High-Power Ceiling Mount Wireless 300N PoE Access Point

User manual

Version 1.0 | 7/15/2015

Table of Content

Chapter 1 Product Introduction

The 300M High Power Wireless Ceiling AP is based on 802.11n standard, using MIMO, OFDM technology, provides a wireless data transmission rate up to 300Mbps; using high power PA design of wireless power up to 400mW, long distance transmission and provide greater coverage simultaneously has signal strong penetration force; by ceiling type installation design that is very suitable enterprises, hotels, airports, schools and other indoor or public places, to realize high-speed network coverage. At the same time the product support Ethernet PoE power and external power adapter, support the IEEE802.3af standard power supply, so that the AP can also be installed in places without power supply, reduces the installation cost, also make the installation and use more simple and convenient, flexible network layout and installation, improve the network layout. This AP also provides very convenient comprehensive network management functions, support a variety of wireless data encryption, can guarantee the security of data in the wireless network transmission, support for IP, for AP SSID, encryption, upgrade, reset and restart management function.

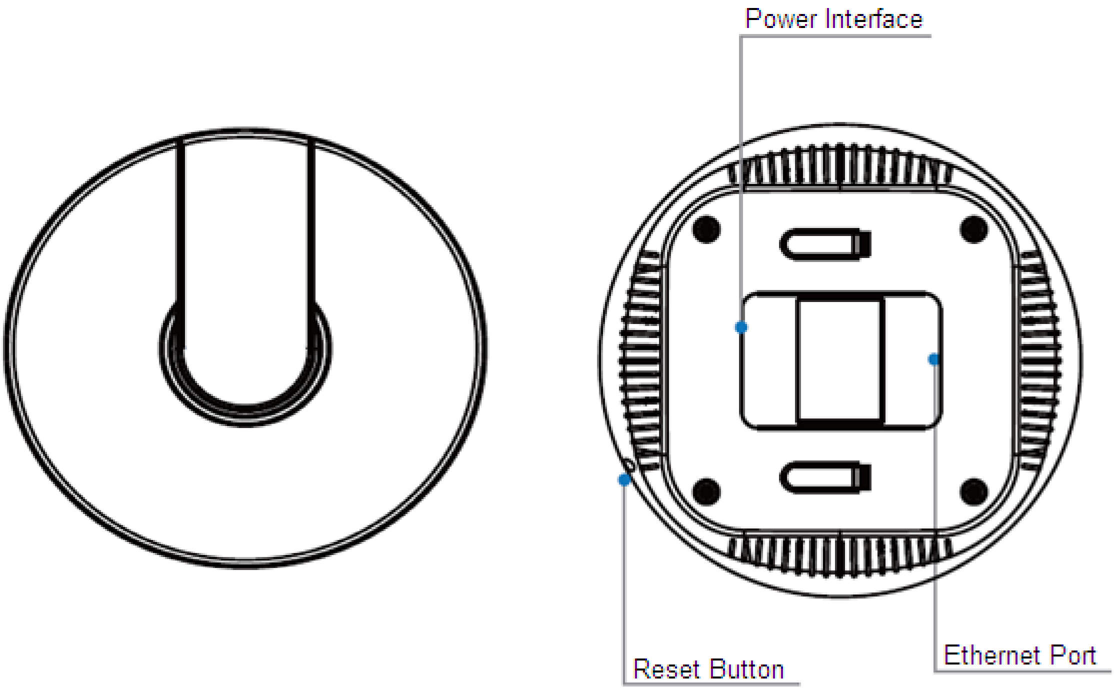
1.1 Product Features

- 1-Port 10/100Mbps RJ45 Ethernet interface, Supports standard 802.3af PoE by electricity.
- Be consistent with 802.11b/g/n wireless protocol, providing up to 300Mbps wireless rate.
- Wireless high power up to 400mW meet the remote transmission and large area coverage.
- Support AP, WDS mode, can easily realize the wireless AP, wireless repeater, a wireless point-to-point, point to multipoint wireless bridge bridge.
- Support 64/128 bit WEP encryption, wpa/wpa2, wpa-psk/wpa2-psk encryption and security mechanism.
- Support Web interface management, which can be configured and management of the rich AP.
- Using ceiling type installation design, indoor decoration. With small size, simple installation and stability.

1.2 Package Contents

- Ceiling AP
- Set of installation accessories
- User Manual
- Warranty Card

1.3 Hardware Description



Ethernet Port: Ethernet port jack (RJ45). For wired Ethernet connection, and PoE -powered devices to be powered by the port to the AP.

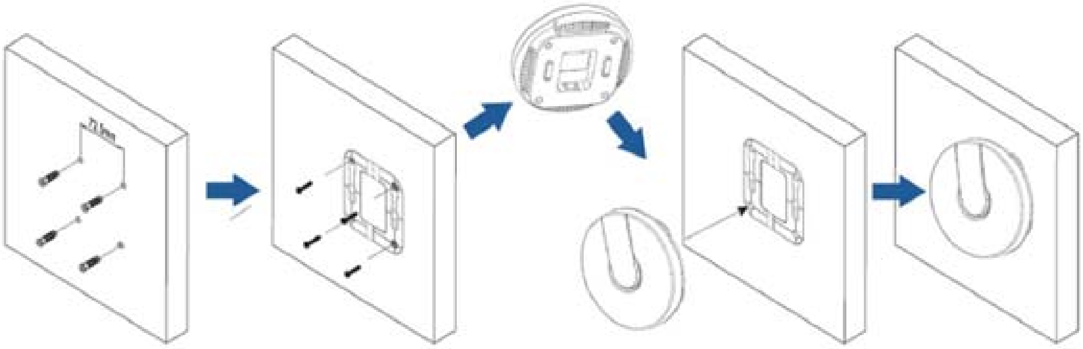
Power Interface: When the Ethernet does not support the PoE power supply, the port can be connected to DC12V/1A power supply adapter.

Reset Button: If you need to restore the AP to the factory default settings, please use sharp object to hold the reset button for about 6 seconds after release, AP will automatically restore factory settings and restart.

Chapter 2 Hardware Installation Wizard

1. The AP chassis are placed on the wall or the ceiling, with mark pen mark hole fixed position, and then drilling.

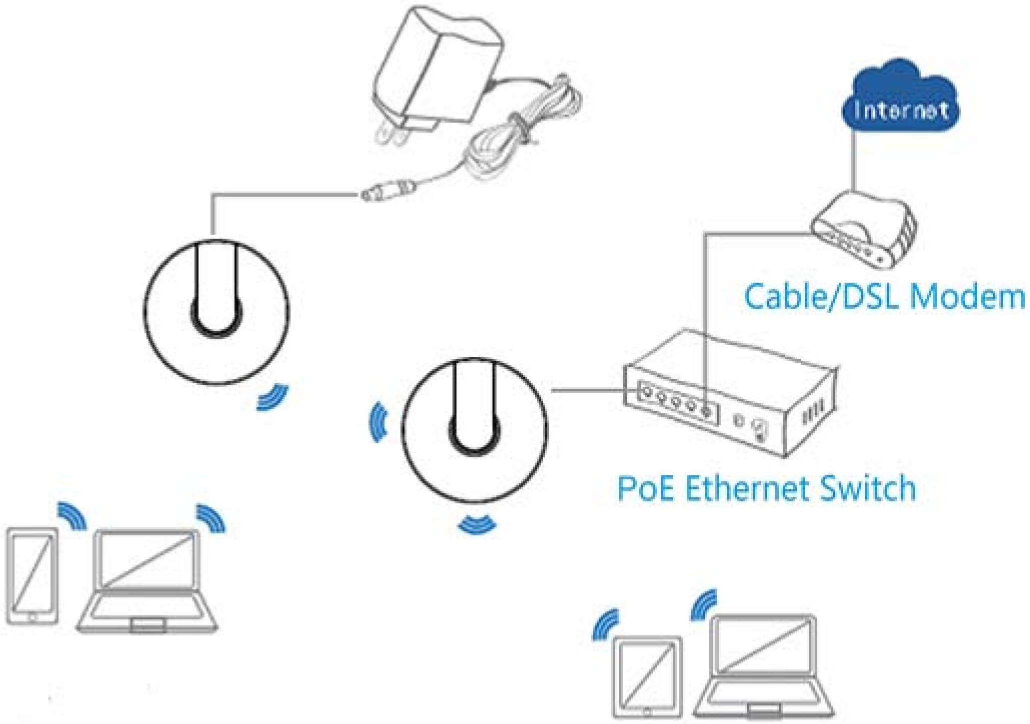
2. AP chassis with screws is fixed on the wall or the ceiling.



3. Will support the PoE Ethernet cable to the AP has been configured Ethernet ports (optional up or down), if you do not support PoE power supply, DC 12V/1A power supply is connected.

4. The AP linked to the fixed good chassis.

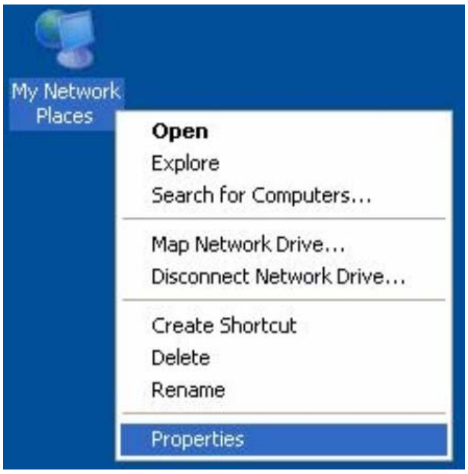
Note: The default SSID for the AP: **OpenWrt**
The default wireless password: **12345678**



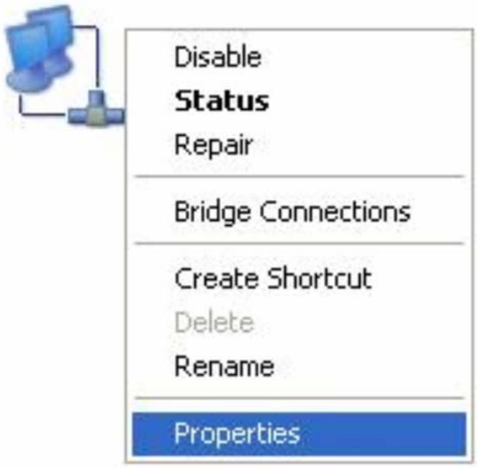
Chapter 3 Configuration Management

3.1 Set Network Configuration

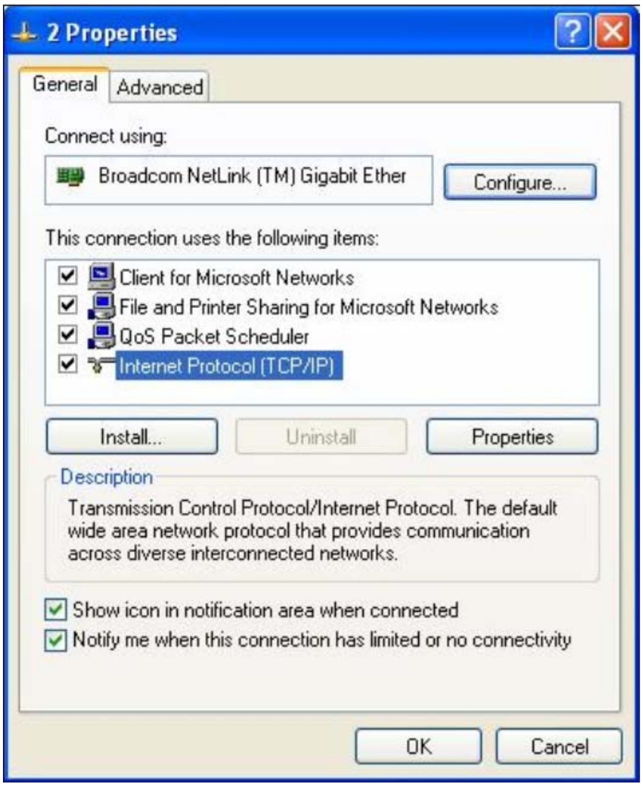
1. On your computer desktop, right click "**My Network Places**" and select "**Properties**".



2. Right click **"local Area Network Connection"** and select **"Properties"**.



3. Select "**Internet Protocol(TCP/IP)**" and click "**Properties**".



2 Properties

General | Advanced

Connect using:

Broadcom NetLink (TM) Gigabit Ether

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

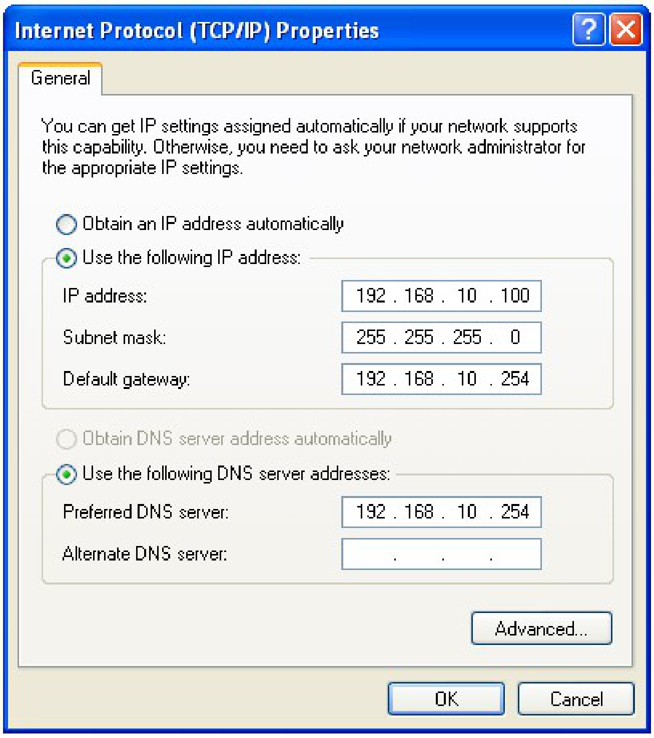
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

4. Select "**Use the following IP address(s)**" and "**Use the following DNS server address**". Click "**OK**".



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 10 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 10 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 10 . 254
Alternate DNS server:	. . .

IP address: 192.168.10.XXX: (XXX is a number from 1~253)

Subnet mask: 255.255.255.0

Default gateway: 192.168.10.254

Preferred DNS server: 192.168.10.254

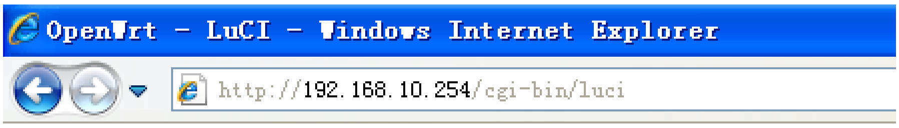
Click "**OK**" to save the setting.

Note: IP address set here is only for entering the AP management page to set specific IP address setting, please refer to the actual use of the environment.

3.2 Login Device Management Interface

1. Connect to the AP through a wireless network or wired network.

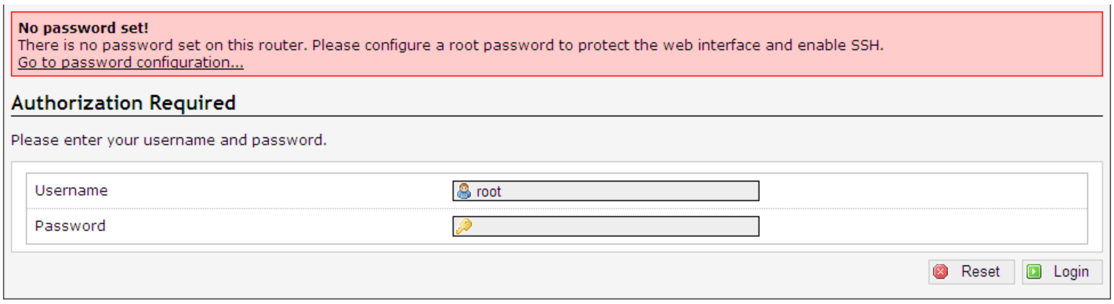
2. Open IE browser, in the address bar enter http://192.168.10.254, press the Enter key to enter the login screen.



OpenWrt – LuCI – Windows Internet Explorer

http://192.168.10.254/cgi-bin/luci

3. The default user name is **root**, the password is **blank**, click on the "Login", the login page as shown below.



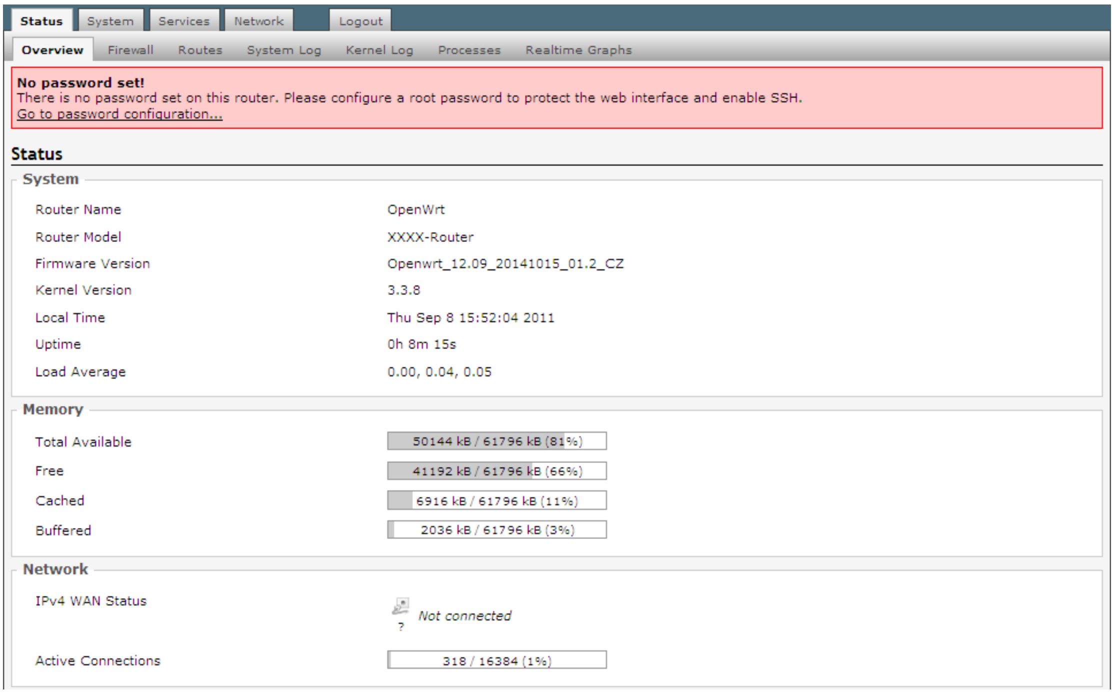
No password set!
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
Go to password configuration...

Authorization Required

Please enter your username and password.

Username	root
Password	

4. After the above steps to successfully log AP management interface page. Click Home at the top of the main menu bar to configure the corresponding function.



No password set!
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
Go to password configuration...

Status

System

Router Name	OpenWrt
Router Model	XXXX-Router
Firmware Version	Openwrt_12.09_20141015_01.2_CZ
Kernel Version	3.3.8
Local Time	Thu Sep 8 15:52:04 2011
Uptime	0h 8m 15s
Load Average	0.00, 0.04, 0.05

Memory

Total Available	50144 kB / 61796 kB (81%)
Free	41192 kB / 61796 kB (66%)
Cached	6916 kB / 61796 kB (11%)
Buffered	2036 kB / 61796 kB (3%)

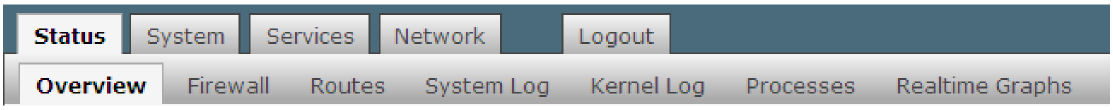
Network

IPv4 WAN Status	? *Not connected*
Active Connections	318 / 16384 (1%)

Chapter 4 Function Deployment

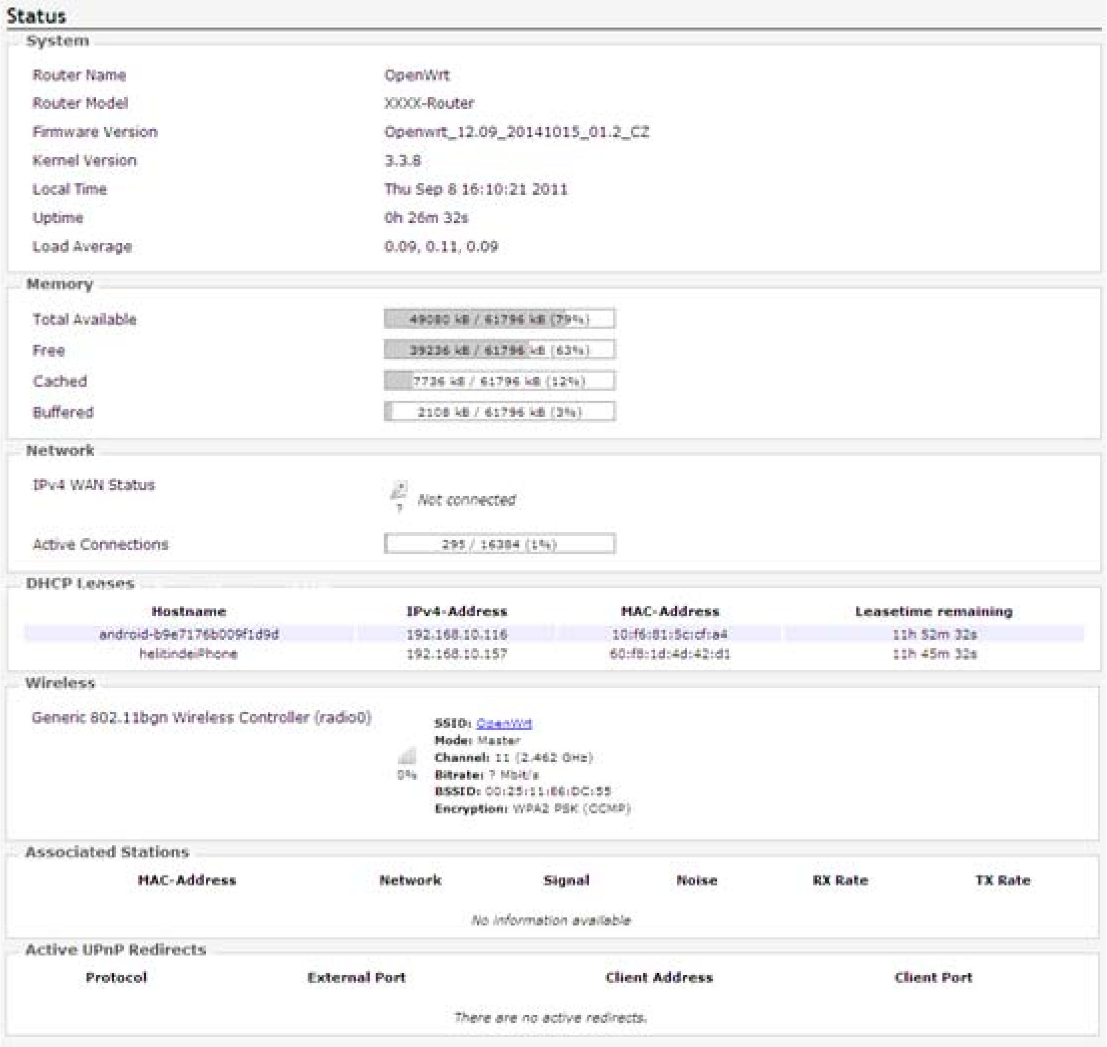
4.1 Status

Click on "Status", you can see the Overview, Firewall, Routes, System Log, Kernel Log, Processes, Realtime Graphs options.



4.1.1 Overview

Click on the "Status>Overview" option, you can see the following interface.



Status

System

Router Name	OpenWrt
Router Model	XXXX-Router
Firmware Version	Openwrt_12.09_20141015_01.2_CZ
Kernel Version	3.3.8
Local Time	Thu Sep 8 16:10:21 2011
Uptime	0h 26m 32s
Load Average	0.09, 0.11, 0.09

Memory

Total Available	49080 kB / 61796 kB (79%)
Free	39236 kB / 61796 kB (63%)
Cached	7736 kB / 61796 kB (12%)
Buffered	2108 kB / 61796 kB (3%)

Network

IPv4 WAN Status	*Not connected*
Active Connections	295 / 16384 (1%)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-b9e7176b009f1d9d	192.168.10.116	10:f6:81:5c:cf:a4	11h 52m 32s
helitindeiPhone	192.168.10.157	60:f8:1d:4d:42:d1	11h 45m 32s

Wireless

Generic 802.11bgn Wireless Controller (radio0)

0%
SSID: OpenWrt
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: ? Mbit/s
BSSID: 00:25:11:86:DC:55
Encryption: WPA2 PSK (CCMP)

Associated Stations

MAC-Address	Network	Signal	Noise	RX Rate	TX Rate

No information available

Active UPnP Redirects

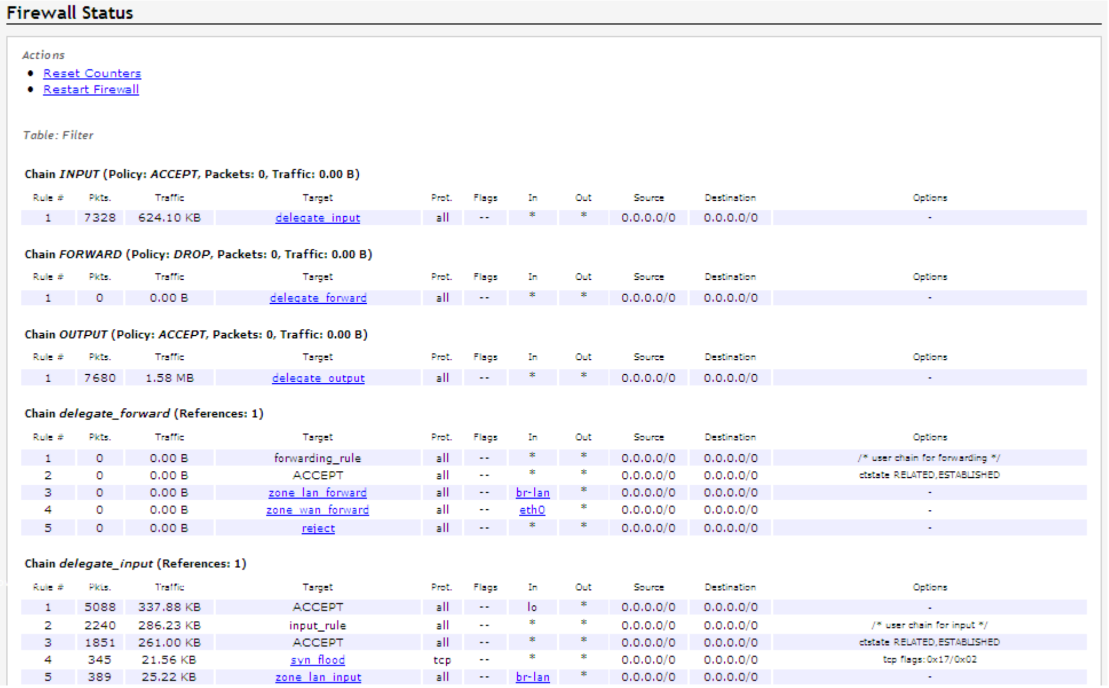
Protocol	External Port	Client Address	Client Port

There are no active redirects.

