNMP V3.

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



The screenshot shows the 'SNMP Configuration' window with the 'General Settings' tab selected. The 'Trap' sub-tab is also active. The form contains the following fields:

Enable SNMP	<input checked="" type="checkbox"/>
SNMP V2c Read Password	public
SNMP V2c Write Password	private
SNMP V3 Username	admin
SNMP V3 Auth Algorithm	MD5
SNMP V3 Auth Password	password
SNMP V3 Privacy Algorithm	DES
SNMP V3 Privacy Password	password

Figure 30: 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 SNMP manager (NMS).

SNMP V2c Write Password: Sets the community string for read-write access by the SNMP manager.

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.

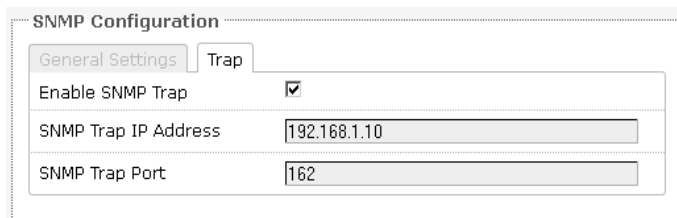
SNMP V3 Auth Algorithm: Shows the authentication algorithm used.

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

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

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

Trap



The screenshot shows the 'SNMP Configuration' window with the 'Trap' sub-tab selected. The form contains the following fields:

Enable SNMP Trap	<input checked="" type="checkbox"/>
SNMP Trap IP Address	192.168.1.10
SNMP Trap Port	162

Figure 31: 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.

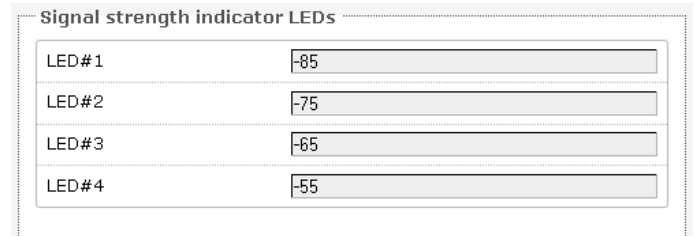
SNMP Trap Port: Sets the port number.

3.5 LED Configuration

The *System* → *LED Configuration* page customizes the behaviour of the LEDs.

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 dB) above which LEDs #1 to #4 would light up.



Signal strength indicator LEDs	
LED #1	-85
LED #2	-75
LED #3	-65
LED #4	-55

Figure 32: Signal strength indicator LEDs and their default threshold values in dB.



Note: The physical arrangement of LEDs on the router may differ for different models. For example, on the WPJ344 router, the LEDs starting from the one nearest the corner are: Power (green), Diagnostics (green), LED#1 (red), LED#2 (orange), LED#3 (green), and LED#4 (green).

3.6 Backup/Flash Firmware

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

3.6.1 Backup/Restore

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



Note: The backup archive file should be stored in a safe place because it contains the wireless password in clear text.

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.

3.6.2 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.

3.7 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* and *Discovery*.