Through this interface, you can learn "System" information(AP Name, AP Model, Firmware Version, Kernel Version, Local Time, Uptime, Load Average), "Memory" information(Total Available, Free, Cached, Buffered), "Network" information(IPv4 WAN Status), "DHCP Leases" information, "Wireless" information, "Associated Stations" information, "Active UPnP Redirects" information.

4.1.2 Firewall

Click on the "Status>Firewall" option, you can see the following interface.



Firewall Status

Actions

- Reset Counters
- Restart Firewall

Table: Filter

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	7328	624.10 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

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

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

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

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	7680	1.58 MB	delegate_output	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain *delegate_forward* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	0	0.00 B	forwarding_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for forwarding */
2	0	0.00 B	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED
3	0	0.00 B	zone_lan_forward	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-
4	0	0.00 B	zone_wan_forward	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0	-
5	0	0.00 B	reject	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

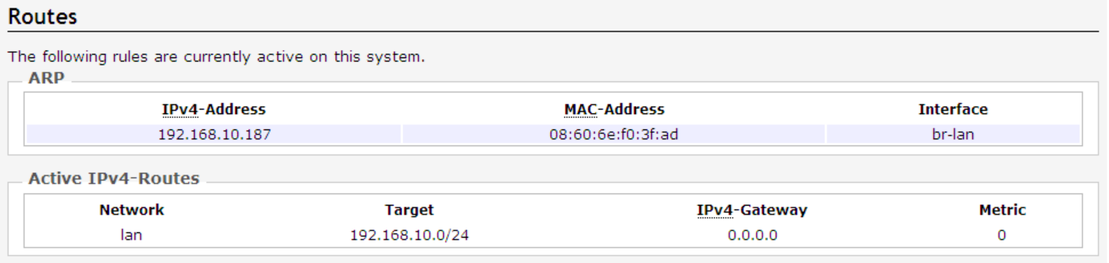
Chain *delegate_input* (References: 1)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	5088	337.88 KB	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0	-
2	2240	286.23 KB	input_rule	all	--	*	*	0.0.0.0/0	0.0.0.0/0	/* user chain for input */
3	1851	261.00 KB	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED
4	345	21.56 KB	syn_flood	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02
5	389	25.22 KB	zone_lan_input	all	--	br-lan	*	0.0.0.0/0	0.0.0.0/0	-

Through this interface, you can know what is allowed by the packet, which is filtered packets.

4.1.3 Routes

Click on the "Status>Routes" option, you can see the following interface.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.10.187	08:60:6e:f0:3f:ad	br-lan

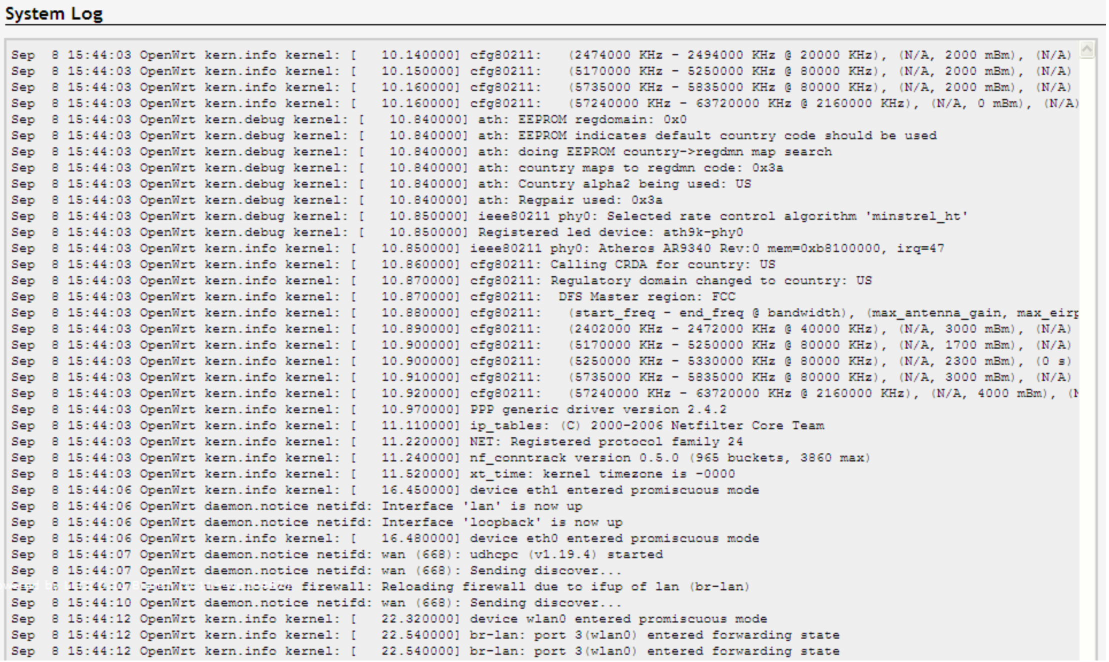
Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
lan	192.168.10.0/24	0.0.0.0	0

Through this interface, you can learn the relevant information systems active connections: IP address, MAC address, and gateway.

4.1.4 System Log

Click on the "Status>System Log" option, you can see the following interface.



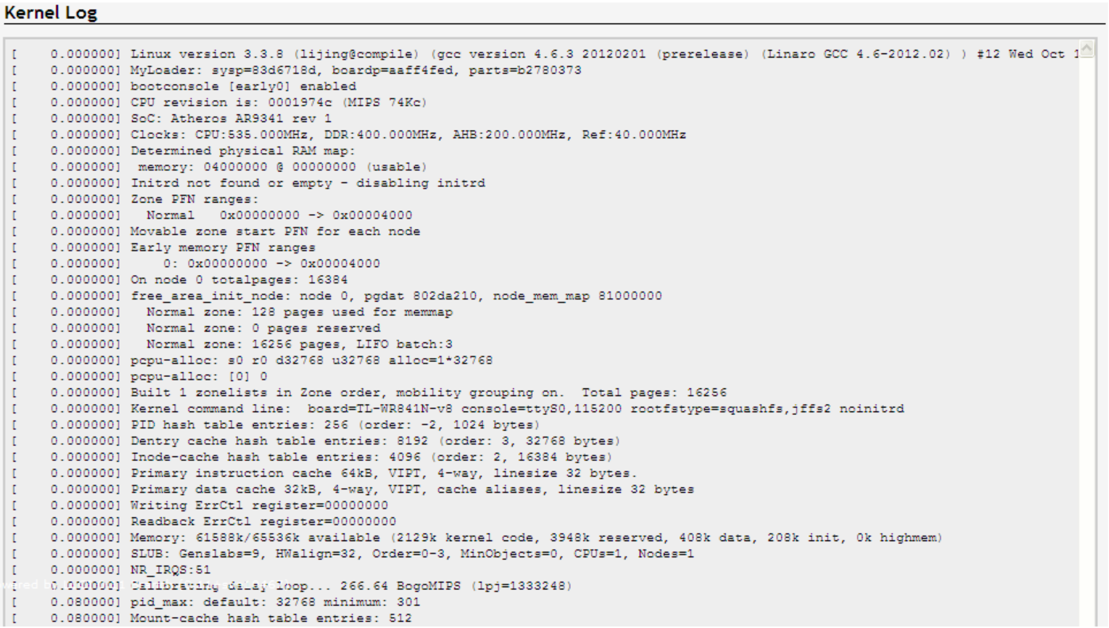
System Log

```
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.140000] cfg80211:   (2474000 KHz - 2494000 KHz @ 20000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.150000] cfg80211:   (5170000 KHz - 5250000 KHz @ 80000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.160000] cfg80211:   (5735000 KHz - 5835000 KHz @ 80000 KHz), (N/A, 2000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.160000] cfg80211:   (57240000 KHz - 63720000 KHz @ 2160000 KHz), (N/A, 0 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: EEPROM regdomain: 0x0
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: EEPROM indicates default country code should be used
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: doing EEPROM country->regdmn map search
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: country maps to regdmn code: 0x3a
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: Country alpha2 being used: US
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.840000] ath: Regpair used: 0x3a
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.850000] ieee80211 phy0: Selected rate control algorithm 'minstrel_ht'
Sep  8 15:44:03 OpenWrt kern.debug kernel: [   10.850000] Registered led device: ath9k-phy0
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.850000] ieee80211 phy0: Atheros AR9340 Rev:0 mem=0xb8100000, irq=47
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.860000] cfg80211: Calling CRDA for country: US
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.870000] cfg80211: Regulatory domain changed to country: US
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.870000] cfg80211:  DFS Master region: FCC
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.880000] cfg80211:   (start_freq - end_freq @ bandwidth), (max_antenna_gain, max_eirp
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.890000] cfg80211:   (2402000 KHz - 2472000 KHz @ 40000 KHz), (N/A, 3000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.900000] cfg80211:   (5170000 KHz - 5250000 KHz @ 80000 KHz), (N/A, 1700 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.900000] cfg80211:   (5250000 KHz - 5330000 KHz @ 80000 KHz), (N/A, 2300 mBm), (0 s)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.910000] cfg80211:   (5735000 KHz - 5835000 KHz @ 80000 KHz), (N/A, 3000 mBm), (N/A)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.920000] cfg80211:   (57240000 KHz - 63720000 KHz @ 2160000 KHz), (N/A, 4000 mBm), (N
Sep  8 15:44:03 OpenWrt kern.info kernel: [   10.970000] PPP generic driver version 2.4.2
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.110000] ip_tables: (C) 2000-2006 Netfilter Core Team
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.220000] NET: Registered protocol family 24
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.240000] nf_conntrack version 0.5.0 (965 buckets, 3860 max)
Sep  8 15:44:03 OpenWrt kern.info kernel: [   11.520000] xt_time: kernel timezone is -0000
Sep  8 15:44:06 OpenWrt kern.info kernel: [   16.450000] device eth1 entered promiscuous mode
Sep  8 15:44:06 OpenWrt daemon.notice netifd: Interface 'lan' is now up
Sep  8 15:44:06 OpenWrt daemon.notice netifd: Interface 'loopback' is now up
Sep  8 15:44:06 OpenWrt kern.info kernel: [   16.480000] device eth0 entered promiscuous mode
Sep  8 15:44:07 OpenWrt daemon.notice netifd: wan (668): udhcpc (v1.19.4) started
Sep  8 15:44:07 OpenWrt daemon.notice netifd: wan (668): Sending discover...
Sep  8 15:44:07 OpenWrt user.notice firewall: Reloading firewall due to ifup of lan (br-lan)
Sep  8 15:44:10 OpenWrt daemon.notice netifd: wan (668): Sending discover...
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.320000] device wlan0 entered promiscuous mode
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.540000] br-lan: port 3(wlan0) entered forwarding state
Sep  8 15:44:12 OpenWrt kern.info kernel: [   22.540000] br-lan: port 3(wlan0) entered forwarding state
```

Through this interface, you can get information link establishment fails, the packet filter log information, etc. through the log. By logging on to the log host, the system administrator can understand the log events for log analysis. Logs can help administrators locate faults, troubleshooting, can also help administrators to manage network security.

4.1.5 Kernel Log

Click on the "Status>Kernel Log" option, you can see the following interface.



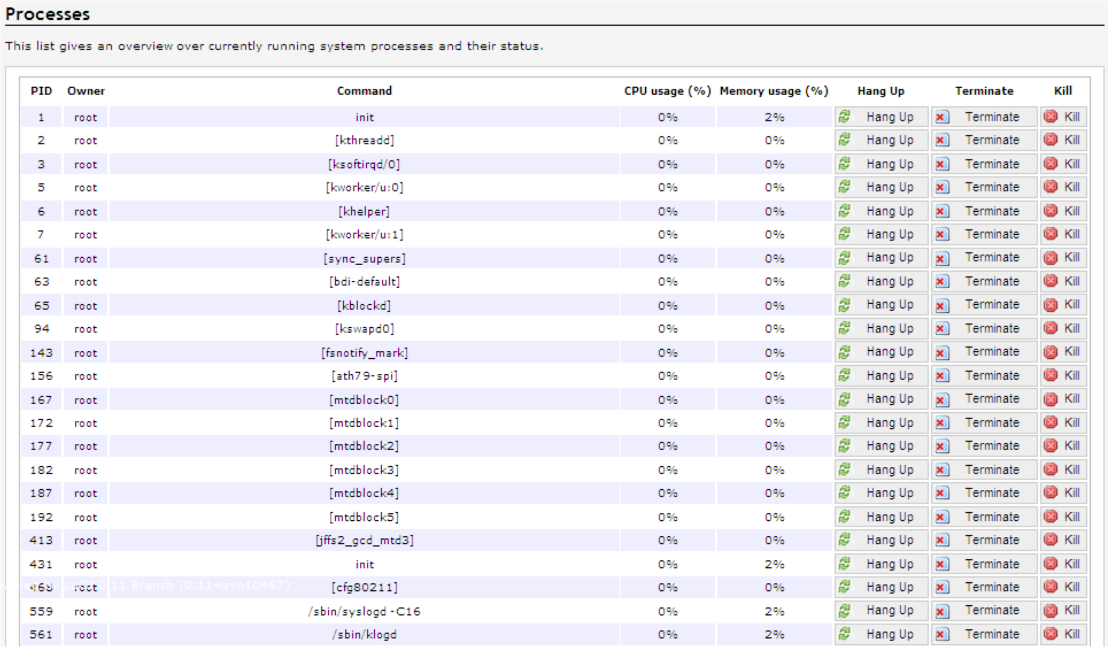
Kernel Log

```
[    0.000000] Linux version 3.3.8 (lijing@compile) (gcc version 4.6.3 20120201 (prerelease) (Linaro GCC 4.6-2012.02) ) #12 Wed Oct 1
[    0.000000] MyLoader: sysp=83d6718d, boardp=aaff4fed, parts=b2780373
[    0.000000] bootconsole [early0] enabled
[    0.000000] CPU revision is: 0001974c (MIPS 74Kc)
[    0.000000] SoC: Atheros AR9341 rev 1
[    0.000000] Clocks: CPU:535.000MHz, DDR:400.000MHz, AHB:200.000MHz, Ref:40.000MHz
[    0.000000] Determined physical RAM map:
[    0.000000]  memory: 04000000 @ 00000000 (usable)
[    0.000000] Initrd not found or empty - disabling initrd
[    0.000000] Zone PFN ranges:
[    0.000000]   Normal   0x00000000 -> 0x00004000
[    0.000000] Movable zone start PFN for each node
[    0.000000] Early memory PFN ranges
[    0.000000]     0: 0x00000000 -> 0x00004000
[    0.000000] On node 0 totalpages: 16384
[    0.000000] free_area_init_node: node 0, pgdat 802da210, node_mem_map 81000000
[    0.000000]   Normal zone: 128 pages used for memmap
[    0.000000]   Normal zone: 0 pages reserved
[    0.000000]   Normal zone: 16256 pages, LIFO batch:3
[    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: 16256
[    0.000000] Kernel command line:  board=TL-WR841N-v8 console=ttyS0,115200 rootfstype=squashfs,jffs2 noinitrd
[    0.000000] PID hash table entries: 256 (order: -2, 1024 bytes)
[    0.000000] Dentry cache hash table entries: 8192 (order: 3, 32768 bytes)
[    0.000000] Inode-cache hash table entries: 4096 (order: 2, 16384 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
[    0.000000] Readback ErrCtl register=00000000
[    0.000000] Memory: 61588k/65536k available (2129k kernel code, 3948k reserved, 408k data, 208k init, 0k highmem)
[    0.000000] SLUB: Genslabs=9, HWalign=32, Order=0-3, MinObjects=0, CPUs=1, Nodes=1
[    0.000000] NR_IRQS:51
[    0.020000] Calibrating delay loop... 266.64 BogoMIPS (lpj=1333248)
[    0.080000] pid_max: default: 32768 minimum: 301
[    0.080000] Mount-cache hash table entries: 512
```

Through this interface, you can record information can not be written about the kernel disk, this is because the information is loaded before the file system generated.

4.1.6 Processes

Click on the "Status>Processes" option, you can see the following interface.



Processes

This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	init	0%	2%	Hang Up	Terminate	Kill
2	root	[kthreadd]	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirqd/0]	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker/u:0]	0%	0%	Hang Up	Terminate	Kill
6	root	[khelper]	0%	0%	Hang Up	Terminate	Kill
7	root	[kworker/u:1]	0%	0%	Hang Up	Terminate	Kill
61	root	[sync_supers]	0%	0%	Hang Up	Terminate	Kill
63	root	[bdi-default]	0%	0%	Hang Up	Terminate	Kill
65	root	[kblockd]	0%	0%	Hang Up	Terminate	Kill
94	root	[kswapd0]	0%	0%	Hang Up	Terminate	Kill
143	root	[fsnotify_mark]	0%	0%	Hang Up	Terminate	Kill
156	root	[ath79-spi]	0%	0%	Hang Up	Terminate	Kill
167	root	[mtdblock0]	0%	0%	Hang Up	Terminate	Kill
172	root	[mtdblock1]	0%	0%	Hang Up	Terminate	Kill
177	root	[mtdblock2]	0%	0%	Hang Up	Terminate	Kill
182	root	[mtdblock3]	0%	0%	Hang Up	Terminate	Kill
187	root	[mtdblock4]	0%	0%	Hang Up	Terminate	Kill
192	root	[mtdblock5]	0%	0%	Hang Up	Terminate	Kill
413	root	[jffs2_gcd_mtd3]	0%	0%	Hang Up	Terminate	Kill
431	root	init	0%	2%	Hang Up	Terminate	Kill
468	root	[cfg80211]	0%	0%	Hang Up	Terminate	Kill
559	root	/sbin/syslogd -C16	0%	2%	Hang Up	Terminate	Kill
561	root	/sbin/klogd	0%	2%	Hang Up	Terminate	Kill

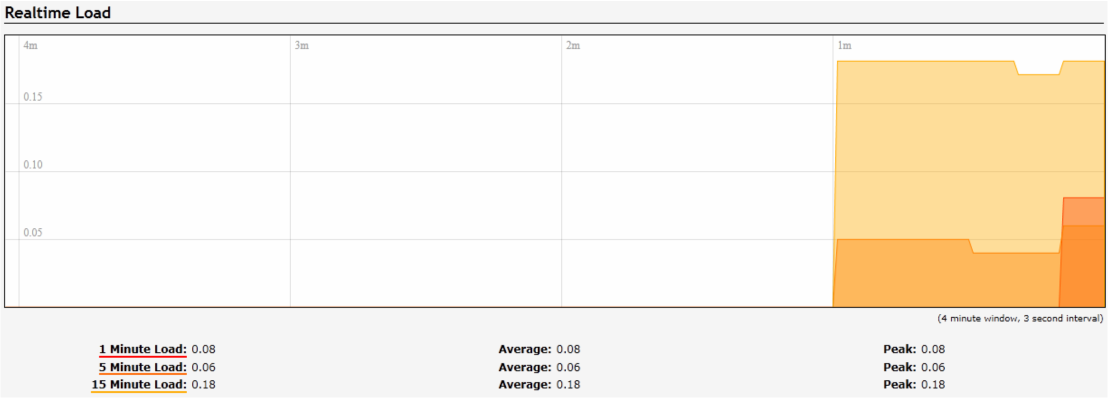
Through this interface, you can understand the process of running the system and their status information. And its suspended, closed, forced to close operations.

4.1.7 Realtime Graphs

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

4.1.7.1 Load

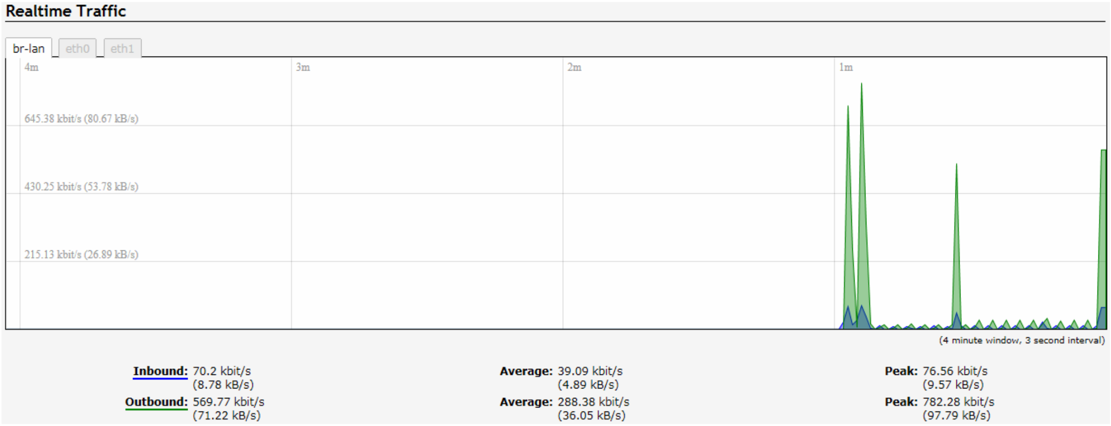
Click the "Status>Realtime Graphs>Load" option, you can see the following screen in Realtime Load information.



1 Minute Load: 0.08	**Average:** 0.08	**Peak:** 0.08
5 Minute Load: 0.06	**Average:** 0.06	**Peak:** 0.06
15 Minute Load: 0.18	**Average:** 0.18	**Peak:** 0.18

4.1.7.2 Traffic

Click the "Status>Realtime Graphs>Traffic" option, you can see the following screen in Realtime Traffic information.


br-lan
eth0
eth1
4m
3m
2m
1m
645.38 kbit/s (80.67 kB/s)
430.25 kbit/s (53.78 kB/s)
215.13 kbit/s (26.89 kB/s)

Realtime Traffic

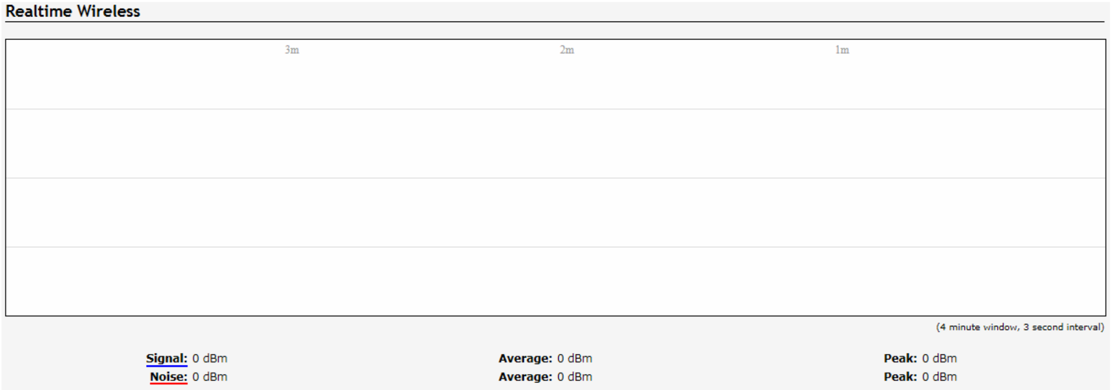
(4 minute window, 3 second interval)

Inbound: 70.2 kbit/s (8.78 kB/s) **Average:** 39.09 kbit/s (4.89 kB/s) **Peak:** 76.56 kbit/s (9.57 kB/s)

Outbound: 569.77 kbit/s (71.22 kB/s) **Average:** 288.38 kbit/s (36.05 kB/s) **Peak:** 782.28 kbit/s (97.79 kB/s)

4.1.7.3 Wireless

Click the "Status>Realtime Graphs>Wireless" option, you can see the following screen in Realtime Wireless information.



Realtime Wireless

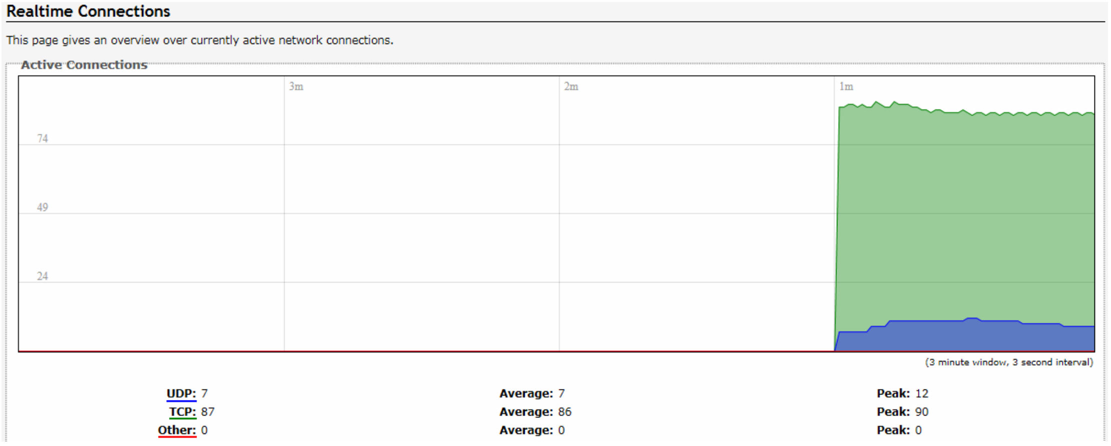
(4 minute window, 3 second interval)

Signal: 0 dBm **Average:** 0 dBm **Peak:** 0 dBm

Noise: 0 dBm **Average:** 0 dBm **Peak:** 0 dBm

4.1.7.4 Connections

Click the "Status>Realtime Graphs>Connections" option, you can see the following screen in Realtime Connections information.



Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(3 minute window, 3 second interval)

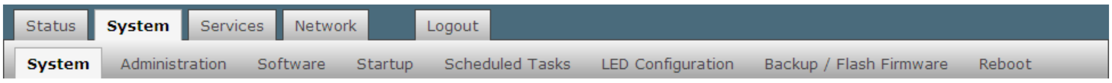
UDP: 7 **Average:** 7 **Peak:** 12

TCP: 87 **Average:** 86 **Peak:** 90

Other: 0 **Average:** 0 **Peak:** 0

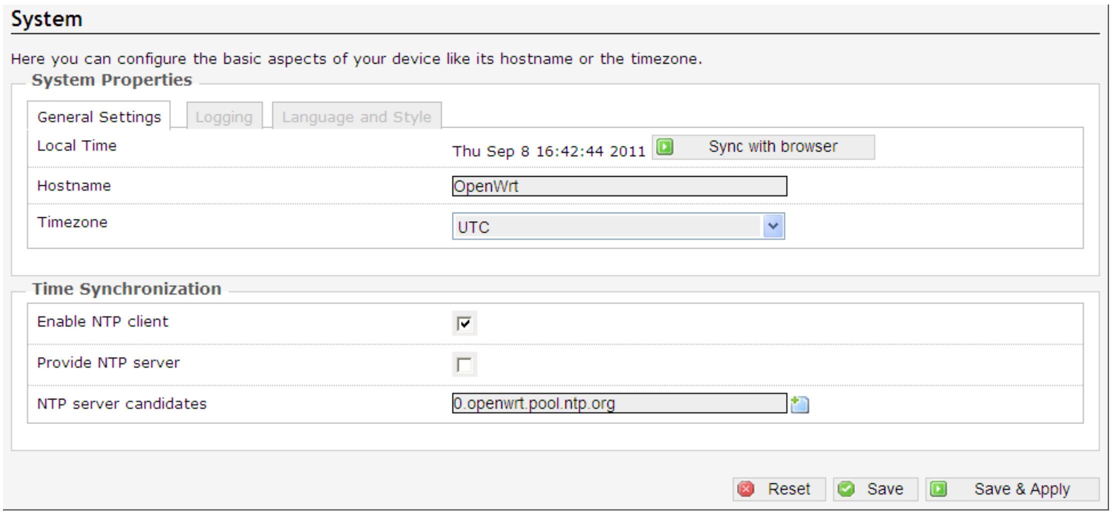
4.2 System

Click on "System", you can see the System, Administration, Software, Starup, Scheduled Tasks, LED Configuration, Backup/Flash Firmware, Reboot options.



4.2.1 System

Click "System>System" option, you can set the System Properties and Time Synchronization.



System

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

System Properties

Local Time	Thu Sep 8 16:42:44 2011
Hostname	OpenWrt
Timezone	UTC

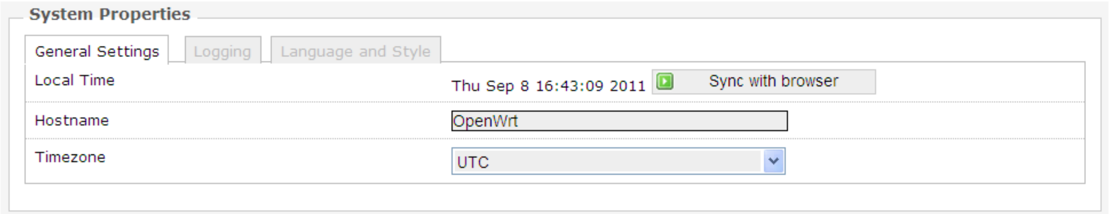
Time Synchronization

Enable NTP client	☑
Provide NTP server	□
NTP server candidates	0.openwrt.pool.ntp.org

System Properties

System Properties are divided into General Settings, Logging, Language and Style three options.

Click on the "General Settings" option, you can see the following interface.



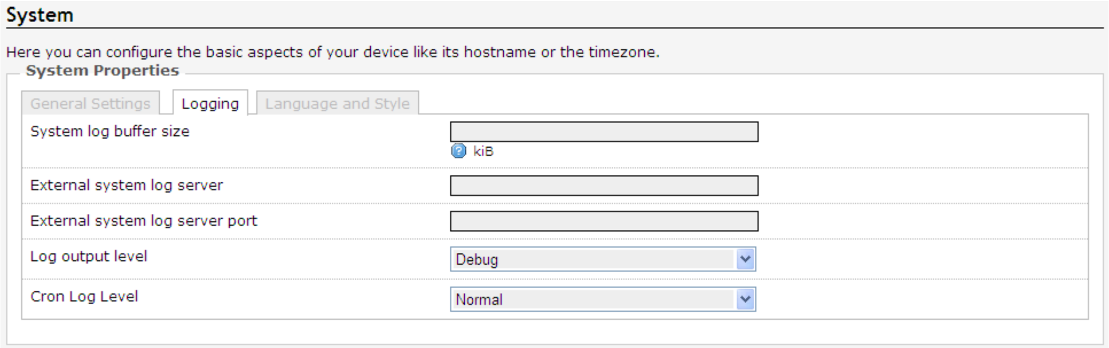
System Properties

Local Time	Thu Sep 8 16:43:09 2011
Hostname	OpenWrt
Timezone	UTC

Local Time: Click "Sync with browser", you can display the time zone that corresponds to your choice time.

Hostname: you use a AP name.

Timezone: you can select the desired time zone from the drop-down list.



System

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

System Properties

System log buffer size	kiB
External system log server	
External system log server port	
Log output level	Debug
Cron Log Level	Normal

System log buffer size: You can specify the size of the log buffer here.

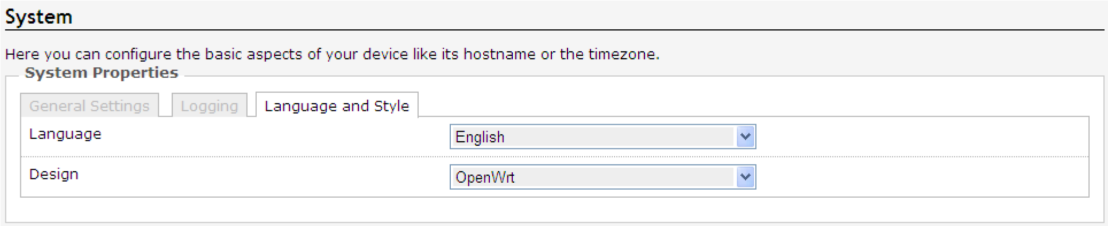
External system log server: remote host is configured to receive log information machine.

External system log server port: configured to receive a remote host machine’s port log information.

Log output level: Select the level of logging, Debug, Info, Notice, Warning, Error, Critical, Alert and Emergency eight grades.

Cron Log Level: Select the level Cron logs, Debug, Normal and Warning three levels.

Click on the "Language and Style" option, you can see the following interface.



System

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

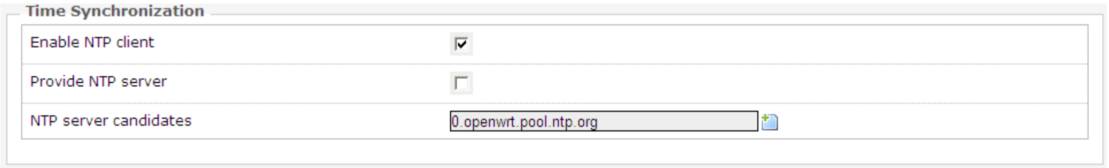
System Properties

Language	English
Design	OpenWrt

Language: Select the AP management interface in the language used, there are auto, English and Chinese three kinds to choose from.

Time Synchronization

Time Synchronization settings interface as shown below.



Time Synchronization

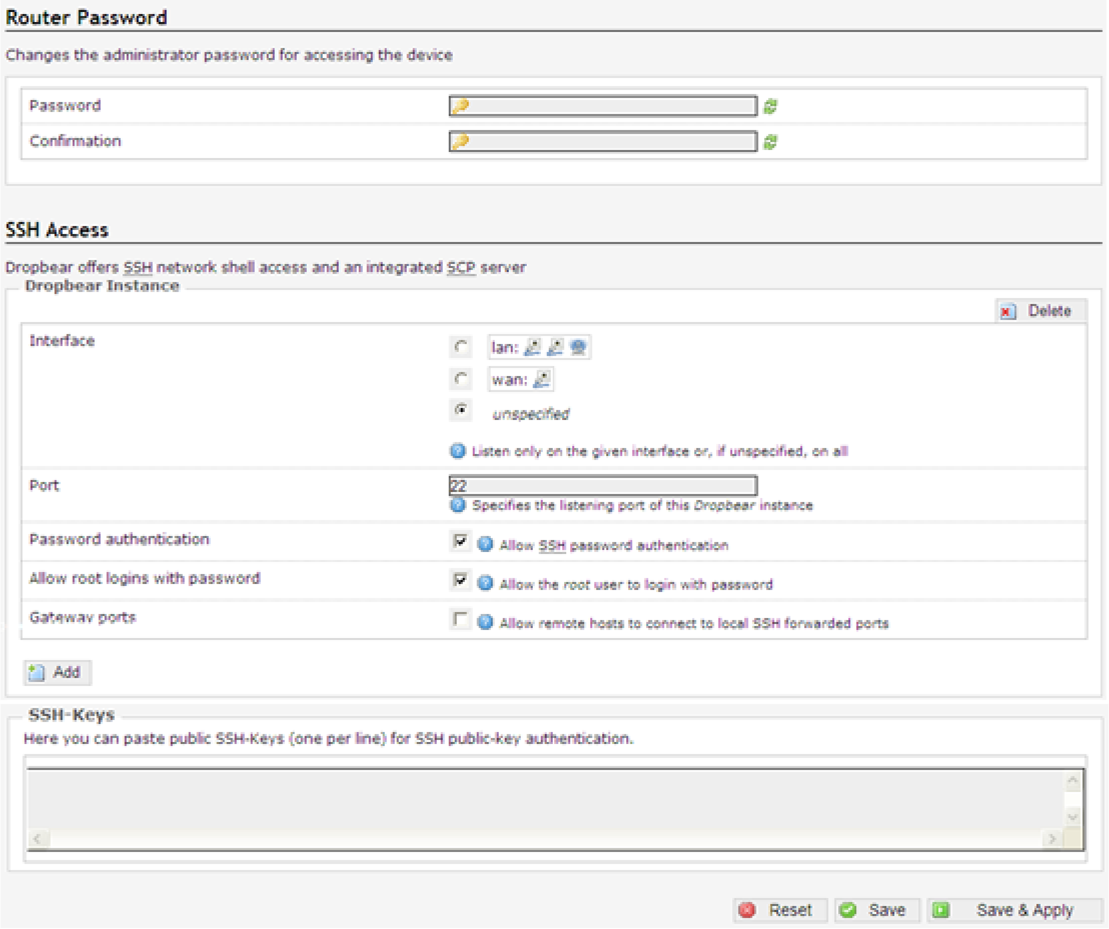
Enable NTP client	☑
Provide NTP server	□
NTP server candidates	0.openwrt.pool.ntp.org

Enable NTP client: If you check this, you can configure the server multiple time sources.

Provide NTP server: As long as your computer can be networked, can be a LAN or WAN computer time calibration within.

4.2.2 Administration

Click on the "System>Administration" option, you can see the following interface.



Router Password

Changes the administrator password for accessing the device

Password	
Confirmation	

SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

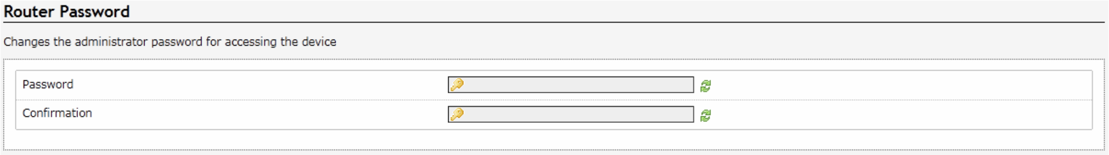
Interface	○ lan: ○ wan: ● *unspecified* Listen only on the given interface or, if unspecified, on all
Port	22 Specifies the listening port of this *Dropbear* instance
Password authentication	☑ Allow SSH password authentication
Allow root logins with password	☑ Allow the root user to login with password
Gateway ports	□ Allow remote hosts to connect to local SSH forwarded ports

SSH-Keys

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

Router Password

Router Password settings interface as shown below.



Router Password

Changes the administrator password for accessing the device

Password	
Confirmation	

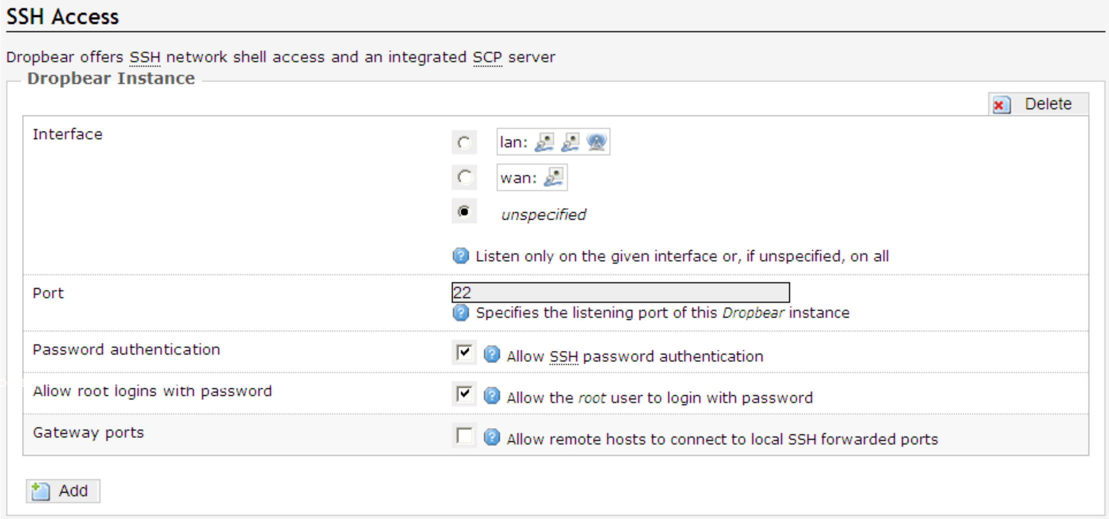
Password: You can modify the registry Router's password in this column, the default password is blank.

Confirmation: Enter your password again.

Click the "Save & Apply",Save your router's password.

SSH Access

SSH Access settings interface as shown below.



SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

Interface	○ lan: ○ wan: ● *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

SSH: Secure Shell SSH abbreviation for the establishment in the application layer and the transport layer on the basis of security protocols. SSH is more reliable, designed to provide security protocol for remote login session, and other network services. SSH protocol can effectively prevent the use of remote management process of information disclosure issue.

Dropbear: Provides integrated SCP server and SSH -based shell access.

Interface: listen specified interface, not specified monitor all of them.

Port: Specify Dropbear listening port is 22.

Password authentication: Check the Allow SSH password authentication.

Allow root logins with password: Check the root user is allowed to log in with a password.

Gateway ports: Allows remote hosts to connect to the local SSH port forwarding.

Public key authentication, in fact, use a pair of encrypted string, called a public key(public key), anyone can see its contents for encryption; another called key(private key). Only to have those who can see, for decryption. By public key encrypted ciphertext can be easily decrypted using a key, but according to public to guess the key is very difficult. SSH public key authentication is to use this feature. Server and client each have their own public and private keys.

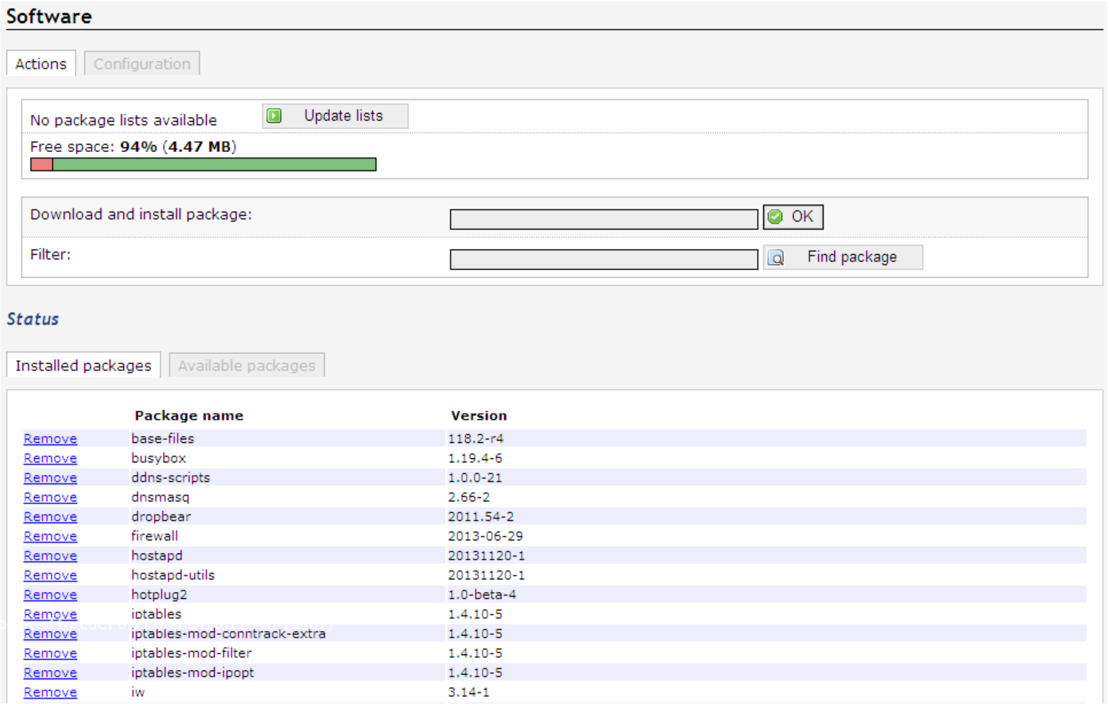
4.2.3 Software

The AP provides two methods to install the package: page installation(action) and telnet or ssh connection backstage installation(configuration).

For example, you want to install tftp server name for tftpd-hpa, then follow the steps below.

Page installation

Click the "System>Software>Actions", the interface as shown below.



No package lists available

Free space: **94%** (**4.47 MB**)

Download and install package:

Filter:

	Package name	Version
Remove	base-files	118.2-r4
Remove	busybox	1.19.4-6
Remove	ddns-scripts	1.0.0-21
Remove	dnsmasq	2.66-2
Remove	dropbear	2011.54-2
Remove	firewall	2013-06-29
Remove	hostapd	20131120-1
Remove	hostapd-utils	20131120-1
Remove	hotplug2	1.0-beta-4
Remove	iptables	1.4.10-5
Remove	iptables-mod-conntrack-extra	1.4.10-5
Remove	iptables-mod-filter	1.4.10-5
Remove	iptables-mod-ipopt	1.4.10-5
Remove	iw	3.14-1

If this AP does not tftpd-hpa server proceed as follows.

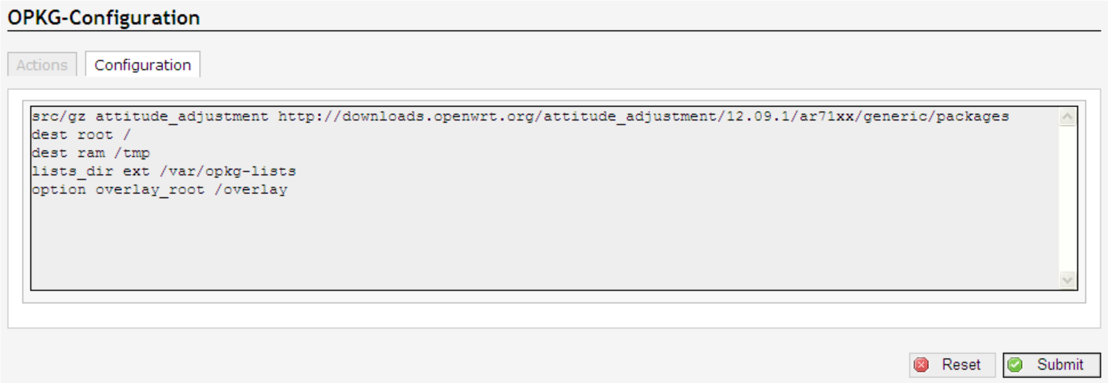
Enter "tftpd" in the "Download and install the package", click "OK" to.

If this AP has tftpd-hpa server proceed as follows.

In the "Filter" which enter "tftpd", click on "Find packages" in the "Status" box below to show the current OpenWrt support packages and find you need, click the "install" .

telnet or ssh connection backstage installation

Click the "System>Software>Configuration" screen as shown below.



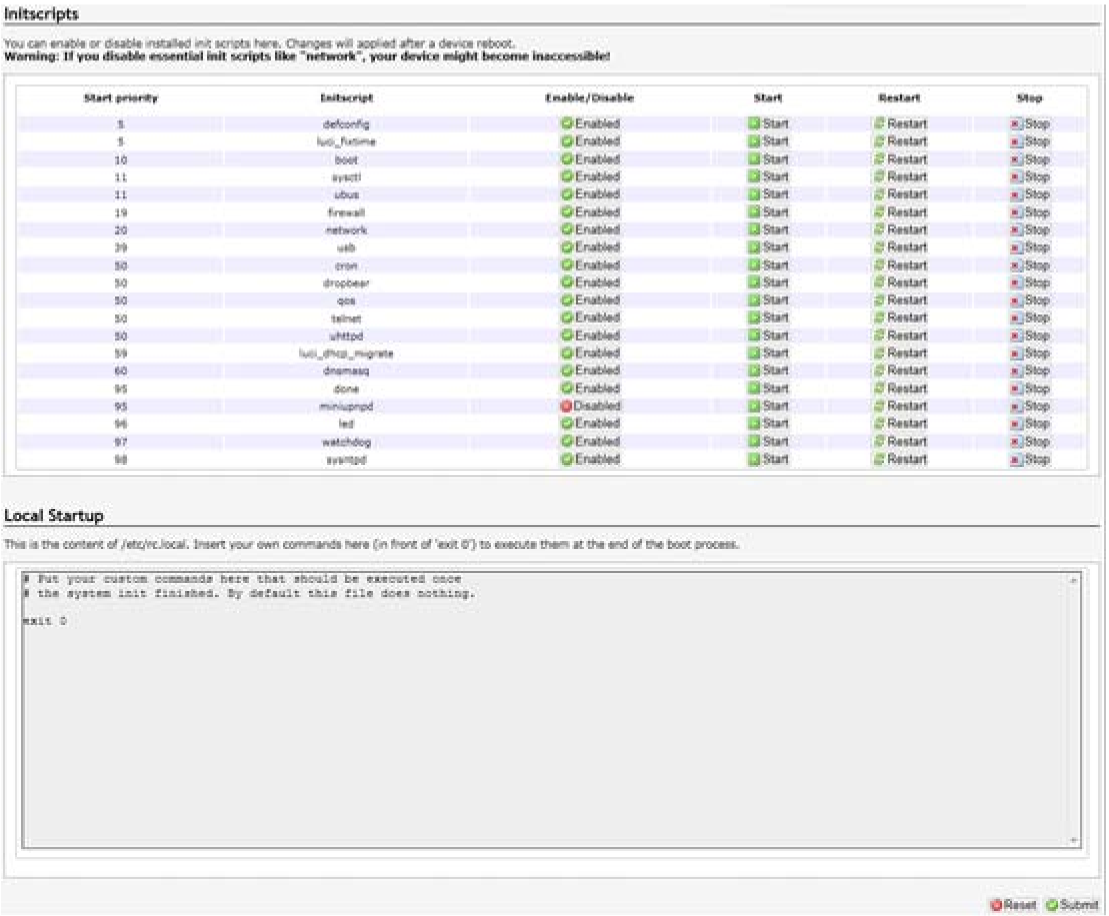
```
src/gz attitude_adjustment http://downloads.openwrt.org/attitude_adjustment/12.09.1/ar71xx/generic/packages
dest root /
dest ram /tmp
lists_dir ext /var/opkg-lists
option overlay_root /overlay
```

Input box in the image above: #opkg download tftpd-hpa /download packages

#opkg install tftpd-hpa / installation package

4.2.4 Startup

Click on the "System>Startup" option, you can see the following interface.



Initscripts

You can enable or disable installed init scripts here. Changes will applied after a device reboot.
Warning: If you disable essential init scripts like "network", your device might become inaccessible!

Start priority	Initscript	Enable/Disable	Start	Restart	Stop
5	defconfig	Enabled	Start	Restart	Stop
5	luci_fixtime	Enabled	Start	Restart	Stop
10	boot	Enabled	Start	Restart	Stop
11	sysctl	Enabled	Start	Restart	Stop
11	ubus	Enabled	Start	Restart	Stop
19	firewall	Enabled	Start	Restart	Stop
20	network	Enabled	Start	Restart	Stop
39	usb	Enabled	Start	Restart	Stop
50	cron	Enabled	Start	Restart	Stop
50	dropbear	Enabled	Start	Restart	Stop
50	qos	Enabled	Start	Restart	Stop
50	telnet	Enabled	Start	Restart	Stop
50	uhttpd	Enabled	Start	Restart	Stop
59	luci_dhcp_migrate	Enabled	Start	Restart	Stop
60	dnsmasq	Enabled	Start	Restart	Stop
95	done	Enabled	Start	Restart	Stop
95	miniupnpd	Disabled	Start	Restart	Stop
96	led	Enabled	Start	Restart	Stop
97	watchdog	Enabled	Start	Restart	Stop
98	sysntpd	Enabled	Start	Restart	Stop

Local Startup

This is the content of /etc/rc.local. Insert your own commands here (in front of 'exit 0') to execute them at the end of the boot process.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