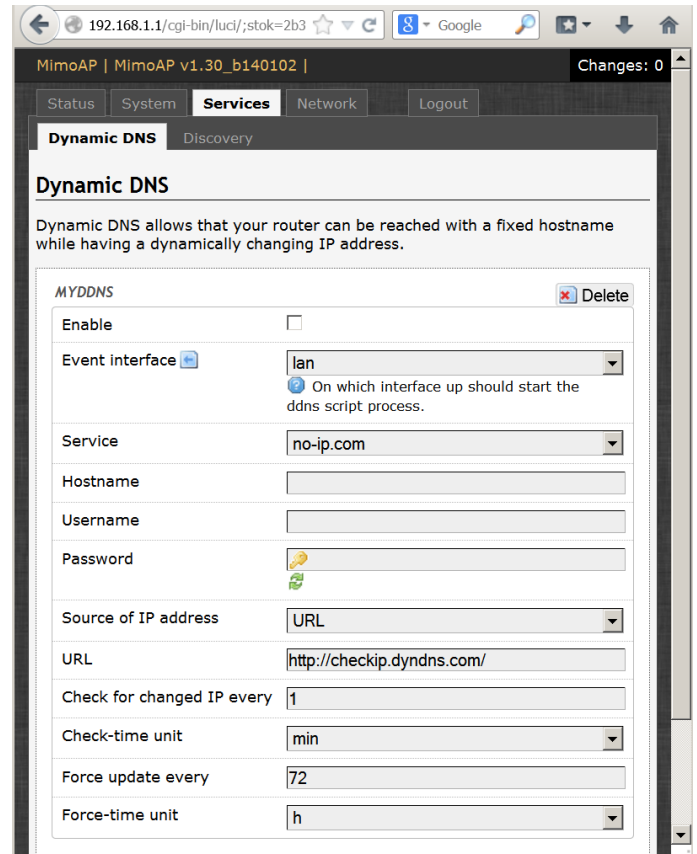


Figure 33: The *Services* top-level tab.

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.

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. `no-ip.com`.

Hostname: Specifies the hostname e.g. `y0033.no-ip.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 Discovery

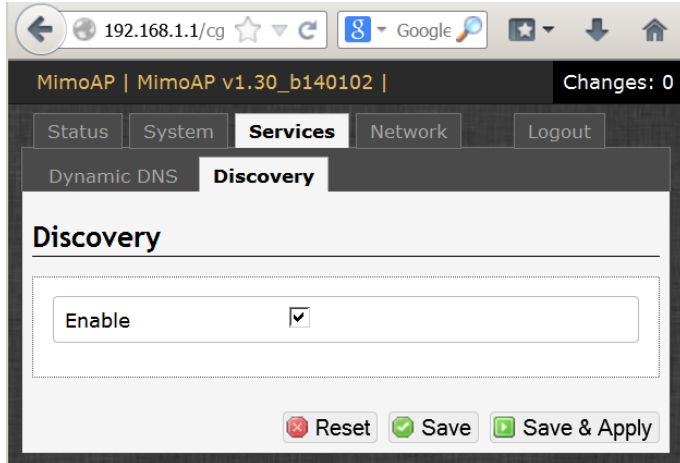


Figure 34: The *Services* → *Discovery* page.

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

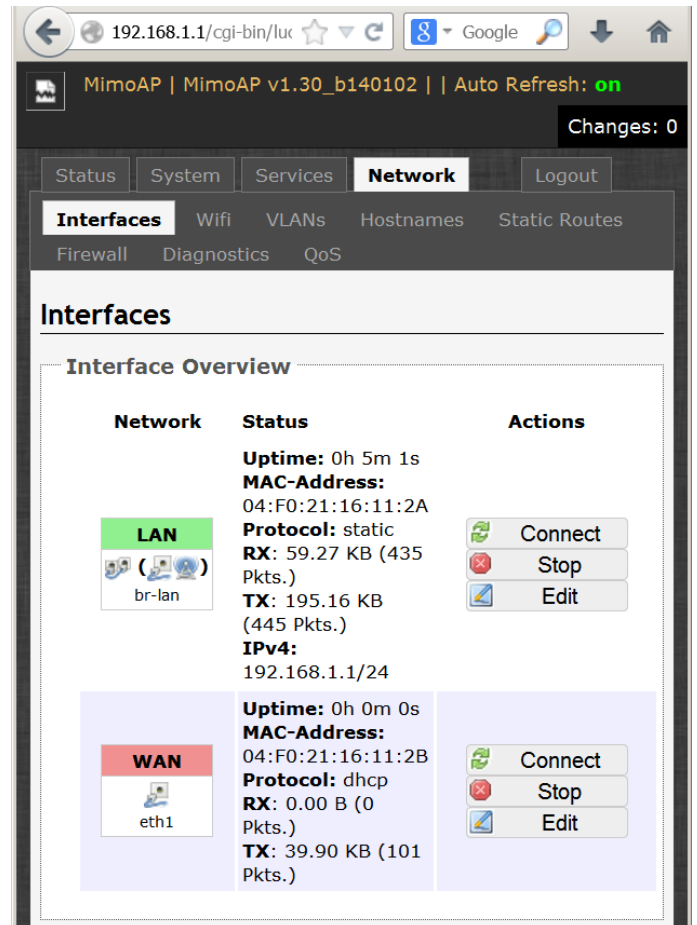


Figure 35: The *Network* top-level tab.