exit 0
```

Start the project when the system is switched on in the foreground or the background programs running.

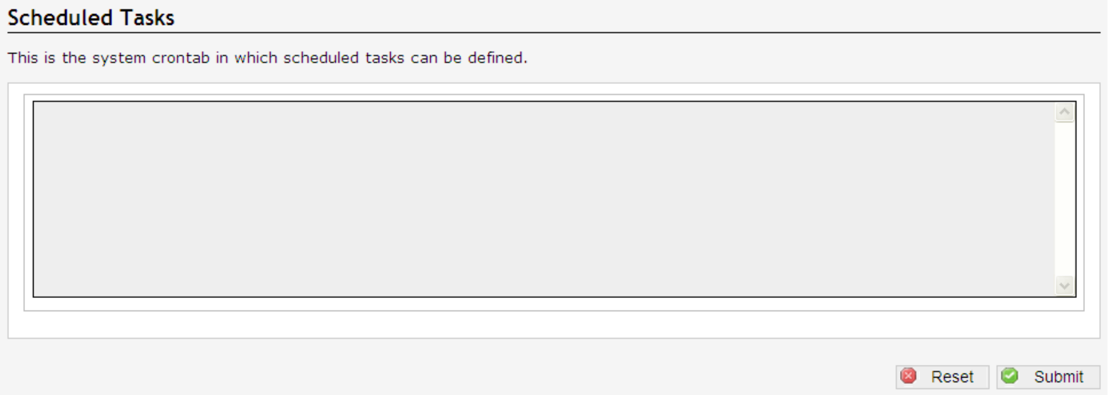
You can enable or disable installed init scripts here. Change will applied after a device reboot. Different starup scripts start with different priorities, starup scripts can be Enable/Disable, Start, Restart and Stop operations.

Startup script: startup script to enable or disable installed. Changes take effect after the device reboot. (**Note:** If you disable the necessary startup script, such as "network", may cause the device can not access and therefore do not arbitrarily change the startup script!)

Local startup script: You can block the figure of "exit 0" previously entered commands to start or stop a service. /etc/init.d/ in store all the startup script, we usually can start an application by/etc/init.d/ script name start up mode. For example, enter the command "/etc/init.d/smb start" to start the smb service. Although/etc/in it. d directory script can start and stop individual services, but at system boot, in it not find the startup script for each service directly in the /etc/init.d catalog, but in/ etc/ under rc.d/ directory lookup, this directory contains rc0.d, rc1.d, respectively, representing different levels of subdirectories init starts, each subdirectory contains the corresponding start -level startup script.

4.2.5 Scheduled Tasks

Click on the "System>Scheduled Tasks" option, you can see the following interface.



Scheduled Tasks

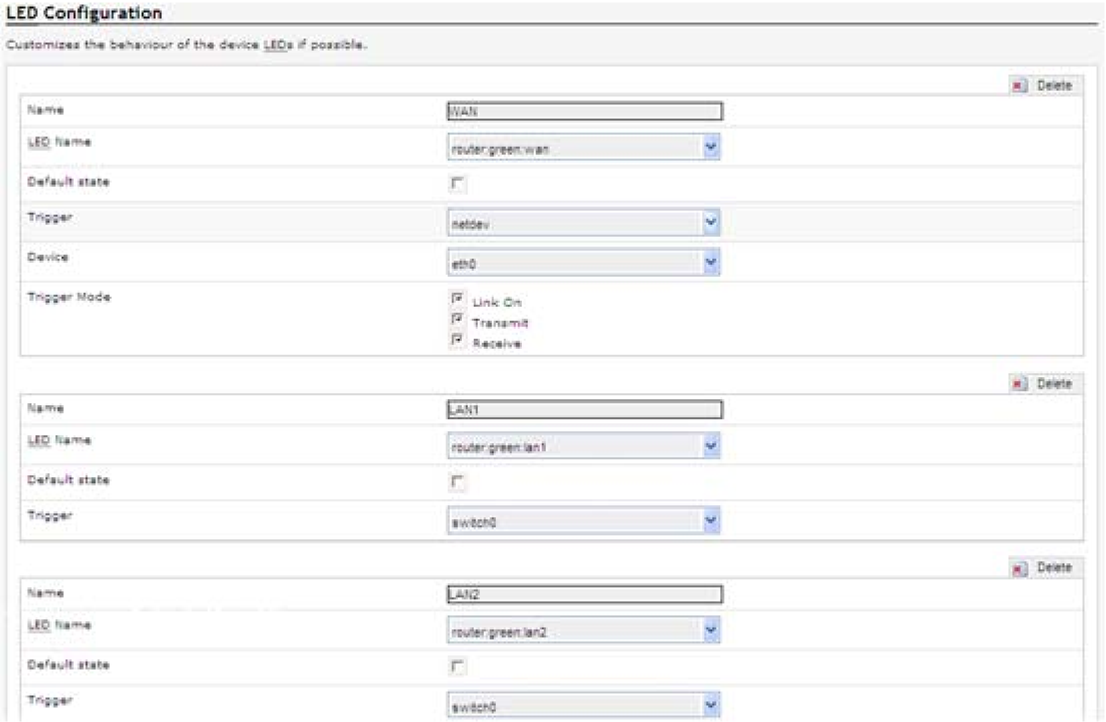
This is the system crontab in which scheduled tasks can be defined.

You can fill you want to accomplish in the box, especially repetitive tasks.

Example: Yon want to restart the AP every night at 21.30(OpenWrt), would enter in the box "30 21 * * * /usr/local/etc/rc.d/OpenWrt restart".

4.2.6 LED Configuration

Click on the "System>LED Configuration" option, you can see the following interface.



LED Configuration

Customizes the behaviour of the device LEDs if possible.

Name	WAN
LED Name	router:green:wan
Default state	□
Trigger	netdev
Device	eth0
Trigger Mode	☑ Link On ☑ Transmit ☑ Receive

Name	LAN1
LED Name	router:green:lan1
Default state	□
Trigger	switch0

Name	LAN2
LED Name	router:green:lan2
Default state	□
Trigger	switch0

Name: Name of the AP interface.

LED Name: Corresponds to the name of its display lights.

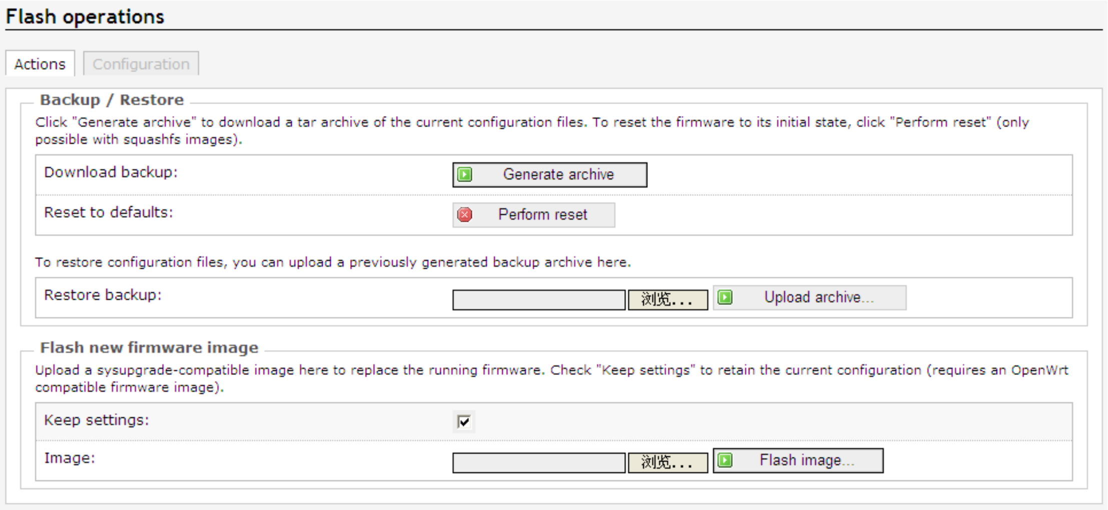
Default state: Trigger mode determines the corresponding LED lights flashing mode interface. Either way you can choose to trigger the drop-down list provide.

4.2.7 Backup/Flash Firmware

Click "System>Backup/Flash Firmware" option, you can see the Action and Configuration two options.

Action

Click on the "Action" option, you can see the following interface.



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

Reset to defaults:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:

Flash new firmware image

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

Keep settings: ☑

Image:

Download backup: This feature can be set up the AP as files stored in the computer to prepare for the next use; AP software upgrade or a new configuration file before loading the original backup AP configuration, software upgrades can effectively prevent or load the new configuration file is lost during the original configuration issues. Click the "Generate Backup" to complete this operation.

Reset to defaults: Click the "Perform reset" to restore to factory settings, restore factory settings, the AP will automatically restart the AP to restore all settings to the factory default state(Including: the default user name: root; default password: empty; default IP address: 192.168.10.154; default netmask: 255.255.255.0)

Note: Please restore the factory settings before configuration information backup system, if necessary through the load configuration information to restore the backup AP configuration.

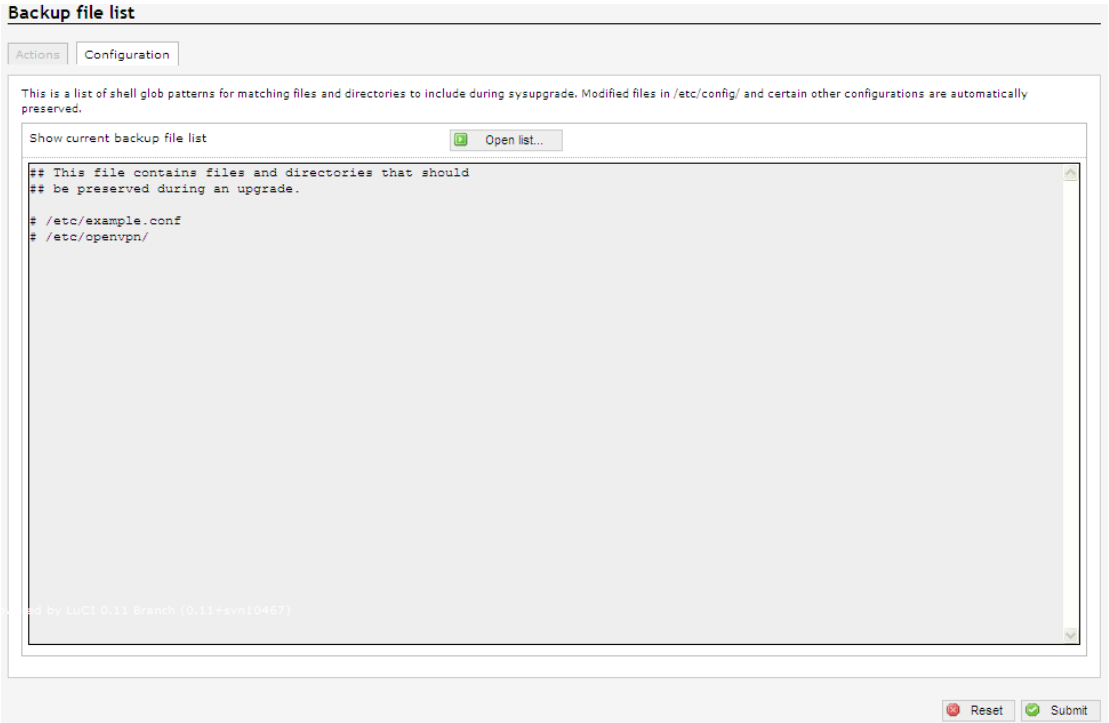
Restore backup: Click "Browse" to find the file has been backed up, select a file has been backed up, and then click the "upload archive..." to complete the recover configuration.

Keep settings: Check the box, you can write the new firmware in the brush, still retain the original system configuration information; If not checked, the original system configuration information in the brush to write the new firmware, it will be erased.

Image: Click "浏览" to find the new firmware file, select the new firmware file, then click on the "Flash image" to flash the new firmware operation.

Configuration

Click on the "Configuration" option, you can see the following interface.



Backup file list

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

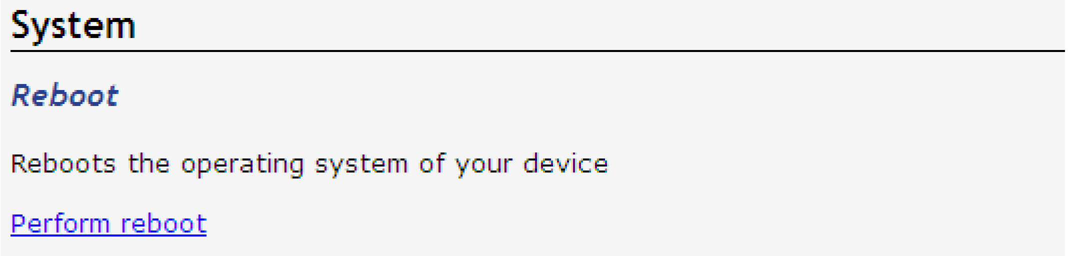
Show current backup file list

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

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

Click "Open list", you can see a list of files to be backed up, The configuration file contains the changes necessary foundation files and user-defined files to be backed up.

4.2.8 Reboot

Click on the "System>Reboot" option, you can see the following interface.



System

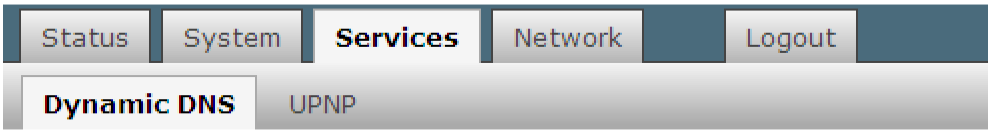
Reboot

Reboots the operating system of your device

Click "Perform reboot" to complete manual restart the AP.

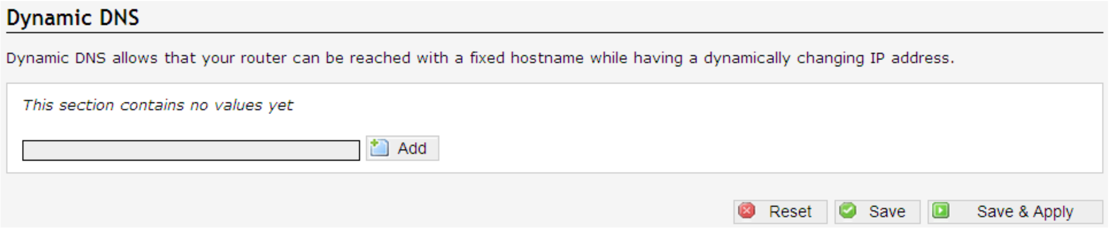
4.3 Services

Click on "Services", you can see the Dynamic DNS, UPNP options.



4.3.1 Dynamic DNS

Click on the "Services>Dynamic DNS" option, you can see the following interface.



Dynamic DNS

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

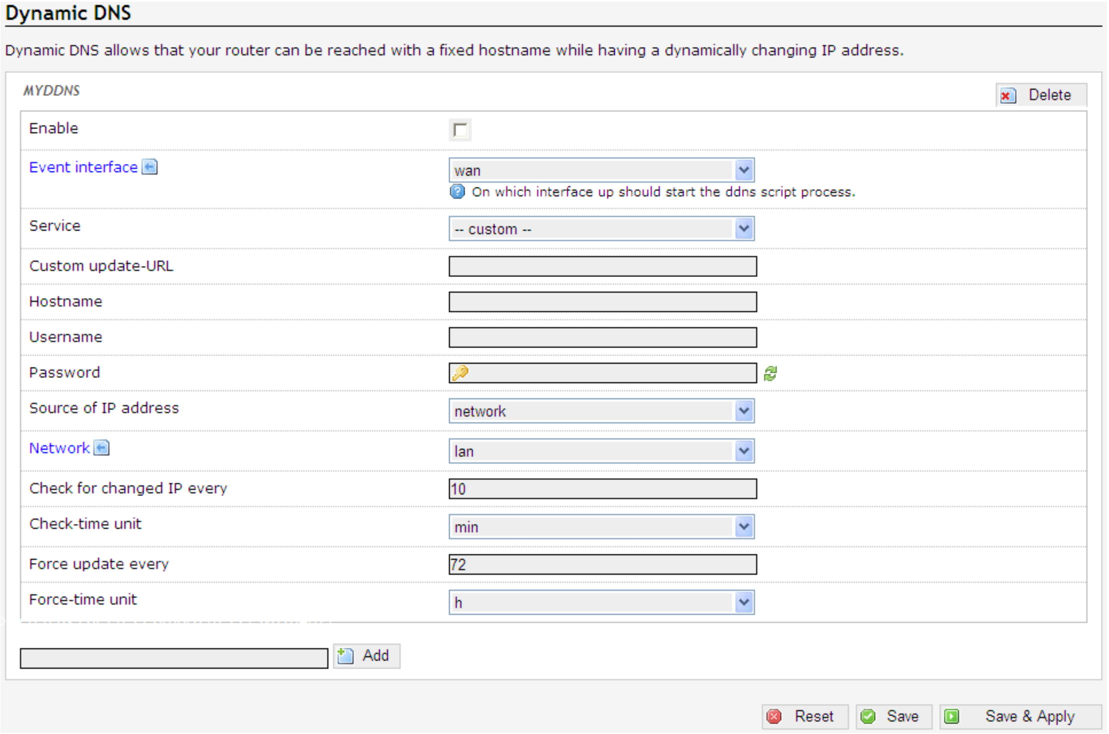
This section contains no values yet

Dynamic DDNS: Its main function is to achieve a fixed domain name to resolve dynamic IP address. If the address of the AP's WAN port IP address is dynamically acquired through this feature allows access to other hosts on the Internet AP or virtual server with a fixed domain approach.

Dynamic DNS feature for user dynamic IP address each time the Internet to get a new IP address, AP built-in Dynamic DNS software will send the IP address to the DDNS server provided by DDNS service providers, and update resolves database. When other users on the Internet need to access this domain name, dynamic DNS server will return the correct IP address. This feature is not used for the majority of users of fixed IP address can also be economical and efficient to build its own network.

For example, on dyndns.org apply a dynamic domain mypersonaldomain.dyndns.org, user name usename, password 1234567890.

Click the "Add" button, make the following configuration, the configuration is completed, click "Save&Apply" button.



Dynamic DNS

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

MYDDNS

Enable	□
Event interface	wan On which interface up should start the ddns script process.
Service	-- custom --
Custom update-URL	
Hostname	
Username	
Password	
Source of IP address	network
Network	lan
Check for changed IP every	10
Check-time unit	min
Force update every	72
Force-time unit	h

Service: Choose to provide dynamic domain name service provider, in this case, is dyndns.org.

Hostname: The host name of the application.

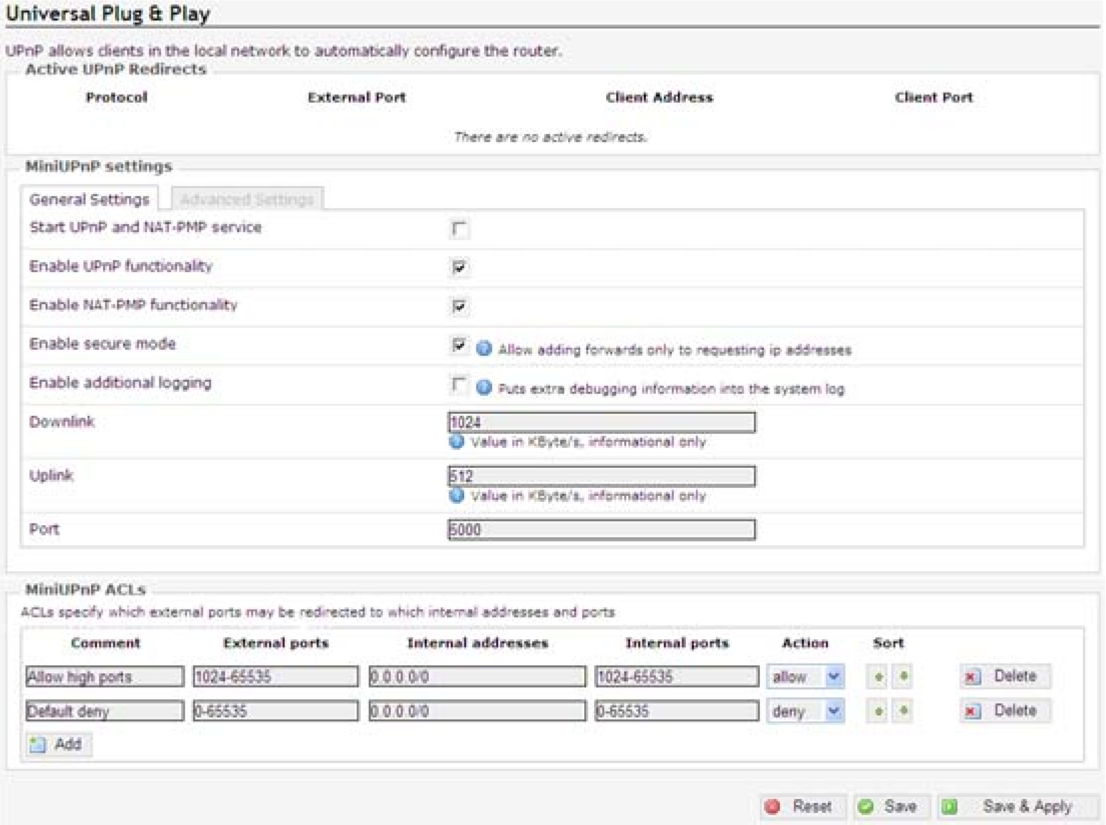
Username: User name to use when applying for dynamic domain name.

Password: Password used when applying dynamic domain name.

Source of IP address: The IP address of your Internet possible source URL, or network interface.

4.3.2 UPNP

Click on the "Services>UPNP" option, you can see the following interface.



Universal Plug & Play

UPnP allows clients in the local network to automatically configure the router.

Active UPnP Redirects

Protocol	External Port	Client Address	Client Port

There are no active redirects.

MiniUPnP settings

General Settings | Advanced Settings

Start UPnP and NAT-PMP service	□
Enable UPnP functionality	☑
Enable NAT-PMP functionality	☑
Enable secure mode	☑ Allow adding forwards only to requesting ip addresses
Enable additional logging	□ Puts extra debugging information into the system log
Downlink	1024 Value in KByte/s, informational only
Uplink	512 Value in KByte/s, informational only
Port	5000

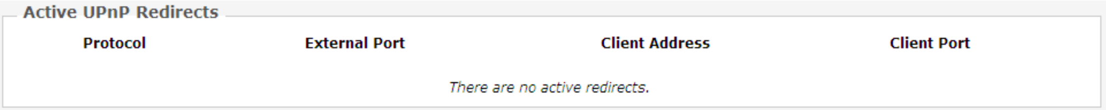
MiniUPnP ACLs

ACLs specify which external ports may be redirected to which internal addresses and ports

Comment	External ports	Internal addresses	Internal ports	Action	Sort	
Allow high ports	1024-65535	0.0.0.0/0	1024-65535	allow		Delete
Default deny	0-65535	0.0.0.0/0	0-65535	deny		Delete

Universal Plug and Play(UPnP) is an architecture for PC and smart devices(or equipment) common peer network connections, especially in the home. UPnP to Internet standards and technologies(such as TCP /IP, HTTP and XML)-based, so that such devices can automatically connect to each other and work together, so that the network (especially the home network) for more people to become possible. Relying on UPnP(Universal Plug and Play, Universal Plug and Play) protocol functions, LAN hosts can request automatic port switching AP, so that the external host can access resources on the internal host when needed, such as Windows XP and Windows ME systems the installation of MSN Messenger or Thunder, BT, PPLive and other applications that support the UPnP protocol.

Active UPnP Redirect

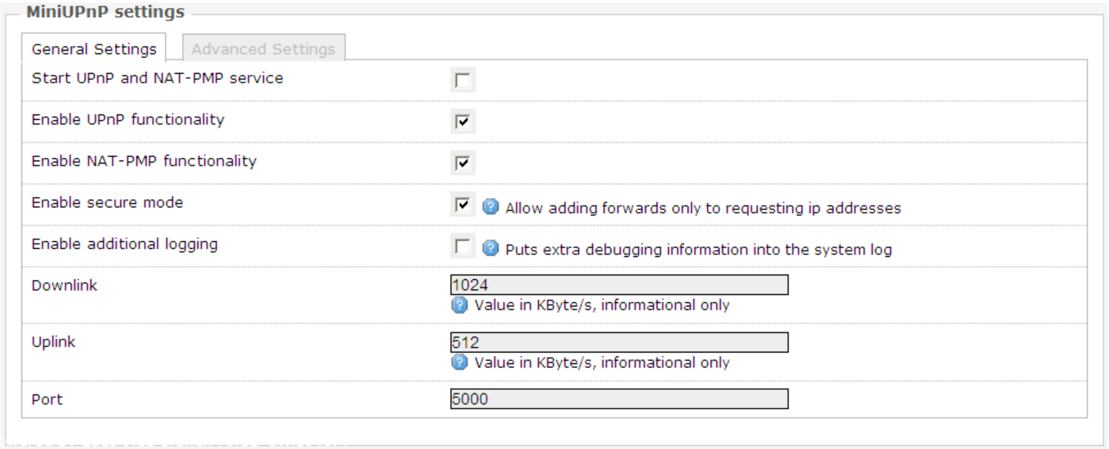


Active UPnP Redirects

Protocol	External Port	Client Address	Client Port

There are no active redirects.

MiniUPnP settings



MiniUPnP settings

General Settings | Advanced Settings

Start UPnP and NAT-PMP service	□
Enable UPnP functionality	☑
Enable NAT-PMP functionality	☑
Enable secure mode	☑ Allow adding forwards only to requesting ip addresses
Enable additional logging	□ Puts extra debugging information into the system log
Downlink	1024 Value in KByte/s, informational only
Uplink	512 Value in KByte/s, informational only
Port	5000

Start UPnP and NAT-PMP service: Check this box is switched on when this feature is enabled.

Enable UPnP functionality: Check this box is switched on when this feature is enabled.

Enable NAT-PMP functionality: NAT-PMP is to allow private network inside the device and routing communication to external devices and it can contact, based on UDP protocol.

Enable secure mode: Allows you to add only forwarded to the requesting IP address, when enabled, UPnP clients can be forwarded only to its IP.

Enable additional logging: enabled the extraction of additional debugging information to the system log.

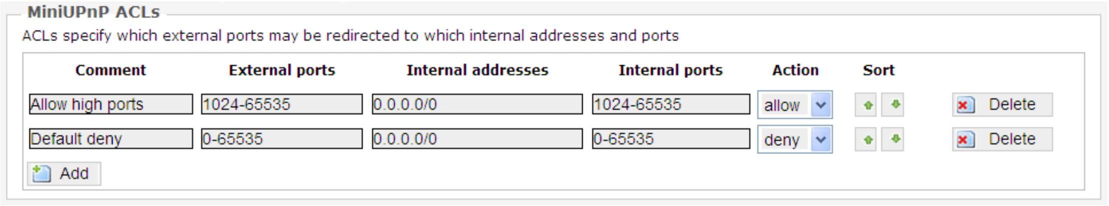
Downstream and upstream rates according to their actual broadband modifications.

Port: Input port services provided by the server within the network used.

MiniUPnP of ACL

Access Control List ACL(Access Control List) is a list of APs and switches command interface to control the port out of the packet. ACL is applicable to all routing protocols. ACL can limit network traffic and improve network performance. For example, ACL packet according to the agreement specifies the packet priority. ACL provides traffic control measures. For example, ACL can limit or simplify routing update information length, thus limiting through a AP on a network segment traffic. ACL is to provide access to basic means of network security. ACL allow Host A to access the Human Resources Network, and refused access to the host B. ACL can decide what type of traffic is forwarded or blocked at the AP port. For example, users can allow E-mail traffic is routed, reject all Telnet traffic. a department requires only use WWW this feature, you can achieve by ACL; another example, a department in order to privacy, do not allow it to access the Internet, are not allowed outside the network to access it, you can achieve through the ACL.

Click the "Add" button.you can see the following interface.



MiniUPnP ACLs

ACLs specify which external ports may be redirected to which internal addresses and ports

Comment	External ports	Internal addresses	Internal ports	Action	Sort	
Allow high ports	1024-65535	0.0.0.0/0	1024-65535	allow		Delete
Default deny	0-65535	0.0.0.0/0	0-65535	deny		Delete

Add

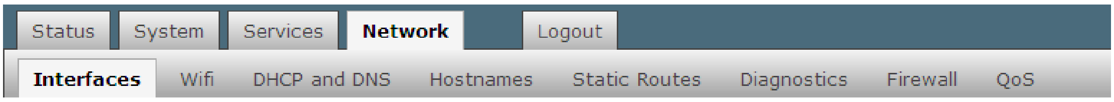
Comment: Memo entries can name.

External ports: Display practical AP for port switching time.

Internal addresses: Shows the need for a LAN host IP address port translation.
Internal Ports: Displays the port needs to be converted LAN host port number.
Action: Allow(allow) or reject(deny) access the internal or external network.

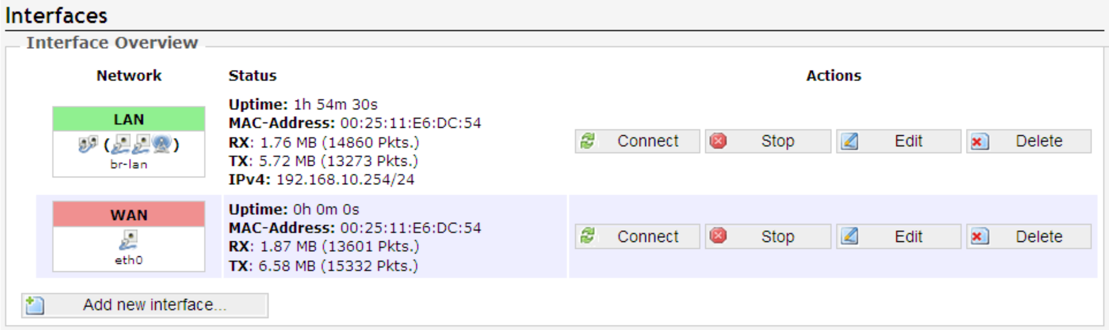
4.4 Network

Click on “Network”, you can see the Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall and QoS options.



4.4.1 Interfaces

Click the "Network>Interfaces" option, you can see the following screen.



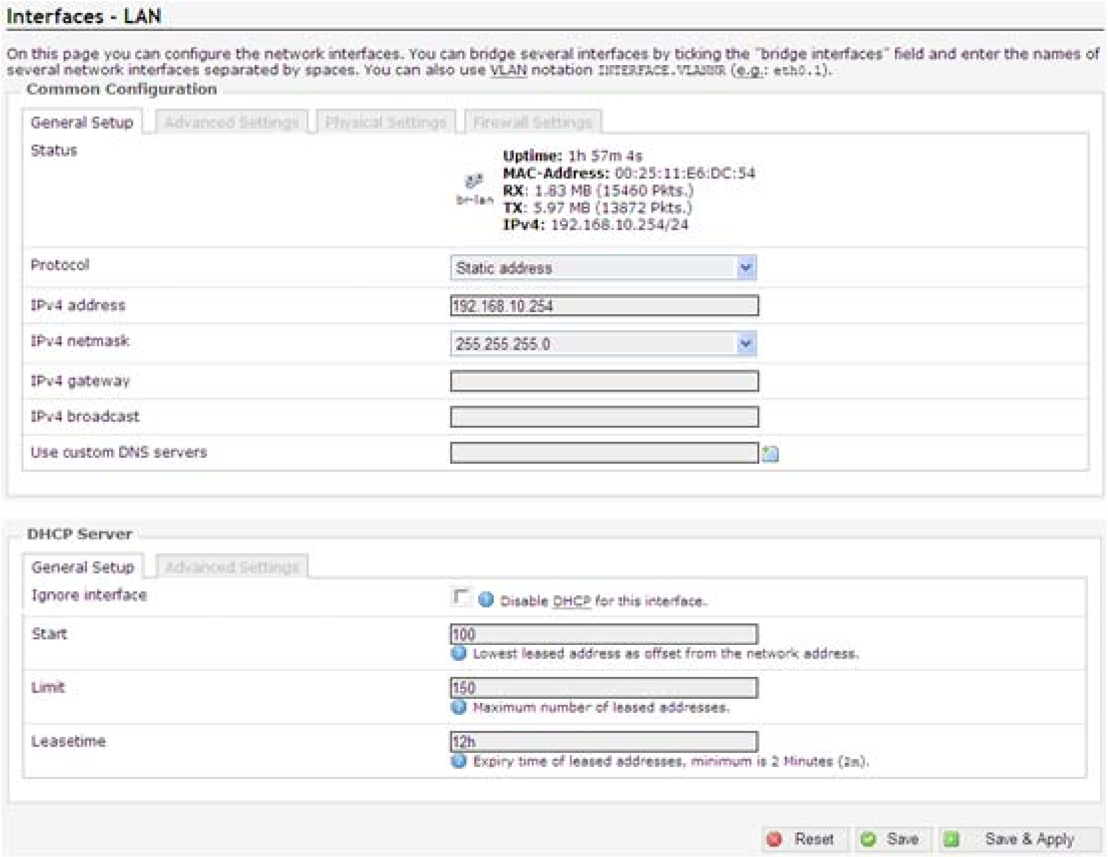
Uptime: 1h 54m 30s
MAC-Address: 00:25:11:E6:DC:54
RX: 1.76 MB (14860 Pkts.)
TX: 5.72 MB (13273 Pkts.)
IPv4: 192.168.10.254/24

Uptime: 0h 0m 0s
MAC-Address: 00:25:11:E6:DC:54
RX: 1.87 MB (13601 Pkts.)
TX: 6.58 MB (15332 Pkts.)

On this page, you can select and set WAN or LAN.

4.4.1.1 LAN

Click the "Network>Interfaces>LAN" option, On this page you can configure the network interfaces(lan).



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: Uptime: 1h 57m 4s
MAC-Address: 00:25:11:E6:DC:54
RX: 1.83 MB (15460 Pkts.)
TX: 5.97 MB (13872 Pkts.)
IPv4: 192.168.10.254/24

Protocol: Static address

IPv4 address: 192.168.10.254

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

DHCP Server

Ignore interface: ☐ Disable DHCP for this interface.

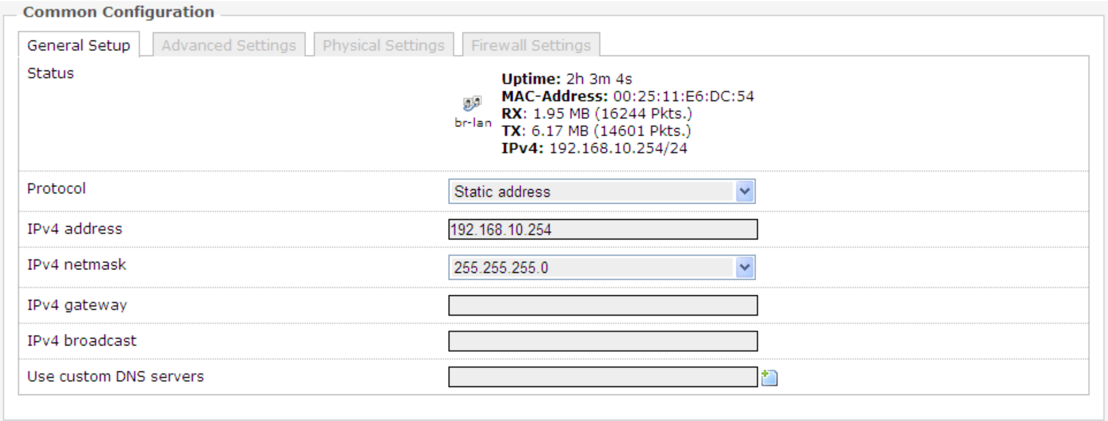
Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 Minutes (2m).

Common Configuration

Common Configuration screen as shown below.



Common Configuration

Status: Uptime: 2h 3m 4s
MAC-Address: 00:25:11:E6:DC:54
RX: 1.95 MB (16244 Pkts.)
TX: 6.17 MB (14601 Pkts.)
IPv4: 192.168.10.254/24

Protocol: Static address

IPv4 address: 192.168.10.254

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

On this page you can set IP address and netmask. Yon can manage the AP via this IP address. If you share access for ordinary family, you do not need to change the IP address of the LAN port, keep the default value.

Protocol: Select the protocol type.

IPv4 address: Enter the AP's IP address on the LAN. IP address of all computer in LAN must be in the same network segment and the default gateway for this IP address. The factory default IP address is 192.168.10.254, for Class C IP address, you can change it according to the network needs.

IPv4 netmask: Select the AP on the LAN net-mask. Class C IP address corresponding to the net-mask is 255.255.255.0. To ensure that the network connection is normal, do not change the net-mask. Yon can choose different types of LAN net-mask according to the actual IP address types.

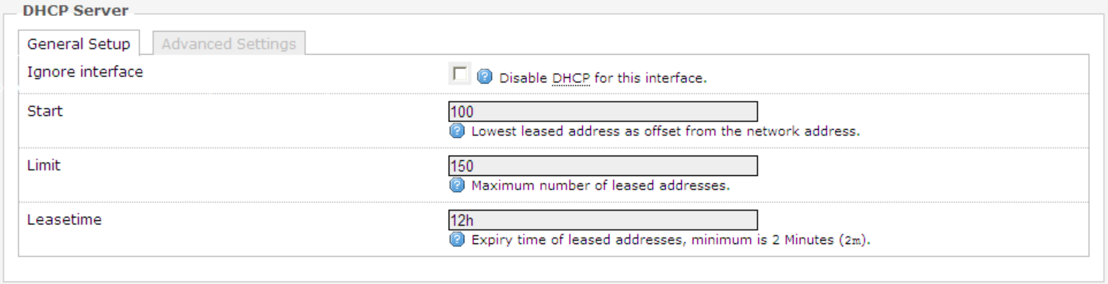
IPv4 gateway: Enter this AP on the LAN gateway. The default is 192.168.1.1.

Use custom DNS servers: DNS address provided by your ISP, if not provided, the default is 192.168.1.1.

Note: If you change the local IP address, you must login with a new IP address to the AP's Web management interface, and the default gateway for all computer in the LAN must be set to the IP to the normal Internet. Their net-mask must be set the same net-mask here. Advanced settings and physical settings are the default values, do not do the settings.

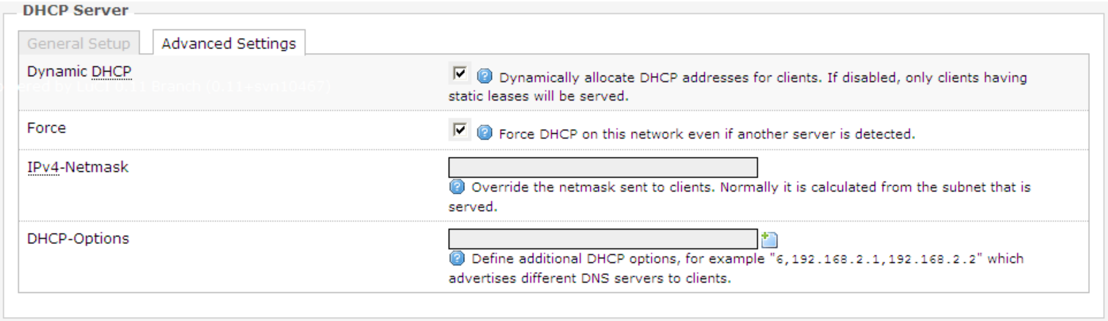
DHCP Server

DHCP Server setting interface as shown below.



DHCP Server

Ignore interface	☐ Disable DHCP for this interface.
Start	100 Lowest leased address as offset from the network address.
Limit	150 Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 Minutes (2m).



DHCP Server

Dynamic DHCP	☑ Dynamically allocate DHCP addresses for clients. If disabled, only clients having static leases will be served.
Force	☑ Force DHCP on this network even if another server is detected.
IPv4-Netmask	Override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DHCP-Options	Define additional DHCP options, for example "6,192.168.2.1,192.168.2.2" which advertises different DNS servers to clients.

DHCP: Dynamic Host Configuration Protocol. OpenWrt has a built-in DHCP server, the computer can automatically assign IP address on the LAN.

Ignore interface: Check this box, you can disable this DHCP function interface.

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

Limit: Maximum number of leased addresses. The AP default to 150.

Leasetime: Setting DHCP server IP address for client retention lease expiration time. In that period, the server will not assign IP address to other hosts. The AP default to 12h.

Dynamic DHCP: Dynamic allocation of DHCP addresses. If disabled, it can only provide network services for static lease table client.

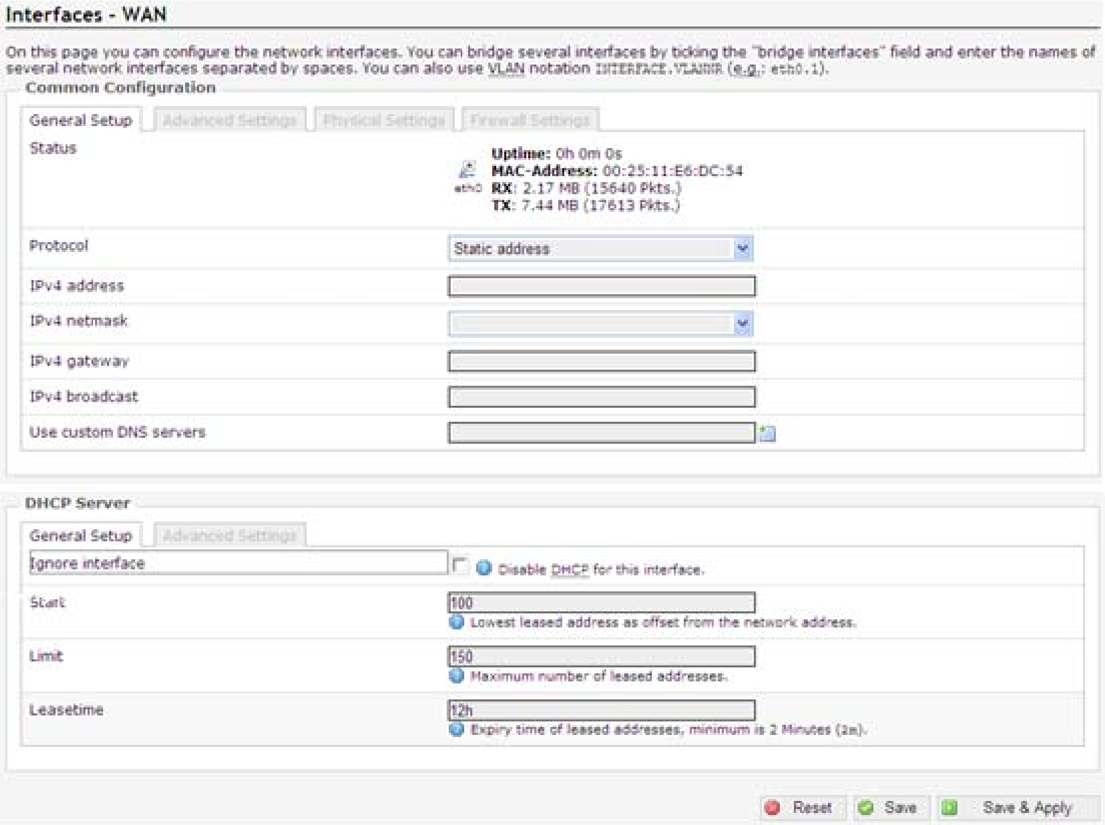
Force: Force DHCP on this network even if another server is detected.

IPV4-Netmask: The default net-mask DHCP server assigned to the client.

DHCP-Options: Set DHCP additional options, such as setting "6, 192.168.2.1, 192.168.2.2" means notice different DNS server to the client.

4.4.1.2 WAN

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



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: **Uptime:** 0h 0m 0s
MAC-Address: 00:25:11:E6:DC:54
RX: 2.17 MB (15640 Pkts.)
TX: 7.44 MB (17613 Pkts.)

Protocol: Static address

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

DHCP Server

Ignore interface □ Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

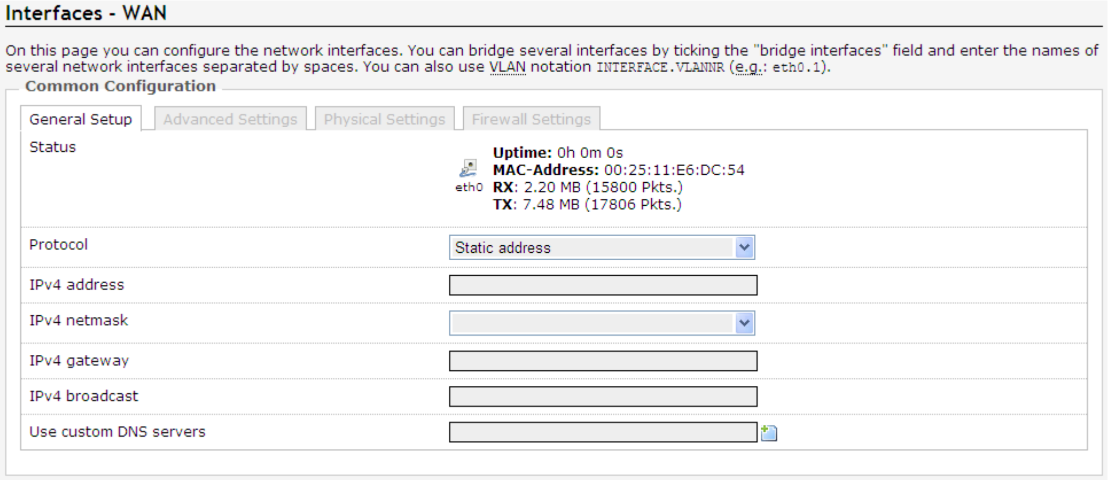
Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 Minutes (2m).

Expand Agreement are: Static address, DHCP client, PPPOE.

Static address

If you select the "static address" protocol, please complete the following information to suppliers(ISP)requirements. Click "Save&Apply" button, the next step is set.



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: **Uptime:** 0h 0m 0s
MAC-Address: 00:25:11:E6:DC:54
RX: 2.20 MB (15800 Pkts.)
TX: 7.48 MB (17806 Pkts.)

Protocol: Static address

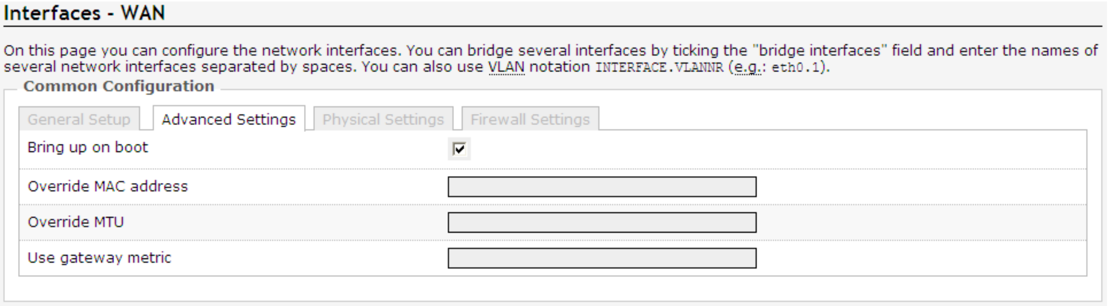
IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bring up on boot ☑

Override MAC address

Override MTU

Use gateway metric

Ipv4 address: The AP's IP address on the WAN. Please enter the public IP address provided by your ISP.

Ipv4 netmask: The net-mask for the WAN AP. Please enter the Net-mask provided by your ISP.

Ipv4 gateway: Please fill in the gateway provided by your ISP.

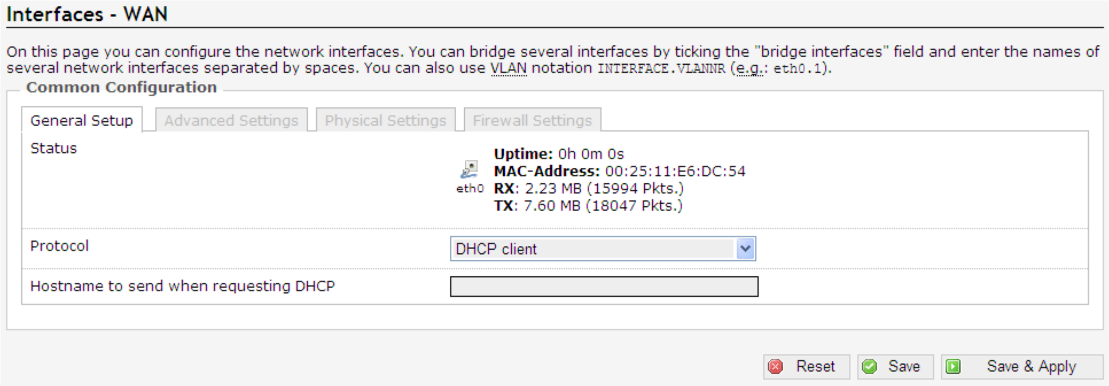
Use custom DNS server: Please fill provided by your ISP's DNS address.

Override MAC address: Please fill in this AP for WAN MAC address, the MAC address of the default AP WAN's physical interface MAC address. Some ISP may require MAC address binding, then the ISP will provide a valid MAC address to the user, based on the value you as long as it provides input to the "MAC address" column. Change the MAC address is not recommended unless the ISP has special requirements.

Override MTU: MTU called the data transmission unit, the default value is 1500. Please ask if you need to change to the ISP. Such as non-special needs, do not change.

DHCP client

If you select "DHCP client" protocol. Simply enter the MAC address of the computer as your modem MAC address of your AP. Click "Save&Apply" button,the next step is set.



Interfaces - WAN

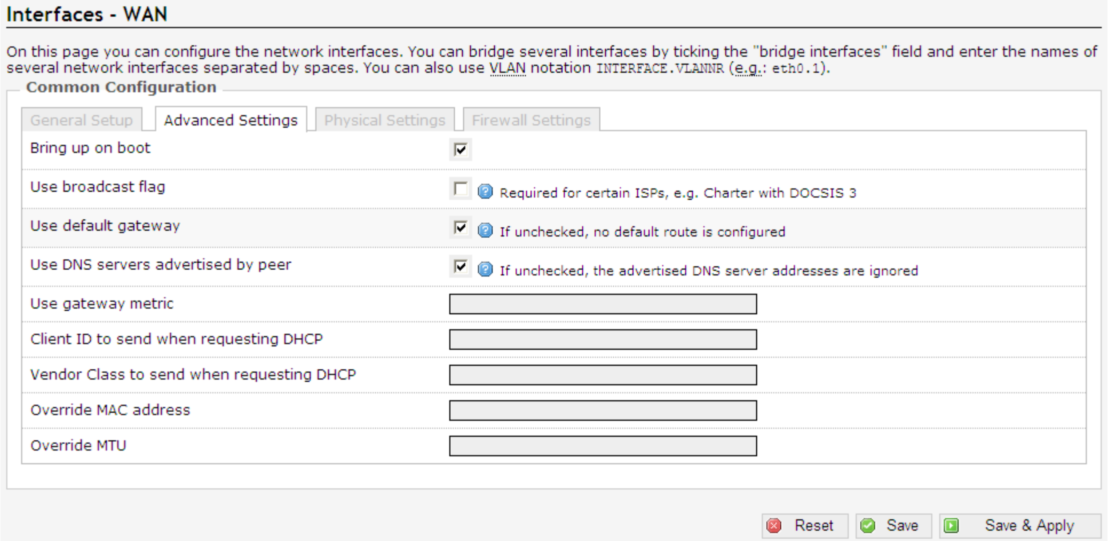
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: eth0 **Uptime:** 0h 0m 0s **MAC-Address:** 00:25:11:E6:DC:54 **RX:** 2.23 MB (15994 Pkts.) **TX:** 7.60 MB (18047 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP:



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bring up on boot ☑

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

Use default gateway ☑ If unchecked, no default route is configured

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

Use gateway metric:

Client ID to send when requesting DHCP:

Vendor Class to send when requesting DHCP:

Override MAC address:

Override MTU:

Host name when requesting DHCP sent: Enter the host name of this feature.

Bring up on boot: Check the power automatically when you select this means of access.

Use broadcast flag: You can fill this need according to ISP.

Use default gateway: Check in at the gateway to fill empty default route is not configure.

Use DNS servers advertised by peer: Check the DNS server address in the fill blank are ignored at the advertised DNS server address.

Use gateway metric: The destination network midway take several segments, that is, how many APs through.

Client ID to send when requesting DHCP: Enter the DHCP mode when you apply online, ISP provide your identity label number.

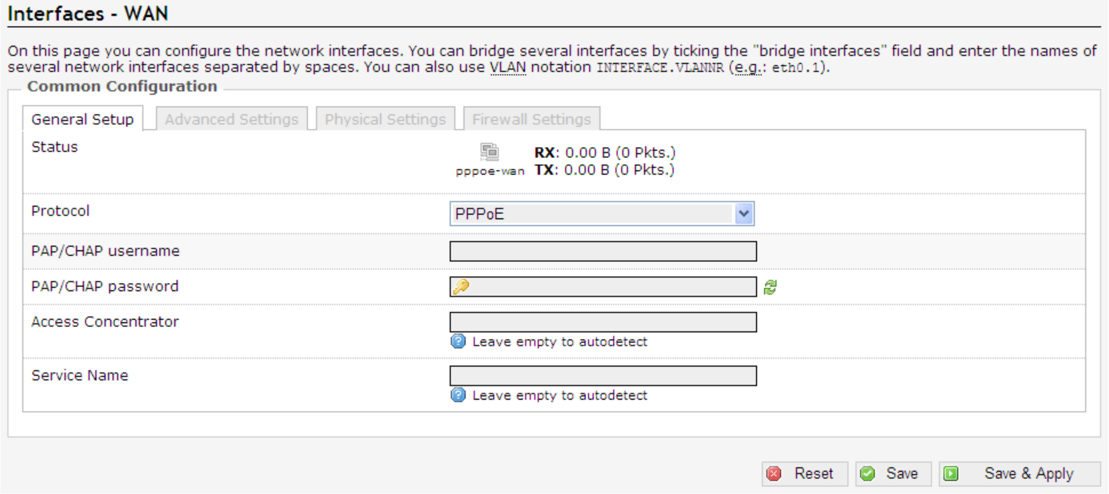
Vendor Class to send when requesting DHCP:DHCP mode input to your Internet provider category.

Override MAC address: Please fill in this AP for WAN MAC address, the MAC address of the default AP WAN's physical interface MAC address. Some ISP may require MAC address binding, then the ISP will provide a valid MAC address to the user, based on the value you as long as it provides input to the "MAC address" column. Change the MAC address is not recommended unless the ISP has special requirements.

Override MTU: MTU called the data transmission unit, the default value is 1500. Please ask if you need to change to the ISP. Such as non-special needs, do not change.

PPPoE

If you select "PPPoE" protocol. Click "Save&Apply" button, the next step is set.