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.



Interface Overview		
Network	Status	Actions
<p>LAN</p>  <p>br-lan</p>	<p>Uptime: 1d 22h 47m 40s MAC-Address: 00:80:48:79:3A:A0 Protocol: static RX: 170.57 MB (785762 Pkts.) TX: 212.55 MB (715849 Pkts.) IPv4: 192.168.21.1/24</p>	<p>Connect Stop Edit</p>
<p>WAN</p>  <p>eth1</p>	<p>Uptime: 1d 22h 47m 34s MAC-Address: 00:80:48:79:3A:A1 Protocol: dhcp RX: 221.78 MB (1604852 Pkts.) TX: 122.44 MB (345360 Pkts.) IPv4: 192.168.3.118/24</p>	<p>Connect Stop Edit</p>

Figure 36: The *Interface Overview* on the *Network* → *Interfaces* page.

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

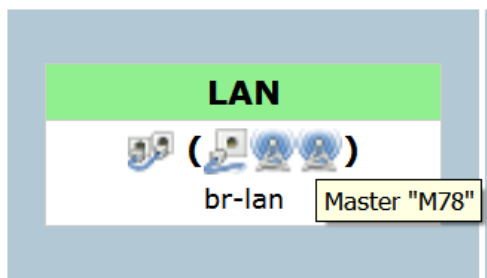


Figure 37: An infotip appears when hovering the mouse over an icon.

In Figure 37, 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 “M78” 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

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 38: Status of the “eth1” interface of the WAN zone.

Protocol: Chooses between *DHCP client* (default), where the device obtains its 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. 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 - PPTP

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 password* 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 password* 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 *No Interface* is selected, all interfaces would be within the LAN zone.



Note: For all the routers with the CompexWRT firmware, when the router is placed flat on the table, and you look at the Ethernet ports from the side, the LAN port is on the right and the WAN port is on the left, by default. However, the name that is assigned to the physical ports (eth0 or eth1) on the router may vary for different models of routers.

5.2 Interfaces - LAN

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

Figure 39: 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 its 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. 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.



Note: All the following options in this *DHCP Server* section depend on DHCP being enabled.

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.

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.

Hostname	MAC-Address	IPv4-Address	
MP7	00:37:6D:62:F6:C4	192.168.21.107	Delete
			Delete
Add			

Figure 40: 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
MP7	192.168.21.107	00:37:6d:62:f6:c4	11h 57m 54s

Figure 41: 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. The wireless local area networks (WLANs) are displayed.

The screenshot shows the 'Wireless Overview' page with two radio configurations. At the top, there are tabs for 'wifi1: Master "M6"' and 'wifi0: Master "M7"'. The first radio is 'AR9220 802.11abgn Radio' with channel 1 (2.412 GHz) and a bitrate of 300 Mbit/s. It has an SSID of 'M7' and a BSSID of '00:80:48:79:3A:A2'. The second radio is 'Generic 802.11bg Radio' with an SSID of 'M6' and a BSSID of 'Master Wireless is disabled or not associated'. Both radios have 'Add', 'Disable', and 'Edit' buttons.

Figure 42: The [Wireless Overview](#) page showing two radios.

In Figure 42, two tabs are shown at the top, `wifi0: Master "M7"` and `wifi1: Master "M6"`. These correspond to the two radios shown below.

The buttons are explained as follows.

Add: Allows you to add virtual access points (VAPs) to the radio.

Enable: Enables the radio.

Disable: Disables the radio.

Edit: Brings you to the configuration page. Clicking this button is equivalent to clicking the corresponding tab above e.g. `wifi0: Master "M7"` for the radio with SSID given as "M7".



Note: When this device 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
04:F0:21:16:11:2C	M7	-59 dBm	-62,-62,-95 dBm	-95 dBm	222.8 Mbit/s	254.9 Mbit/s	89 %

Figure 43: 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.

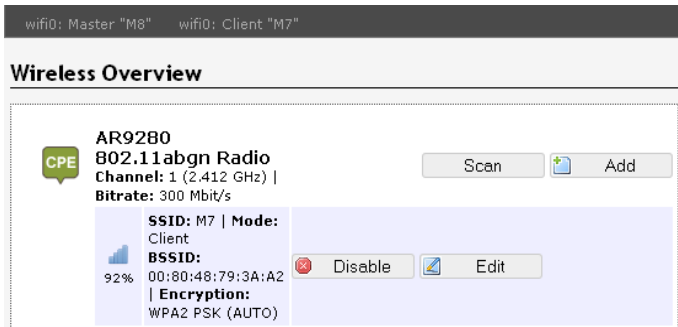


Figure 44: The Wireless Overview page showing a radio as a Client (station).



Note: The following buttons are for the device 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 wireless local area network (WLAN) would bring you to the configuration page. This page contains the sections *Device Configuration* and *Interface Configuration*.

5.4.1 Device Configuration

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.

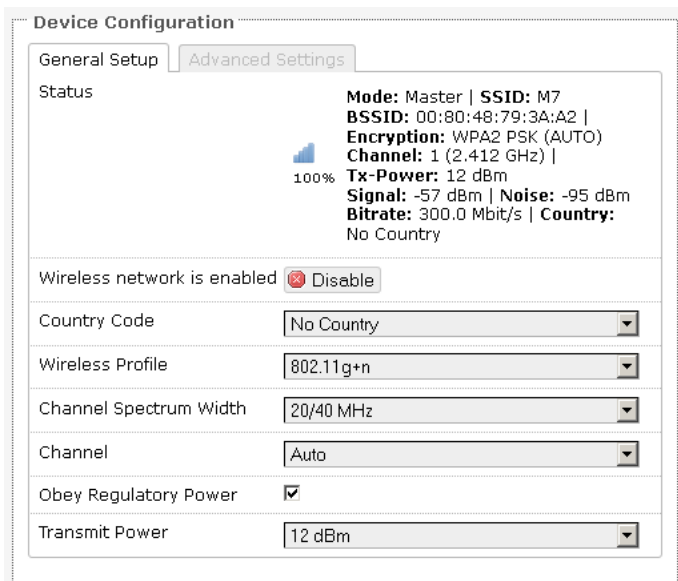


Figure 45: The Wifi Device Configuration section.

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.

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.

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: Satisfies the legally permitted maximum for the equivalent isotropically radiated power (EIRP) limits of the selected country.

Transmit Power: Chooses the transmit power of the radio e.g. 4 dBm, 5 dBm, ..., 22 dBm or Max. This is the total power supplied to the antennas of the radio.

Advanced Settings

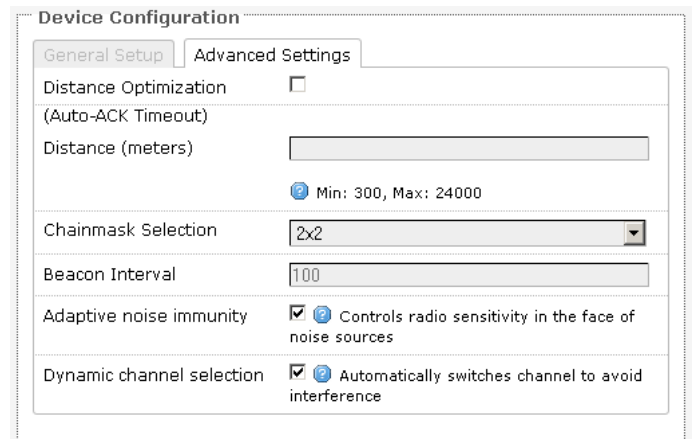


Figure 46: *Advanced Settings* for the Wifi Device Configuration.