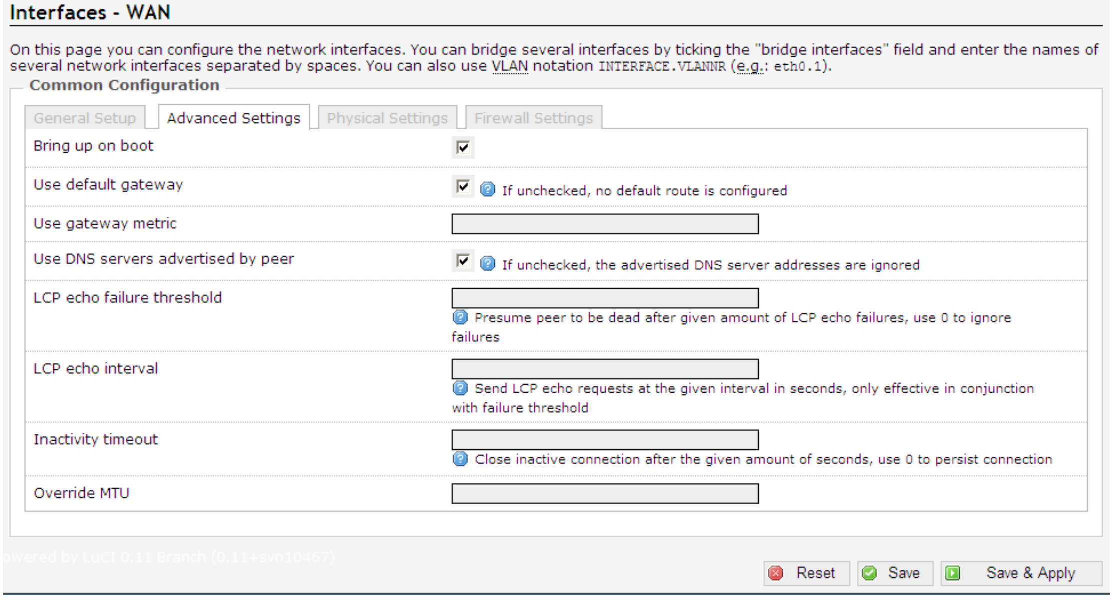


Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status	pppoe-wan **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)
Protocol	PPPoE
PAP/CHAP username	
PAP/CHAP password	
Access Concentrator	Leave empty to autodetect
Service Name	Leave empty to autodetect



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bring up on boot	☑
Use default gateway	☑ If unchecked, no default route is configured
Use gateway metric	
Use DNS servers advertised by peer	☑ If unchecked, the advertised DNS server addresses are ignored
LCP echo failure threshold	Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP echo interval	Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactivity timeout	Close inactive connection after the given amount of seconds, use 0 to persist connection
Override MTU	

owered by LuCI 0.11 Branch (0.11+svn10467)

PAP/CHAP username, PAP/CHAP password: Please enter your ISP username and password.

Access Concentrator: input connector center terminal, computer or communications device connection point device. Leave empty to autodetect.

Service Name: Enter the name of your broadband connection, leave empty to autodetect.

Use default gateway: Check in at the gateway to fill empty default route is not configured.

Use gateway metric: Destination network segment midway need to go through a few, that is, how many APs through.

Use DNS servers advertised by peer: Check the DNS server address in the fill blank are ignored at the advertised DNS server address.

LCP echo failure threshold: LCP, which link control protocol(Link Control Protocol), is a subset of the PPP agreement, the PPP communication, the sender and receiver by sending LCP packets to determine that the necessary information in the data transmission. Check the link LCP identification equipment, the decision whether to accept or reject; determine the number of bytes transferred in packets that can be received; check both configurations match, if you do not match the broken link. Only in the case of LCP packet links are available, the data communication network can be achieved. LCP is responsible for creating a link between the equipment, maintenance and termination. After a specified number of LCP response failures assumed link is disconnected, 0 to ignore failure.

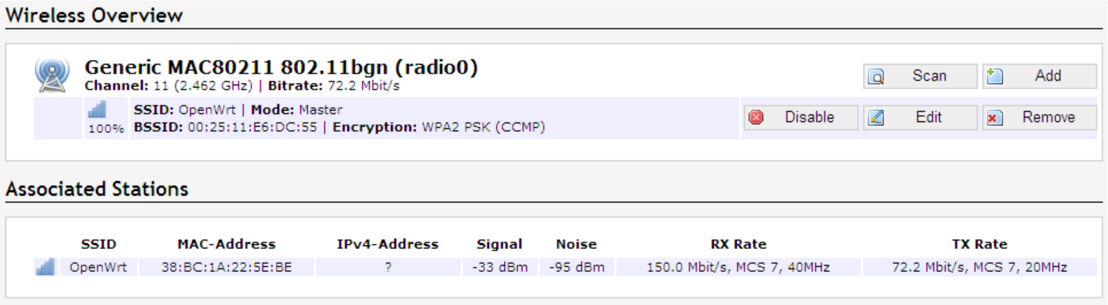
LCP echo interval: time to send LCP response(s), only when combined with effective fault threshold.

Inactivity timeout: Timing off inactive link(s), 0 for persistent connections.

Override MTU: MTU called the data transmission unit, the default is 1500. Please ask if need to change to the ISP. Such as non-special needs, do not change.

4.4.2 Wifi

Click the "Network>Wifi" option, you can see the following screen.



Wireless Overview

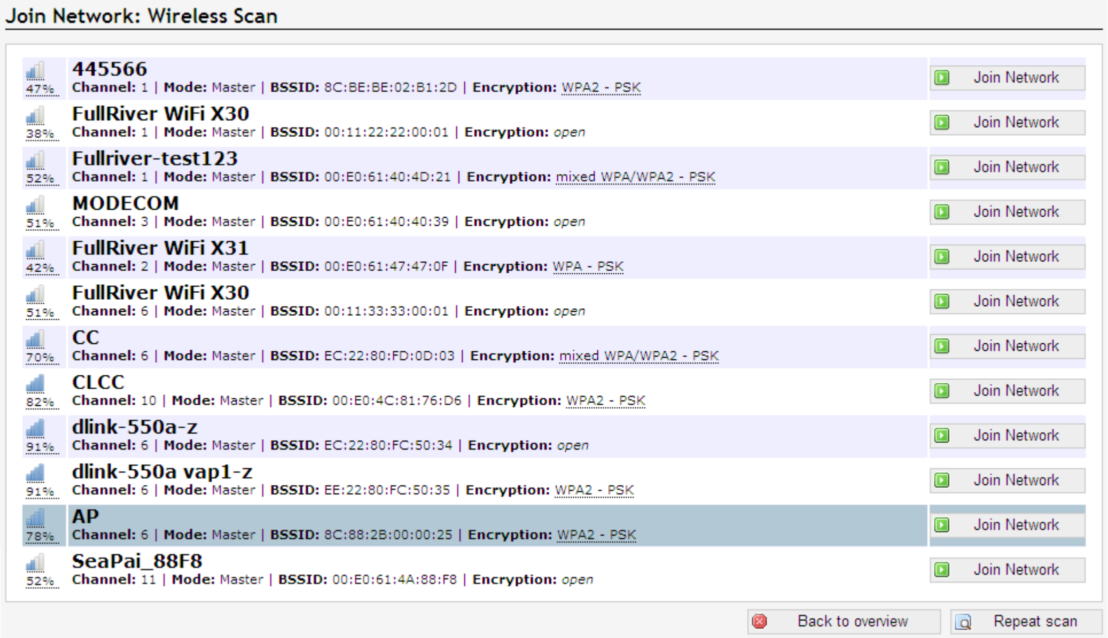
Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 72.2 Mbit/s

100% **SSID:** OpenWrt | **Mode:** Master
BSSID: 00:25:11:E6:DC:55 | **Encryption:** WPA2 PSK (CCMP)

Associated Stations

	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
	OpenWrt	38:BC:1A:22:5E:BE	?	-33 dBm	-95 dBm	150.0 Mbit/s, MCS 7, 40MHz	72.2 Mbit/s, MCS 7, 20MHz

Click on the "Scan" button, you can enter the following interface.



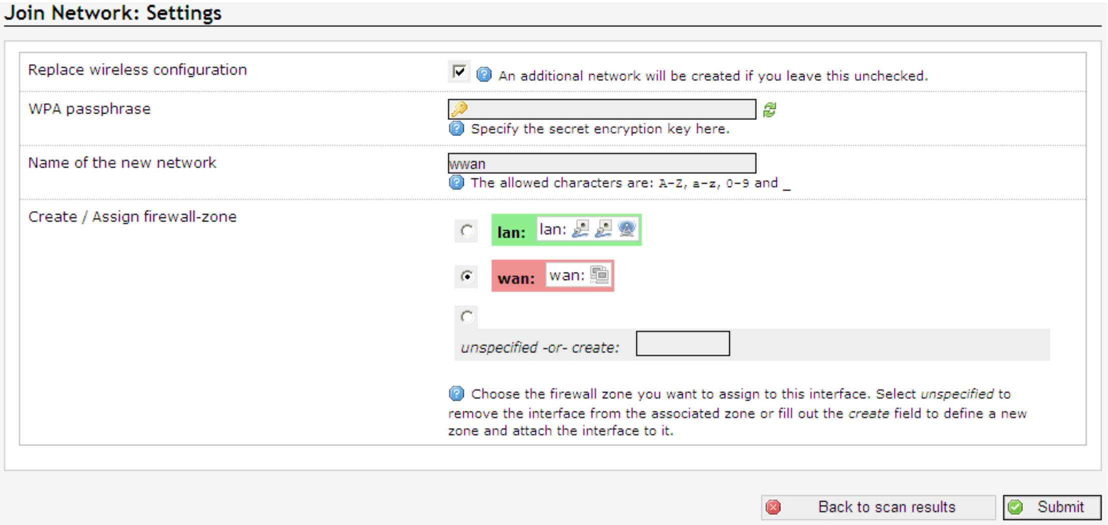
Join Network: Wireless Scan

47%	**445566** **Channel:** 1 | **Mode:** Master | **BSSID:** 8C:BE:BE:02:B1:2D | **Encryption:** WPA2 - PSK	Join Network
38%	**FullRiver WiFi X30** **Channel:** 1 | **Mode:** Master | **BSSID:** 00:11:22:22:00:01 | **Encryption:** *open*	Join Network
52%	**Fullriver-test123** **Channel:** 1 | **Mode:** Master | **BSSID:** 00:E0:61:40:4D:21 | **Encryption:** mixed WPA/WPA2 - PSK	Join Network
51%	**MODECOM** **Channel:** 3 | **Mode:** Master | **BSSID:** 00:E0:61:40:40:39 | **Encryption:** *open*	Join Network
42%	**FullRiver WiFi X31** **Channel:** 2 | **Mode:** Master | **BSSID:** 00:E0:61:47:47:0F | **Encryption:** WPA - PSK	Join Network
51%	**FullRiver WiFi X30** **Channel:** 6 | **Mode:** Master | **BSSID:** 00:11:33:33:00:01 | **Encryption:** *open*	Join Network
70%	**CC** **Channel:** 6 | **Mode:** Master | **BSSID:** EC:22:80:FD:0D:03 | **Encryption:** mixed WPA/WPA2 - PSK	Join Network
82%	**CLCC** **Channel:** 10 | **Mode:** Master | **BSSID:** 00:E0:4C:81:76:D6 | **Encryption:** WPA2 - PSK	Join Network
91%	**dlink-550a-z** **Channel:** 6 | **Mode:** Master | **BSSID:** EC:22:80:FC:50:34 | **Encryption:** *open*	Join Network
91%	**dlink-550a vap1-z** **Channel:** 6 | **Mode:** Master | **BSSID:** EE:22:80:FC:50:35 | **Encryption:** WPA2 - PSK	Join Network
78%	**AP** **Channel:** 6 | **Mode:** Master | **BSSID:** 8C:88:2B:00:00:25 | **Encryption:** WPA2 - PSK	Join Network
52%	**SeaPai_88F8** **Channel:** 11 | **Mode:** Master | **BSSID:** 00:E0:61:4A:88:F8 | **Encryption:** *open*	Join Network

If you want to join the SSID as "AP" in the network, according to the following steps to configure.

Step 1: first determine the IP "AP" where(for example 192.168.1.2), encryption(WPA), channels(6 channels). Then modify your AP's LAN port IP, must be "AP" in the same subnet(192.168.1.X), encryption, channel must also be "AP" setting is the same.

Step 2: Select the "AP", click on the option of "Join Network" button, enter the following setting interface.



Join Network: Settings

Replace wireless configuration ☑ An additional network will be created if you leave this unchecked.

WPA passphrase
Specify the secret encryption key here.

Name of the new network wwan
The allowed characters are: A-Z, a-z, 0-9 and _

Create / Assign firewall-zone
○ lan: lan:
● wan: wan:
○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Step 3: Fill WPA passphrase(AP wireless password), the same of the new network.

Step 4: Select "Create/assign firewall-zone", or if you choose, you have a good firewall distribution area; If selected, fill in the "Create" tab, you can create a firewall area.

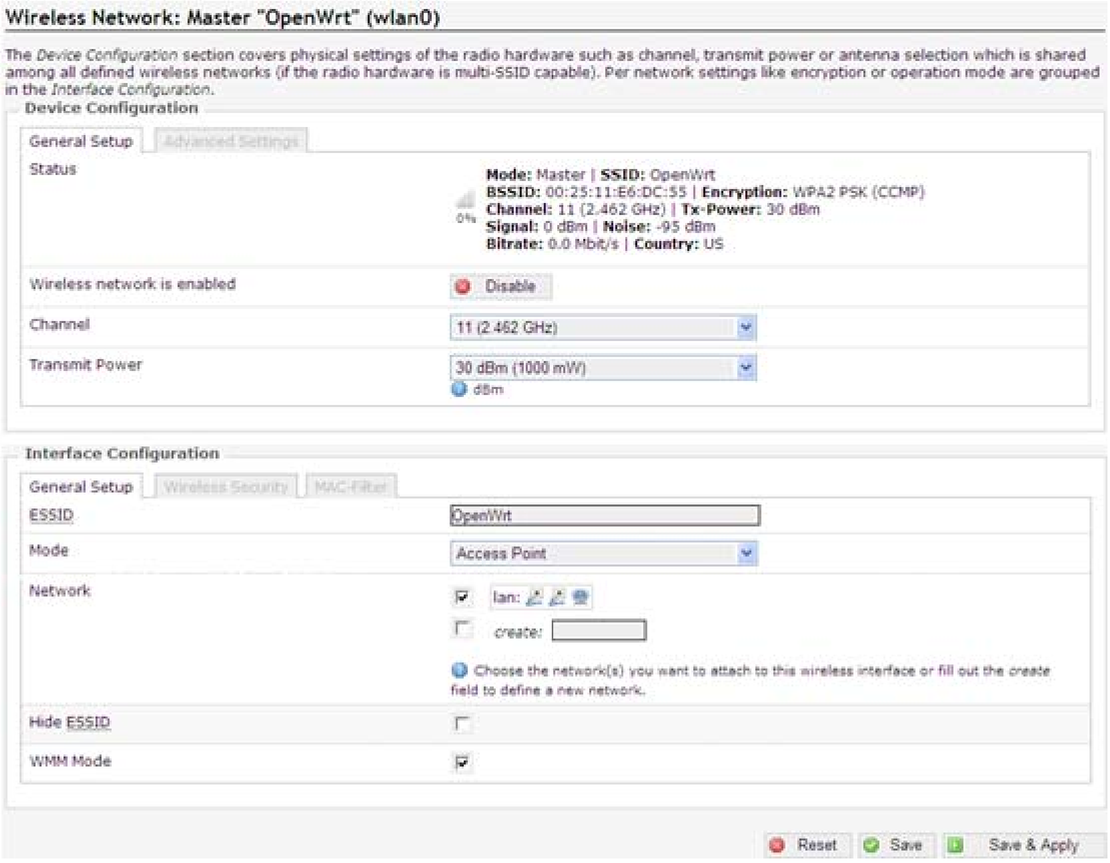
Step 5: Click "Submit" button, enter the following interface.

Associated Stations

You can see the information on this device is connected to your wireless network, MAC address, IP address, signal, noise, transmission rate and receive rates and other information.

4.4.2.1 Radio0: Master "OpenWrt"

Click the "Network>Wifi>Radio0: Master "OpenWrt" option, Device Configuration and Interface Configuration can be configured.



Wireless Network: Master "OpenWrt" (wlan0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which is shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

Status: 0% **Mode:** Master | **SSID:** OpenWrt
BSSID: 00:25:11:E6:DC:55 | **Encryption:** WPA2 PSK (CCMP)
Channel: 11 (2.462 GHz) | **Tx-Power:** 30 dBm
Signal: 0 dBm | **Noise:** -95 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

Wireless network is enabled: Disable

Channel: 11 (2.462 GHz)

Transmit Power: 30 dBm (1000 mW)
dBm

Interface Configuration

ESSID: OpenWrt

Mode: Access Point

Network: ☑ lan:
☐ create:
Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

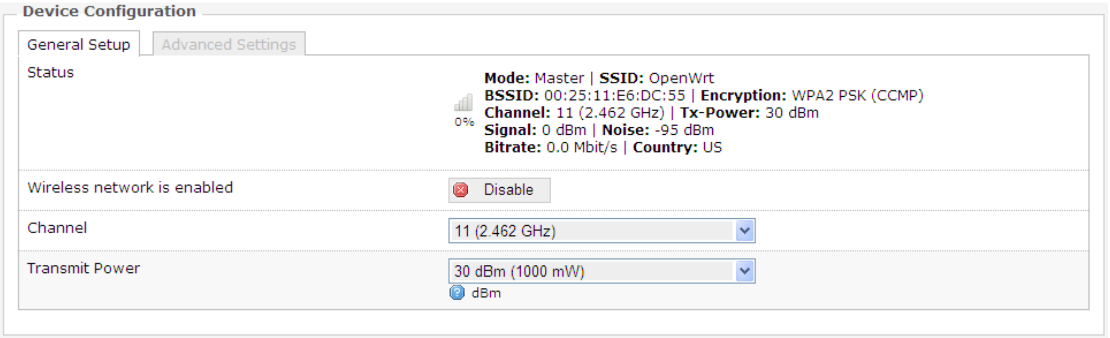
Hide ESSID: ☐

WMM Mode: ☑

Device Configuration

Device Configuration is divided into General Setup and Advance Settings.

Click on the "General Setup" option, you can see the following interface.



Device Configuration

Status: 0% **Mode:** Master | **SSID:** OpenWrt
BSSID: 00:25:11:E6:DC:55 | **Encryption:** WPA2 PSK (CCMP)
Channel: 11 (2.462 GHz) | **Tx-Power:** 30 dBm
Signal: 0 dBm | **Noise:** -95 dBm
Bitrate: 0.0 Mbit/s | **Country:** US

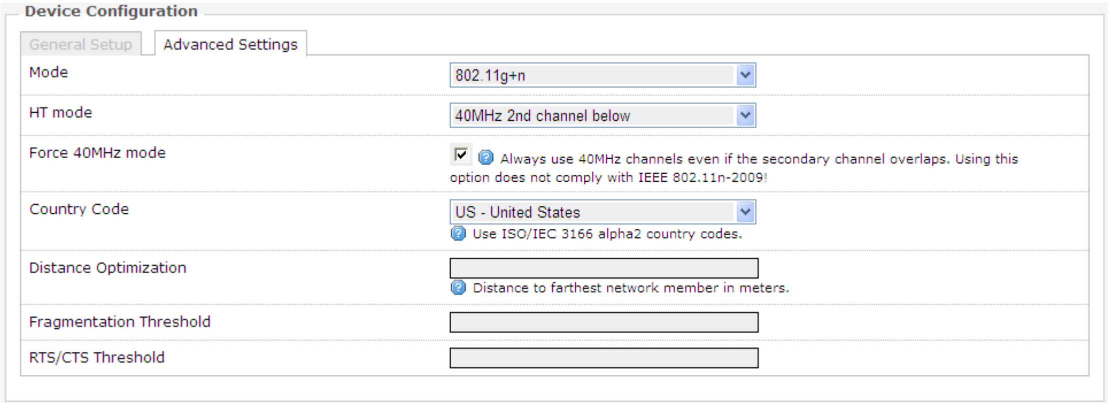
Wireless network is enabled: Disable

Channel: 11 (2.462 GHz)

Transmit Power: 30 dBm (1000 mW)
dBm

Channel: In the wireless signal transmitted as a data signal transmission media, channel selection range from 1 to 11.
Transmit Power: You can choose according to need to select the appropriate power.

Click on the "Advanced Settings" option, you can see the following interface.



Device Configuration

General Setup | Advanced Settings

Mode	802.11g+n
HT mode	40MHz 2nd channel below
Force 40MHz mode	☑ Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!
Country Code	US - United States Use ISO/IEC 3166 alpha2 country codes.
Distance Optimization	Distance to farthest network member in meters.
Fragmentation Threshold	
RTS/CTS Threshold	

Mode: Wireless AP is used to set the operating mode "automatic", "802.11b", "802.11g", "802.11g+n" four modes, we recommend that you select "802.11g+n", spread faster, more transmission range wide.

HT mode: "20MHZ", "40MHZ HT40-", “40MHZ HT40+” modes.

Country Code: Yon can select the desired country code from the drop-down list.

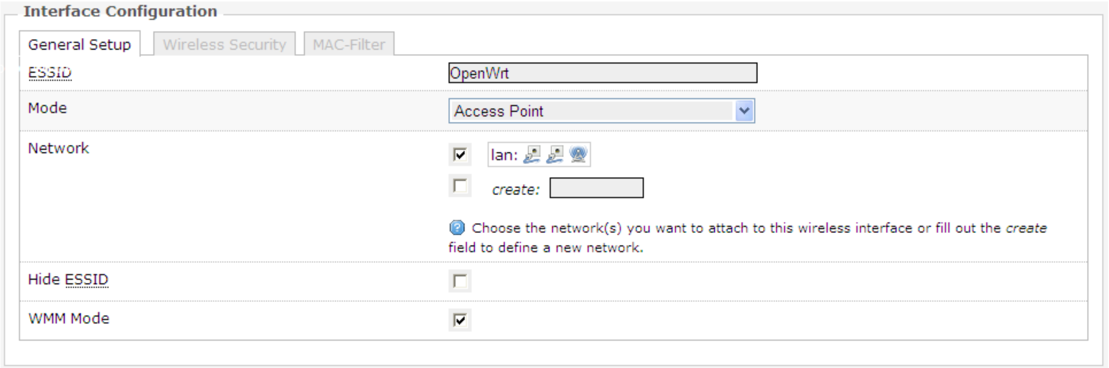
Distance Optimization: The data used to determine the maximum size of the package is divided into several packages before higher if the packet error rate, you may slightly increase the Fragmentation Threshold; if fragmentation threshold is set too low, it may degrade network performance. Recommended slightly lower defaults, but in most cases, should be left at its default value of 2346.

RTS/CTS Threshold: RTS is a Request-To-Send shorthand, CTS is Clear-To-Send shorthand. After setting up the RTS threshold, if it exceeds this threshold will send a message to be sent before the RTS, to reduce interference, the corresponding CTS will respond before the RTS. AP sends CTS data are generally rather Station sends RTS data.

Interface Configuration

Interface Configuration is divided into General Setup, Wireless Security and MAC-Filter three options.

Click on the "General Setup" option, you can see the following interface.



Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID	OpenWrt
Mode	Access Point
Network	☑ lan: □ *create:* Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.
Hide ESSID	□
WMM Mode	☑

ESSID: The difference between the service number and is used to identify a wireless network radio signals. The AP defaults to "OpenWrt", you can modify it to show your wireless network.

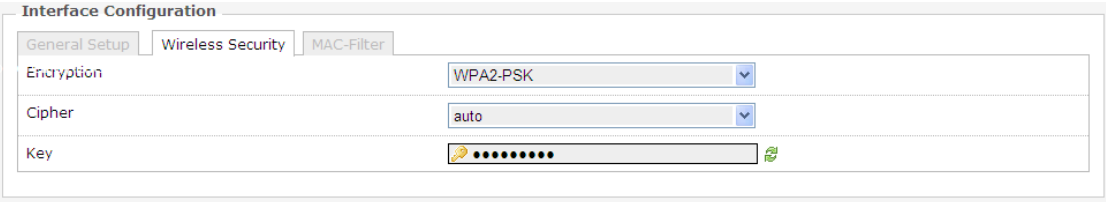
Mode: Yon can select your desired interface mode via the drop-down list.

Network: Select assigned to this network wireless interface.

Hide ESSID: If you check this, the search is less than you are currently using a AP.

WMM Mode: A sub-protocol wireless transmission protocol, to open, then a link to the AP requires hardware(mobile phones, laptops, etc.)are required to support it can ba linked successfully.

Click on the "Wireless Security" option, you can see the following interface.



Encryption: WPA2-PSK

Cipher: auto

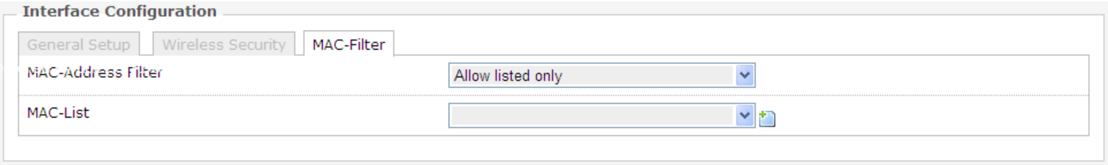
Key: ●●●●●●●●●

Encryption: The AP provides a "WEP Open System/Shared Key", "WPA-PSK/WPA2 -PSK", "WPA-EAP/WPA2-EAP", "WPA-PSK/WPA2-PSK Mixed Mode" and other seven encryption.

Cipher: The AP provides the "auto", "Force CCMP(AES)", "Force TKIP", "Force TKIP and CCMP(AES)".

Key: WEP, enter the 5 or 10 characters; WPA/WPA2, enter 8 or more characters. Recommends using WPA/WPA2 mode.

Click on the "MAC-Filter" option, you can see the following interface.



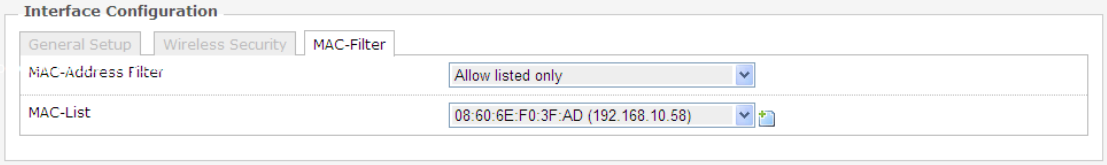
MAC-Address Filter: Allow listed only

MAC-List:

MAC-Address Filter: The AP provides a "disable", "Allow listed only", "Allow all except listed" in three ways.

MAC-List: Yon can fill the need for a host MAC address access restrictions within the wireless network.

Example: If you "MAC-Filter" fill in the interface's MAC address as "08-60-6E-F0-3F-AD" as shown below.



MAC-Address Filter: Allow listed only

MAC-List: 08:60:6E:F0:3F:AD (192.168.10.58)

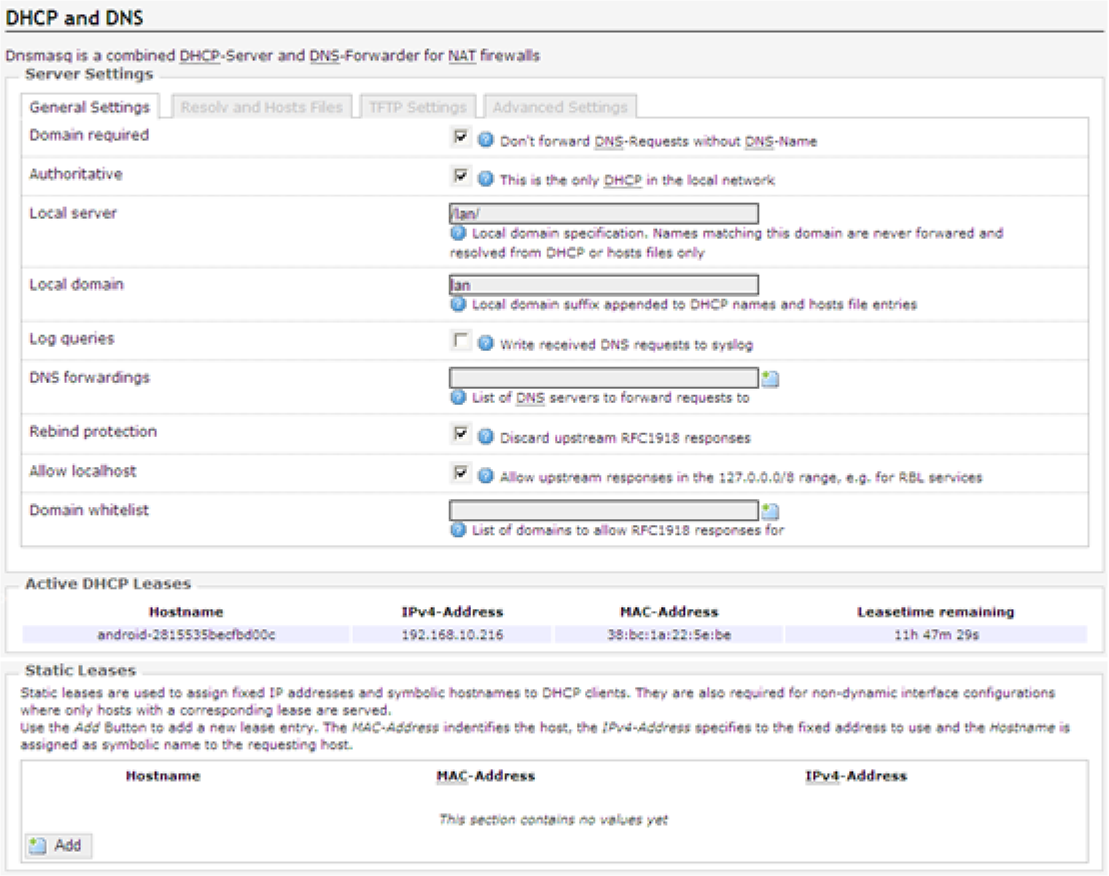
1. In "MAC-Filter" drop-down list, select "disable", the MAC-address filtering does not work.

2. In "MAC-Filter" drop-down list, select "Allow listed only", only allow MAC address is "08-60-6E-F0-3F-AD" host access your wireless network.

3. In "MAC-Filter" drop-down list, select "Allow all except listed", it is prohibited MAC address is "08-60-6E-F0-3F-AD" host access to your wireless network, you can access other hosts.

4.4.3 DHCP and DNS

Click the "Network > DHCP and DNS", you can see the following interface.



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Domain required	☑ Don't forward DNS-Requests without DNS-Name
Authoritative	☑ This is the only DHCP in the local network
Local server	/lan/ Local domain specification. Names matching this domain are never forwarded and resolved from DHCP or hosts files only
Local domain	lan Local domain suffix appended to DHCP names and hosts file entries
Log queries	☐ Write received DNS requests to syslog
DNS forwardings	List of DNS servers to forward requests to
Rebind protection	☑ Discard upstream RFC1918 responses
Allow localhost	☑ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	List of domains to allow RFC1918 responses for

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-2815535becfbd00c	192.168.10.216	38:bc:1a:22:5e:be	11h 47m 29s

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.

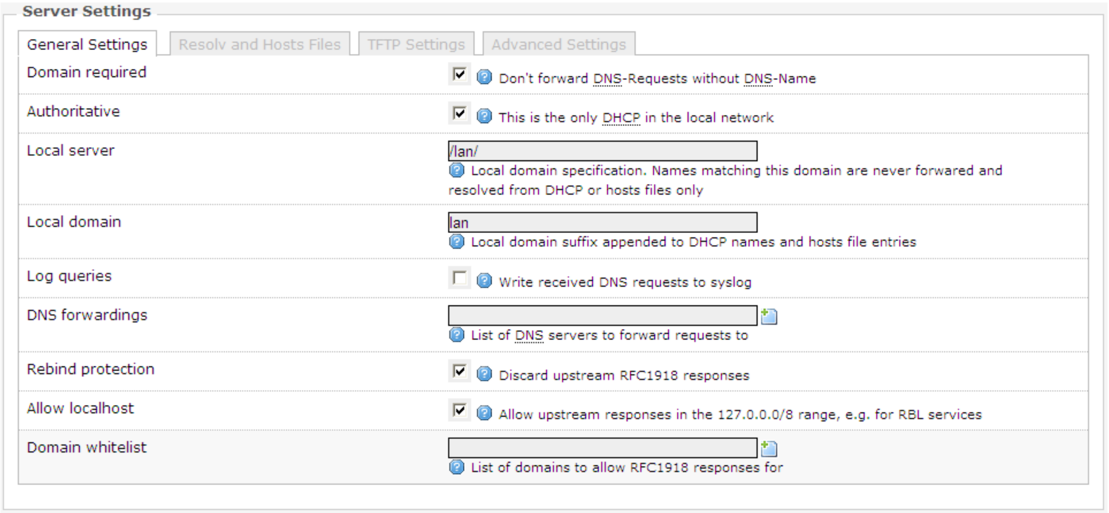
Hostname	MAC-Address	IPv4-Address

This section contains no values yet

Server Settings

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

Click on "General Settings" screen as shown below.



Server Settings

General Settings | Resolv and Hosts Files | TFTP Settings | Advanced Settings

Domain required: ☑ Don't forward DNS-Requests without DNS-Name
Authoritative: ☑ This is the only DHCP in the local network
Local server: /lan/ Local domain specification. Names matching this domain are never forwarded and resolved from DHCP or hosts files only
Local domain: lan Local domain suffix appended to DHCP names and hosts file entries
Log queries: ☐ Write received DNS requests to syslog
DNS forwardings: List of DNS servers to forward requests to
Rebind protection: ☑ Discard upstream RFC1918 responses
Allow localhost: ☑ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist: List of domains to allow RFC1918 responses for

Domain required: Enable DNS names are not forwarded no resolution requests.

Authoritative: unique within the network DHCP server.

Local server: the local domain rule, never forwarded and processed only from the local DHCP or HOSTS file name data.

Local domain: DNS is enabled, you will receive a written request to the system log.

DNS forwardings: The specified domain DNS resolution be forwarded to the specified

DNS server.

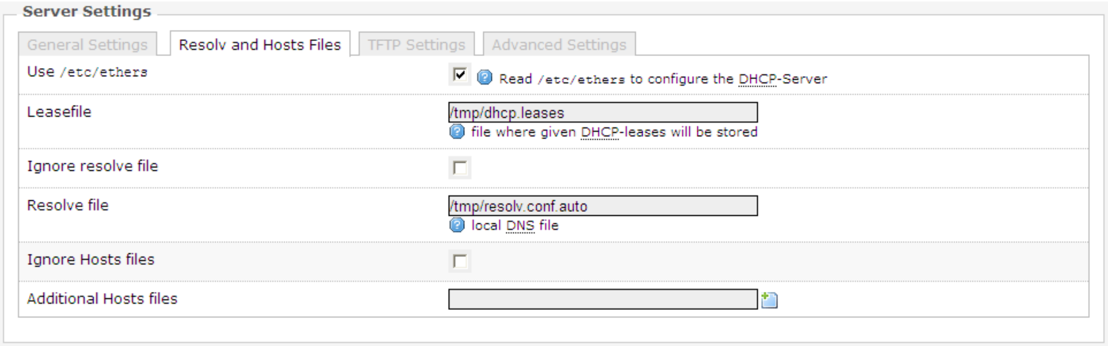
Rebind protection: Enable RFC1918 up link response data is discarded.

Allow localhost: Enable the Allow up link response within 127.0.0.0/8 loop range, for

Example: RBL services.

Domain Whitelist: Enter the allowed domain list RFC1918 response.

Click the "Resolv and Hosts Files", there may be the following interface.



Use /etc/ethers ☑ Read /etc/ethers to configure the DHCP-Server

Leasefile /tmp/dhcp.leases
file where given DHCP-leases will be stored

Ignore resolve file □

Resolve file /tmp/resolv.conf.auto
local DNS file

Ignore Hosts files □

Additional Hosts files

Use/ etc/ ethers: Enable according to/ etc/ ethers to configure DHCP-Server.

Leasefile: Store files DHCP lease.

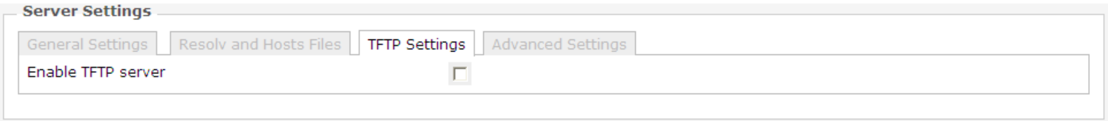
Ignore resolve file: Checked,then turn on this feature.

Resolve file: Store the local DNS resolution files.

Ignore the Hosts files: Checked,then turn on this feature.

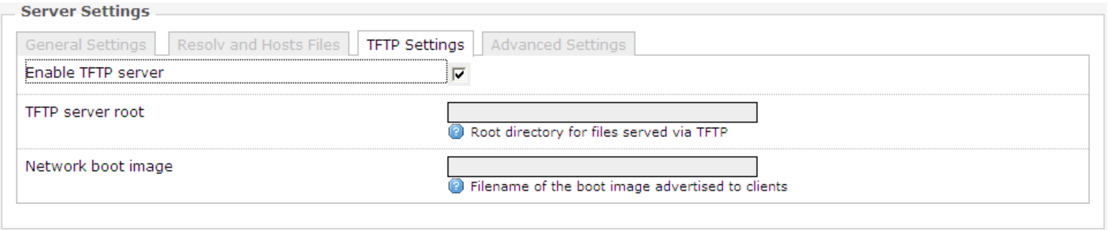
Additional Hosts files: Check this , turn on this feature .

Click "TFTP Settings" screen may appear as follows.



Enable TFTP server □

Enabling the TFTP server, then the following interface.



Enable TFTP server ☑

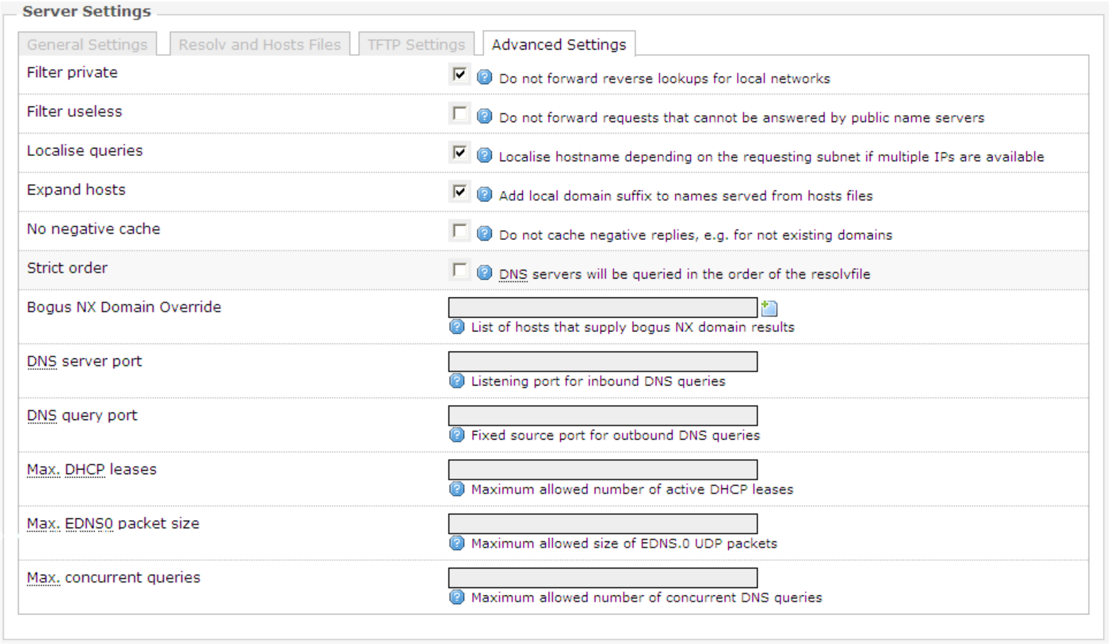
TFTP server root
Root directory for files served via TFTP

Network boot image
Filename of the boot image advertised to clients

TFTP server root: Store the root directory of the TFTP server.

Network boot image: Store advertised to the client boot image file name.

Click on the "Advanced Settings" screen may appear as follows.



Server Settings

Filter private	☑ Do not forward reverse lookups for local networks
Filter useless	□ Do not forward requests that cannot be answered by public name servers
Localise queries	☑ Localise hostname depending on the requesting subnet if multiple IPs are available
Expand hosts	☑ Add local domain suffix to names served from hosts files
No negative cache	□ Do not cache negative replies, e.g. for not existing domains
Strict order	□ DNS servers will be queried in the order of the resolvfile
Bogus NX Domain Override	List of hosts that supply bogus NX domain results
DNS server port	Listening port for inbound DNS queries
DNS query port	Fixed source port for outbound DNS queries
Max. DHCP leases	Maximum allowed number of active DHCP leases
Max. EDNS0 packet size	Maximum allowed size of EDNS.0 UDP packets
Max. concurrent queries	Maximum allowed number of concurrent DNS queries

Filter private: no forwarding enabled local network lookups reverse lookup command.

Filter useless: Public domain name server is not enabled unable to respond to requests forwards.

Localization queries: When there are multiple IP, enabling this feature will be based on the subnet request to localize the source of a host name.

Expand hosts: Enables you to add a local domain suffix to the hosts file name.

No negative cache: cache is not enabled useless responses, such as domain does not exist.

Strict order: Enable you will query the DNS in the specified order.

Bogus NX Domain Override: Enter the domain name to allow false responses empty server list.

DNS server port: Enter the inbound DNS query port.

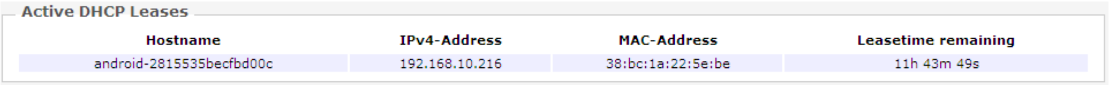
DNS query port: Enter the specified DNS query source port.

Max. DHCP leases: Enter the maximum allowed number of leased DHCP.

Max. EDNS0 packet size: Enter the maximum allowed EDNS.0 UDP packet size.

Max. concurrent queries: Enter the maximum number of concurrent DNS lookup allowed.

Active DHCP Leases



Active DHCP Leases

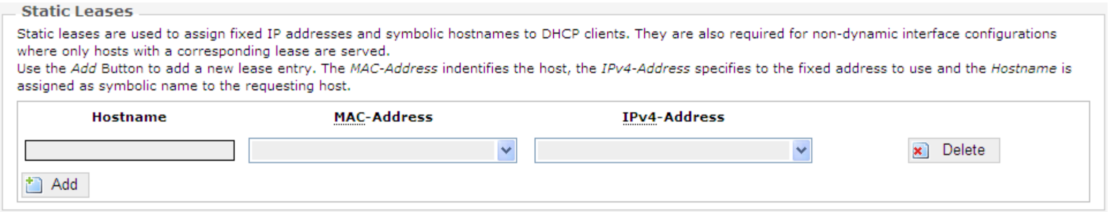
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-2815535becfbd00c	192.168.10.216	38:bc:1a:22:5e:be	11h 43m 49s

If another device is connected to this network, there will be a display device host name, IPv4 address, MAC address, and the remaining lease and other information on this box.

Static Leases

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

Use the Add Button to add a new lease entry. The MAC-Address identifies the host, the IPv4-Address specifies to the fixed address to the Hostname is assigned as symbolic name to the requesting host.



Static Leases

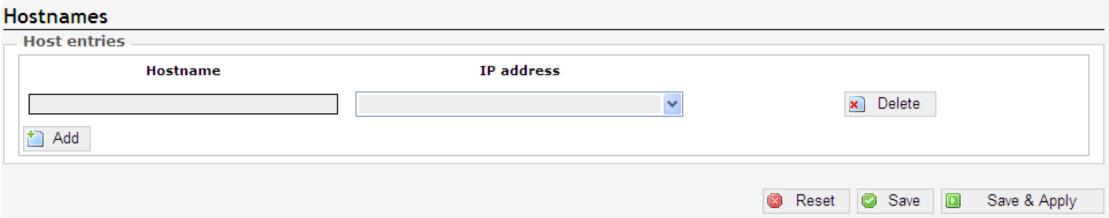
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.

Use the *Add* Button to add a new lease entry. The *MAC-Address* 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	
			Delete

4.4.4 Hostnames

Click on the "Network>Hostnames" option, you can see the following interface.



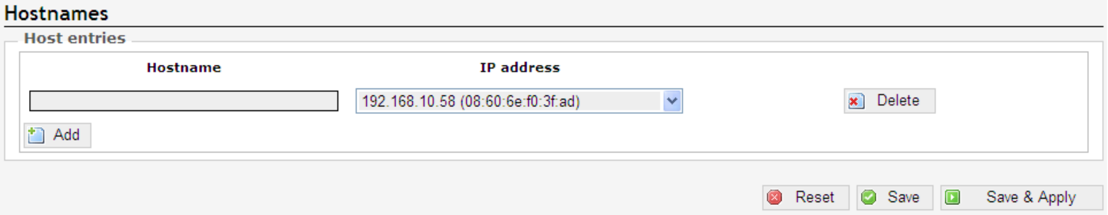
Hostnames

Host entries

Hostname	IP address	
		Delete

This feature is for your convenience with easy to remember way to access the host you need.

Click the "Add" button, fill in the box to add the host name and IP address, and then click "Save&Apply" button.



Hostnames

Host entries

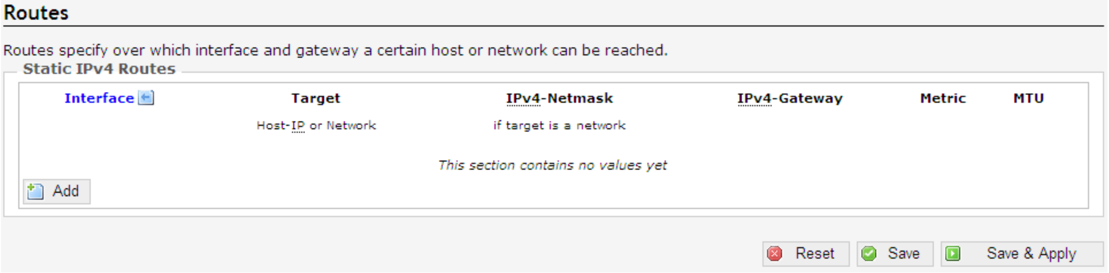
Hostname	IP address	
	192.168.10.58 (08:60:6e:f0:3f:ad)	Delete

Hostname: The name of the host you want to access, for example: aa.

IP address: The host you want to access the corresponding IP address.

4.4.5 Static Routes

Click on the "Network>Static Routes" option, you can see the following interface.



Routes

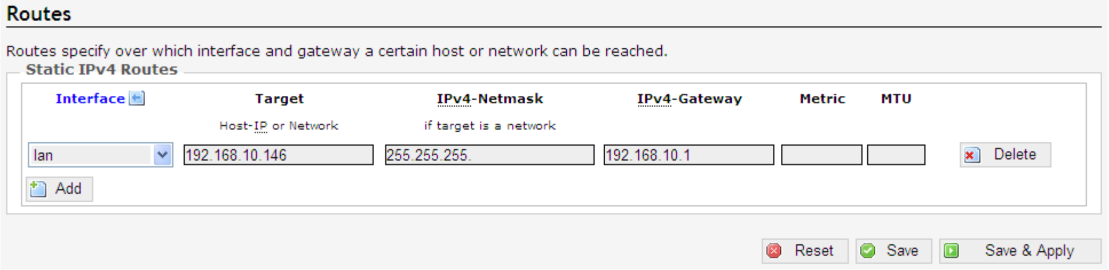
Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

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

This section contains no values yet

Static routing is a static routing table information. In some network environments, you need to modify the static routing table that specifies a static AP to communicate properly. For example, within a specified network host access 192.168.10.146 this network, you can press operation, click the "Add" button, make the following configuration, you can visit with you not in the same segment of the network.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target Host-IP or Network	IPv4-Netmask if target is a network	IPv4-Gateway	Metric	MTU	
lan	192.168.10.146	255.255.255.	192.168.10.1			Delete

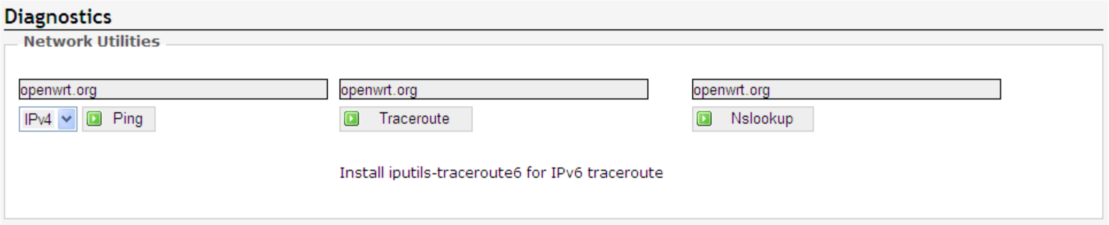
Target: Enter the network address of the destination network.

IPv4-Netmask: Enter the netmask address of the destination network.

IPv4-Gateway: Enter the gateway address that matches the destination network data delivery.

4.4.6 Diagnostics

Click on the "Network>Diagnostics" option, you can see the following interface.



Diagnostics

Network Utilities

openwrt.org | openwrt.org | openwrt.org

Install iputils-traceroute6 for IPv6 traceroute

Use the ping command to test the client-to-gateway connection is normal.

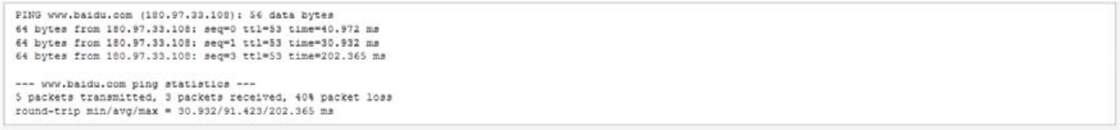
Tracert command to trace the AP, Tracert command can be used to track the use of packet routing (path). Check the network hop routing information to confirm the export terminal to the network connectivity.

Nslookup command to check the DNS resolve is configured correctly.

If you want to check your current network connections, you can follow the steps below.

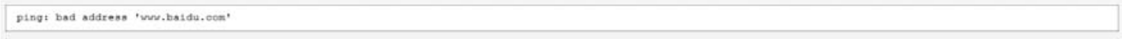
1. Fill "www.baidu.com" In the first box, click on "ping" button.

If the interface is shown, then connect you to the gateway of normal.