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.



Note: The following options are for the device operating as an access point (AP).

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 non-WLAN 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

Interface Configuration	
General Setup Wireless Security MAC-Filter Advanced Settings	
Mode	Access Point
ESSID	M7
Guard Interval	Short
Data Rate (Mbps)	Auto
Hide ESSID	<input type="checkbox"/>

Figure 47: 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.)



Note: If the goal is securing your network, use WPA or preferably WPA2 encryption. Hiding the ESSID does not provide complete security.

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.

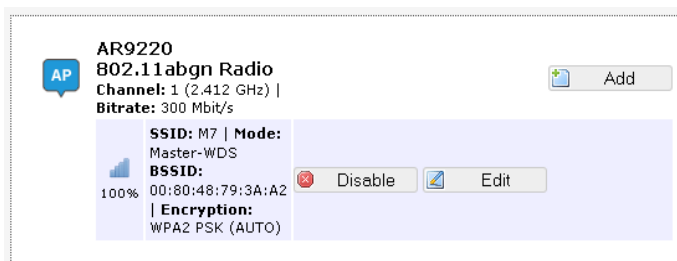


Figure 48: The first router is set to the AP WDS mode.

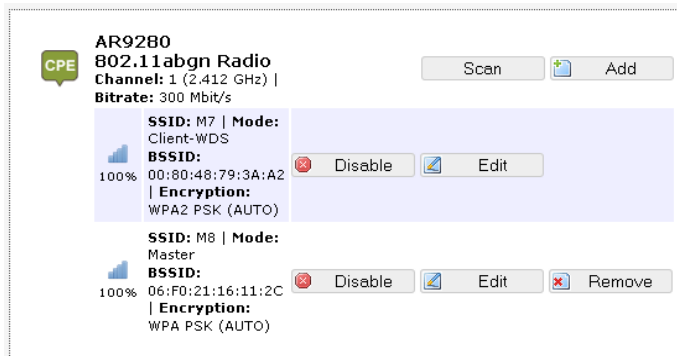


Figure 49: The second router is set to the Station WDS mode.

Multiple stations or *Stations WDS* can connect to an AP WDS. In Figure 49, the *Add* button creates a virtual access point (VAP) on the second router. You can choose *AP mode* or *AP WDS mode* for the VAP's wireless network e.g. "M8" so that devices in *Station mode* or *Station WDS mode* can connect to this network. The pair of *AP WDS* and *Station WDS* (with VAP) together extend the wireless coverage from the location of the *AP WDS* to that of the *Station WDS*. Therefore the *Station WDS* (with VAP) 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.

Wireless Security



Figure 50: 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*, *WPA-PSK/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.

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.



Note: Valid HEX characters are numbers 0-9 and letters A-F, case insensitive. Valid ASCII characters are numbers and the letters of the English alphabet, case sensitive. Based on the number of characters, the key is automatically checked for validity. Invalid keys are represented by red dots while valid keys are represented by black dots. Click the green arrows icon beside the text field to reveal/hide the password.

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)

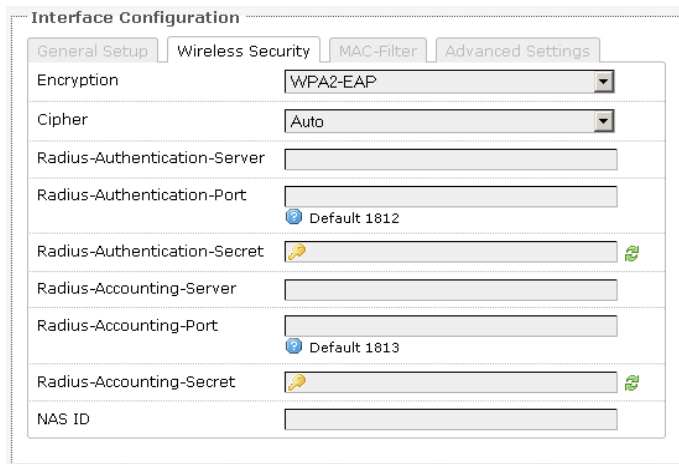


Figure 51: Encryption options for WPA-EAP or WPA2-EAP in AP mode.

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.



Note: Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users that connect and use a network service.

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)

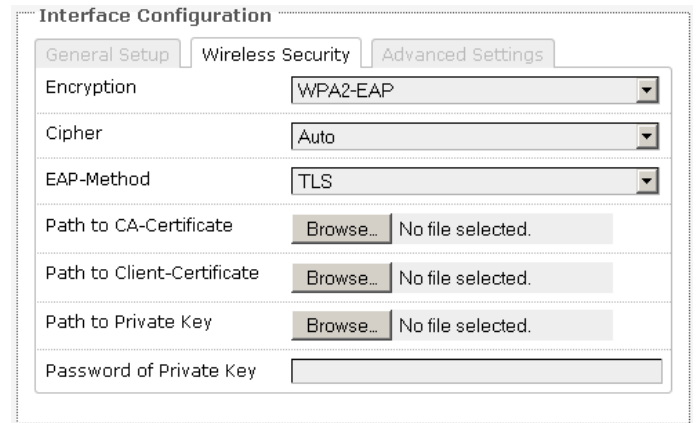


Figure 52: Encryption options for WPA-EAP or WPA2-EAP in Station mode.

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.



Note: The certificate authority (CA) is a trusted third party that issues digital certificates. In a public key infrastructure scheme, a digital certificate certifies the ownership of a public key by the named subject of the 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.

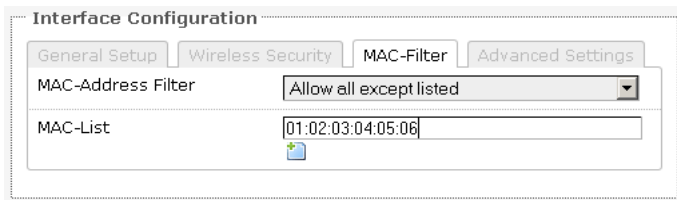


Figure 53: Configuring the *MAC-Filter* for a Wifi AP.

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

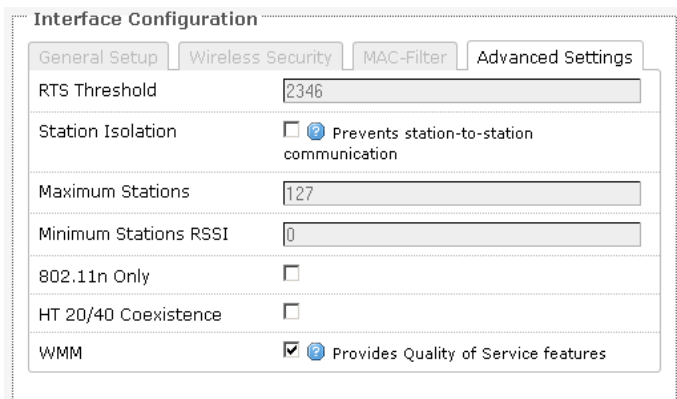


Figure 54: *Advanced Settings* for the Wifi Interface.

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.



Note: The following options for *Station Isolation*, *Maximum Stations*, *Minimum Stations RSSI*, and *802.11n Only* are available only for a device operating as an AP.

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

5.5.1 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.

Managed VLAN	VLAN ID	Priority	IP address	Netmask	Bridge WIF1	Wifi Tagging	Description
<input checked="" type="checkbox"/>	0		192.168.21.1	255.255.255.0	All Others	Disabled	Default LAN net
<input checked="" type="checkbox"/>	3355	4	192.33.55.1	255.255.255.0	M7	Enabled	VLAN Network Delete

Figure 55: *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. Let *VID* be this number. The "eth0" port is tagged with *VID* to give "eth0.VID". This port can have multiple tags corresponding to different VLANs. An "eth0.VID" port would only accept frames that have been tagged with the VLAN ID *VID*.