```
PING www.baidu.com (180.97.33.108): 56 data bytes
64 bytes from 180.97.33.108: seq=0 ttl=53 time=40.972 ms
64 bytes from 180.97.33.108: seq=1 ttl=53 time=30.932 ms
64 bytes from 180.97.33.108: seq=3 ttl=53 time=202.365 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 3 packets received, 40% packet loss
round-trip min/avg/max = 30.932/91.423/202.365 ms
```

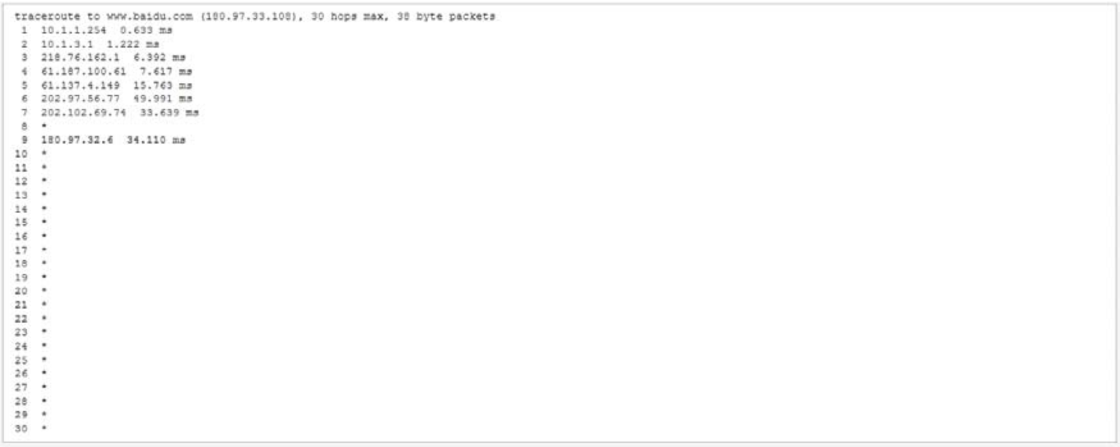
If the interface appears as shown below, then connect you to the gateway is not normal.