Priority: Chooses the priority for transmitting packets. 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 “eth0.VID” port. The choice *All Others* would select all other wireless networks that are currently not selected.

Wifi Tagging: Should be set to Enabled. This tags the Ethernet frames sent over Wifi. This does not add a second tag (QinQ). The wireless interface “ath0” of this VLAN would be tagged to give “ath0.VID” for example.

Description: Provides a short description of the VLAN.

5.5.2 VLAN Ethernet Trunk

The VLAN Ethernet Trunk uses a wireless network as a trunk link to connect physically separate VLANs having the same VLAN ID.

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

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

Figure 56: 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 that would act as a trunk link.

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.

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

Figure 57: Custom hostname entries.



Note: The computers in the same subnet need to set the IP address of this device as their preferred DNS server in order to interpret these custom hostnames.

5.7 Static Routes

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

Interface	Target	IPv4-Netmask	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

Figure 58: 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	<input checked="" type="checkbox"/>
Drop invalid packets	<input type="checkbox"/>
Input	accept
Output	accept
Forward	reject

Figure 59: 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

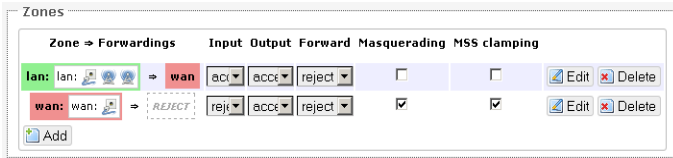


Figure 60: The *Zones* section showing the default settings for the firewall zones.

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.

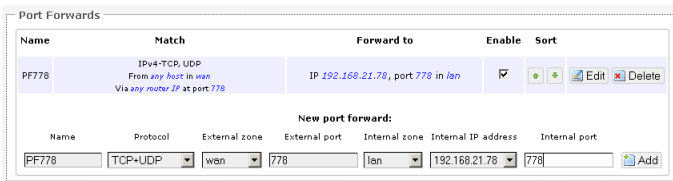


Figure 61: Adding a port forwarding rule.

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.

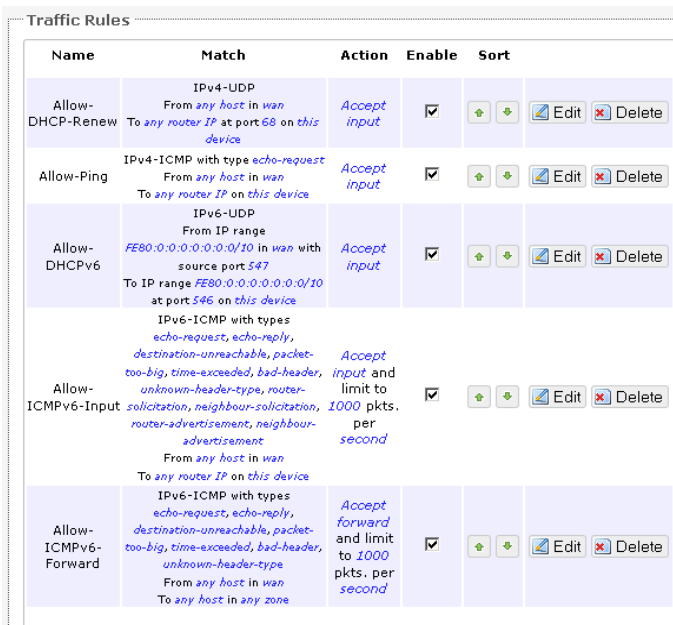


Figure 62: Firewall *Traffic Rules* with the default settings.

Open ports on router:



New forward rule:

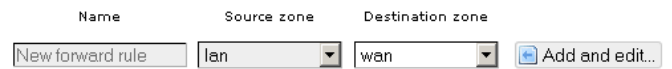


Figure 63: You can choose to open ports on the router or add new forwarding rules.

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.



Figure 64: *Source NAT*.

5.9 Diagnostics

5.9.1 Network Utilities

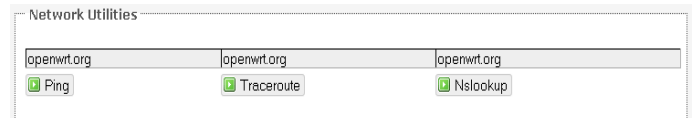


Figure 65: *Network Utilities* consist of *Ping*, *Traceroute*, and *Nslookup*.

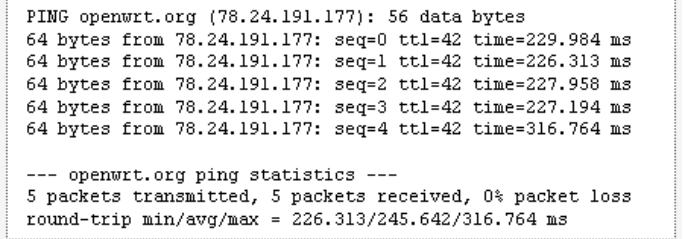


Figure 66: Result of *Ping*.

Chapter 6: Final Notes

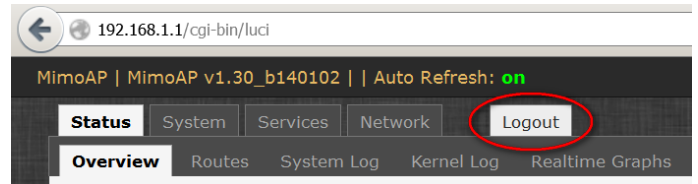


Figure 70: The *Logout* button is circled.

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

Troubleshooting steps

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.

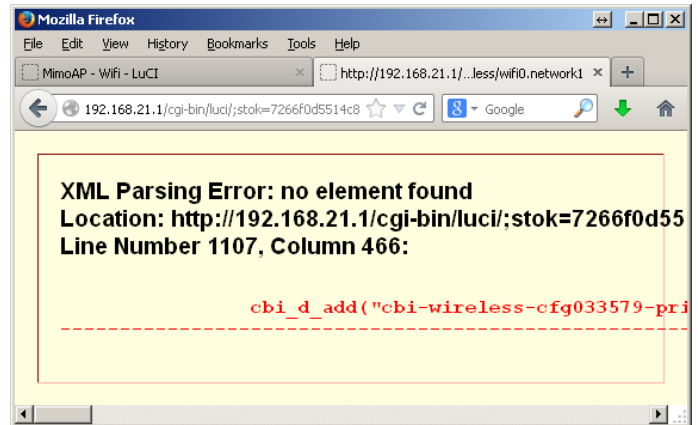


Figure 71: XML Parsing Error.

Solution: Re-enter the IP address into the browser. For example, if the current URL is `192.168.21.1/cgi-bin/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.

Unresponsive router

Symptom: The router does not respond.

Solution: Turn off the router for 10 seconds and then turn it on again.

6.1 Resetting to factory default

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. After a while, the flash would be erased and the router would reboot into its factory default state.

```
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 67: 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 68: 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 selected by addresses, ports, or services. You can limit the download and upload speeds. Network QoS is disabled by default.

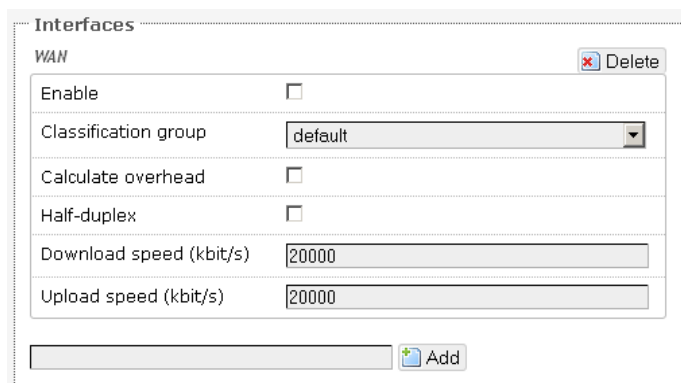


Figure 69: *Network QoS* settings.