```
ping: bad address 'www.baidu.com'
```

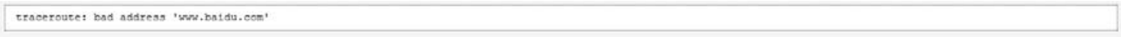
2.Fill "www.baidu.com" in the second box, click the "Traceroute" button.

If the interface is shown below appears, you are connected to the network outlet is.



```
traceroute to www.baidu.com (180.97.33.108), 30 hops max, 38 byte packets
 1  10.1.1.254  0.633 ms
 2  10.1.3.1  1.222 ms
 3  218.76.162.1  6.392 ms
 4  61.187.100.61  7.617 ms
 5  61.137.4.149  15.763 ms
 6  202.97.56.77  49.991 ms
 7  202.102.69.74  33.639 ms
 8  *
 9  180.97.32.6  34.110 ms
10  *
11  *
12  *
13  *
14  *
15  *
16  *
17  *
18  *
19  *
20  *
21  *
22  *
23  *
24  *
25  *
26  *
27  *
28  *
29  *
30  *
```

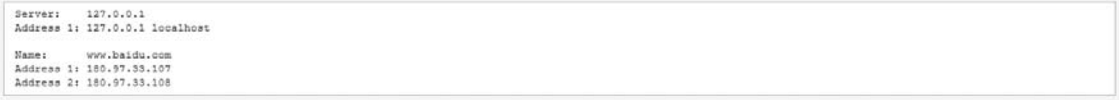
If the interface appears as shown below, then you are not connected to a network of export.



```
traceroute: bad address 'www.baidu.com'
```

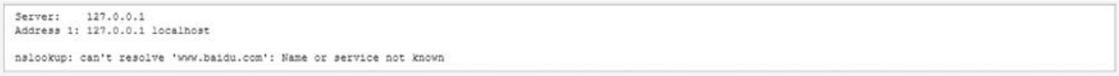
3. Fill "www.baidu.com" In the third box, click on the "Nslookup" button.

If the interface appears as shown below, then configure the correct DNS resolution.



```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

Name:      www.baidu.com
Address 1: 180.97.33.107
Address 2: 180.97.33.108
```

If the interface is shown there, the instructions to configure DNS resolution is not correct.



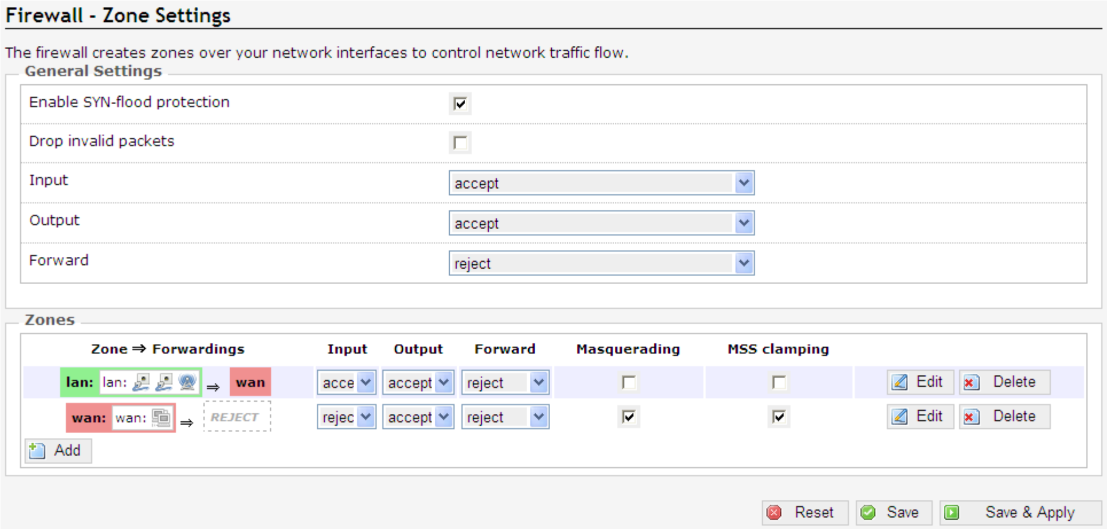
```
Server:    127.0.0.1
Address 1: 127.0.0.1 localhost

nslookup: can't resolve 'www.baidu.com': Name or service not known
```

4.4.7 Firewall

Click on the "Network>Firewall" option, you can make General Settings, Port Forwards, Traffic Rules, Custom Rules.

4.4.7.1 General Settings

Click on the "Network>Firewall>General Settings" option, you can see the following interface.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

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

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan: lan: ⇒ wan	acce	accept	reject	□	□	Edit	Delete
wan: wan: ⇒ REJECT	rejec	accept	reject	☑	☑	Edit	Delete

General Settings

Enable SYN-flood defenses: SYN Flood is currently the most popular DoS(Denial of Service Attack)with one of the DDoS(distributed denial of service attack)approach, which is a using TCP protocol flaw, sending a large number of forged TCP connection requests, thereby causing the attacker depletion of resources(CPU full load or insufficient memory) way to attack. Enabling you can defend some denial of service attacks.

Drop invalid packets: Check the packet is discarded invalid.

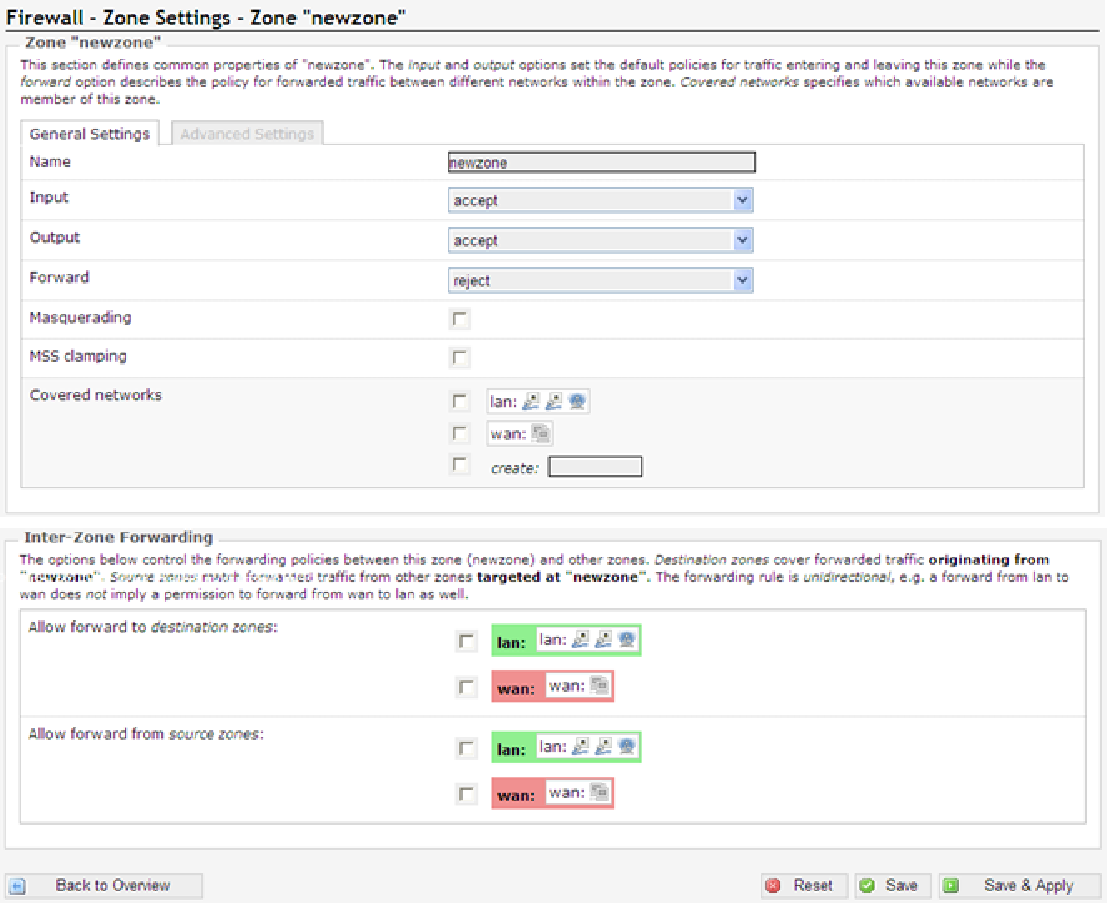
Input: It is passed from the remote data locally. Discarded, simply discards invalid data, does not respond to any feedback. Needs of customers waiting for a timeout, the customer is likely to find himself blocked by a firewall; refused to return a reject(terminate) invalid data packets(TCP FIN or UDP-ICMP-PORT-UNREACHABLE), explicitly rejected the other's connection action; accept, receive effective inbound data.

Output: It refers came from local to remote data.

Forward: It refers to a specific(one or more)data packets between different subnets forwarding area.

Regional

Click the "Add" button, the following interface will appear.



Firewall - Zone Settings - Zone "newzone"

Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

General Settings | Advanced Settings

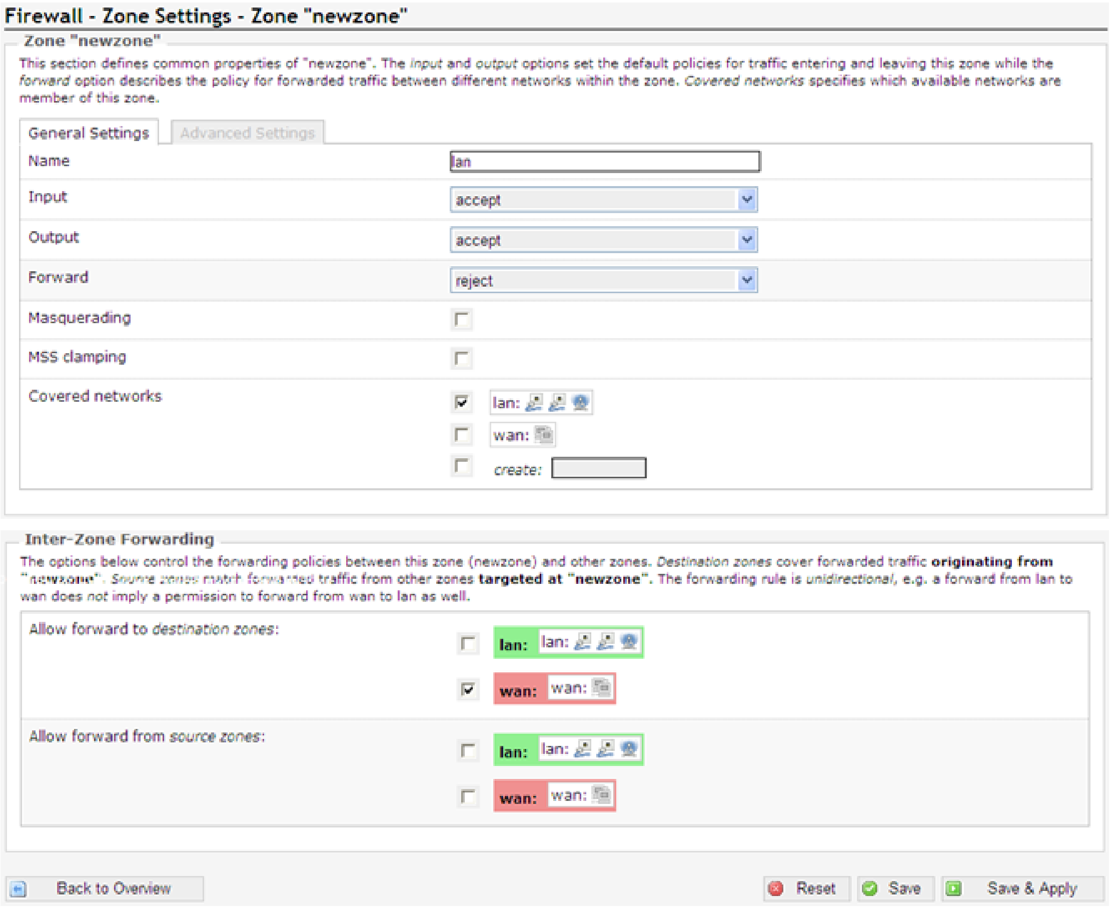
Name	newzone
Input	accept
Output	accept
Forward	reject
Masquerading	□
MSS clamping	□
Covered networks	□ lan: □ wan: □ *create:*

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from "newzone"**. *Source zones match forwarded* traffic from other zones **targeted at "newzone"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones:*	□ **lan:** lan: □ **wan:** wan:
Allow forward from *source zones:*	□ **lan:** lan: □ **wan:** wan:

For example you want to add "lan⇒wan", then make the following settings.



Firewall - Zone Settings - Zone "newzone"

Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

Name	lan
Input	accept
Output	accept
Forward	reject
Masquerading	□
MSS clamping	□
Covered networks	☑ lan: □ wan: □ *create:*

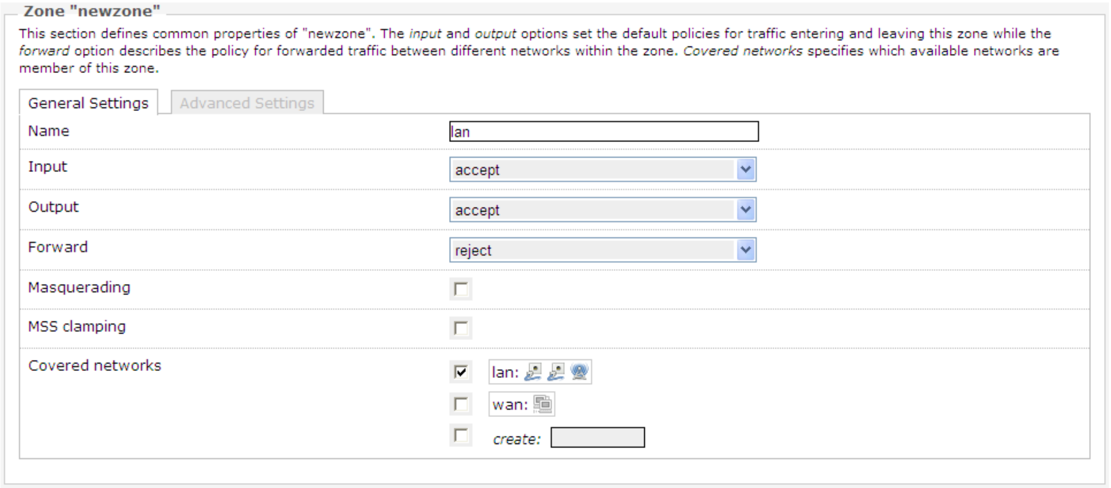
Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from "newzone"**. *Source zones match forwarded* traffic from other zones **targeted at "newzone"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones:*	□ **lan:** lan: ☑ **wan:** wan:
Allow forward from *source zones:*	□ **lan:** lan: □ **wan:** wan:

Regional "newzone"

General Settings



Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

Name	lan
Input	accept
Output	accept
Forward	reject
Masquerading	□
MSS clamping	□
Covered networks	☑ lan: □ wan: □ *create:*

Name: lan.

Inbound and outbound data packet for setting "in" "out" AP(an interface) default.

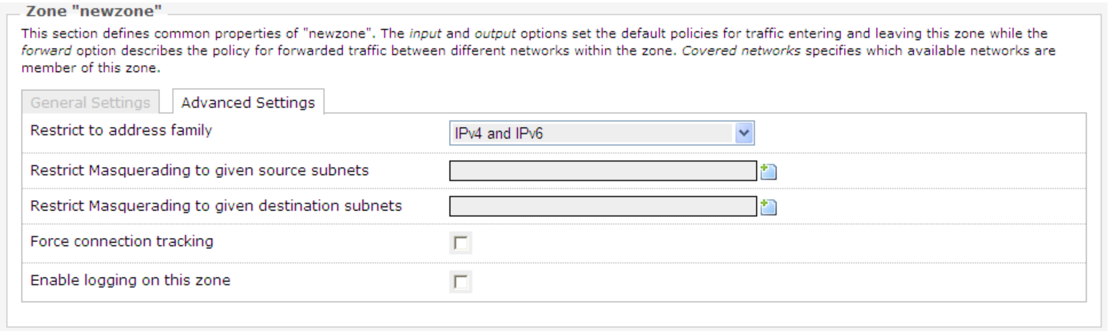
Forward: It refers to a specific(one or more) data packets between different subnets forwarding area.

Masquerading: IP masquerading is a special kind of SNAT rule, when a computer within the network computers to access the external network through the AP, it replaces the source address of IP packets to a predetermined address(usually the external network card address). In this way, the computer will think outside the network, the packet is sent to this AP response packets can be correctly returned to the AP. (Otherwise, the network computer IP address 192.168.XXX.XXX, for external network servers, do not know how to return, or return to other computers go up.)

MSS clamping: MSS value that is the largest data segment for each TCP packet can be transmitted. In order to achieve the best performance of TCP transport protocol connection is established when the two sides are usually negotiated MSS value that the TCP protocol at the time of realization is often replaced with the MTU value, check you can clearly tell the remote: Do sent packets exceed this value.

Covered networks: Select the network belonging to this region.

Advanced Settings



Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

General Settings | Advanced Settings

Restrict to address family	IPv4 and IPv6
Restrict Masquerading to given source subnets	
Restrict Masquerading to given destination subnets	
Force connection tracking	□
Enable logging on this zone	□

Restrict to address family: Here you can choose to limit the type of address.

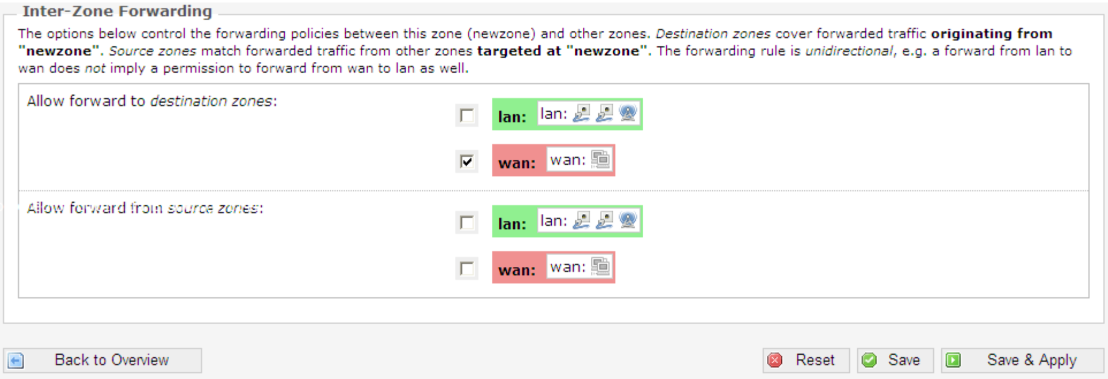
Restrict Masquerading to given source subnets: Enter the IP address of your internal Network.

Restrict Masquerading to given destination subnets: Enter the IP address of the firewall legitimate(usually outside the network card address).

Forced connection tracking: Checked,then turn on this feature.

Enable logging on this zone: Checked,then turn on this feature.

Inter-Zone Forwarding



Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from "newzone"**. *Source zones* match forwarded traffic from other zones **targeted at "newzone"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

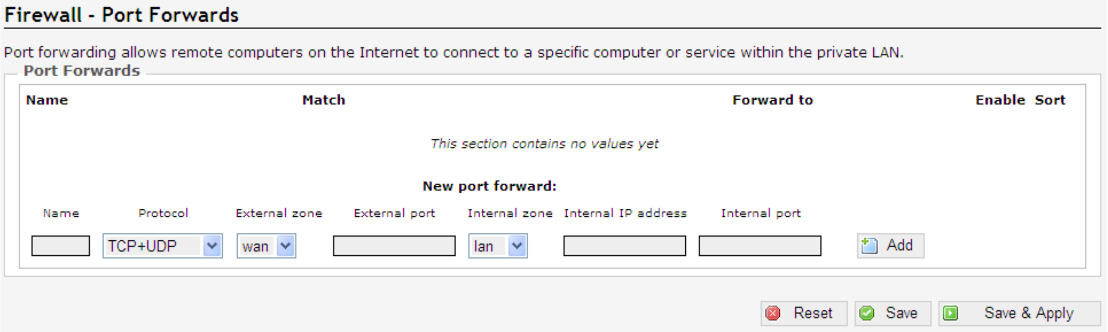
Allow forward to *destination zones*:	□ lan: lan: ☑ wan: wan:
Allow forward from *source zones*:	□ lan: lan: □ wan: wan:

Figure above options can control area (lan) and forwarding rules for other regions. Target area received from "lan" forwarding traffic. Forwarding traffic from the source region to match the target as requiring "lan" in the region. If the hook option shown, then the following rules can not forward: forward lan traffic to wan, but does not allow wan forwarded to the lan.

After the above are set, click "Save & Apply" button to successfully add a firewall area.

4.4.7.2 Port Forwards

Click on the "Network>Firewall>Port Forwards" option, you can see the following interface.



Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort

This section contains no values yet

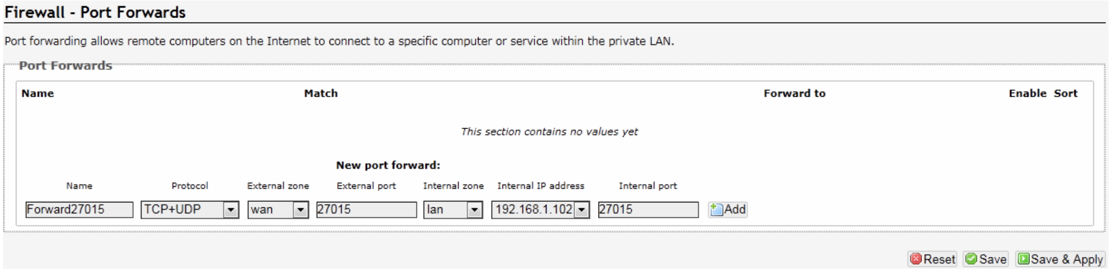
New port forward:

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

This interface provides configure port forwarding rules. When the network using a private address 10.X.X.X/172.16.X.X/192.168.X.X, external network can not access the network directly within the server. By doing port forwarding on the AP, then the configuration of the network server IP and port, external network can access the network server to use the services provided by the network.

Example: There are 50 computers in the network have been configured an FTP server, its IP address is 192.168.1.102, if you want Internet users can also access this server, you can make the following actions.

Click the "Add" button, make the following configuration, the configuration is completed, click "Save&Apply" button.



Firewall - Port Forwards

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

Port Forwards

Name	Match	Forward to	Enable	Sort

This section contains no values yet

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port	
Forward27015	TCP+UDP	wan	27015	lan	192.168.1.102	27015	Add

Name: Please fill in an easy to remember name.

Protocol: Protocol used by the service provided by the server. If not clear what kind of agreement, you can choose "TCP+UDP" protocol. Please refer to the "common ports and services table".

External zone: WAN area.

External port: Specify an opening port, mapped to the internal server ports open. If not specified, the same external port and internal port. Fill in the range 1-65535.

Internet zone: Internal LAN area.

Internet IP address: IP address of the network server.

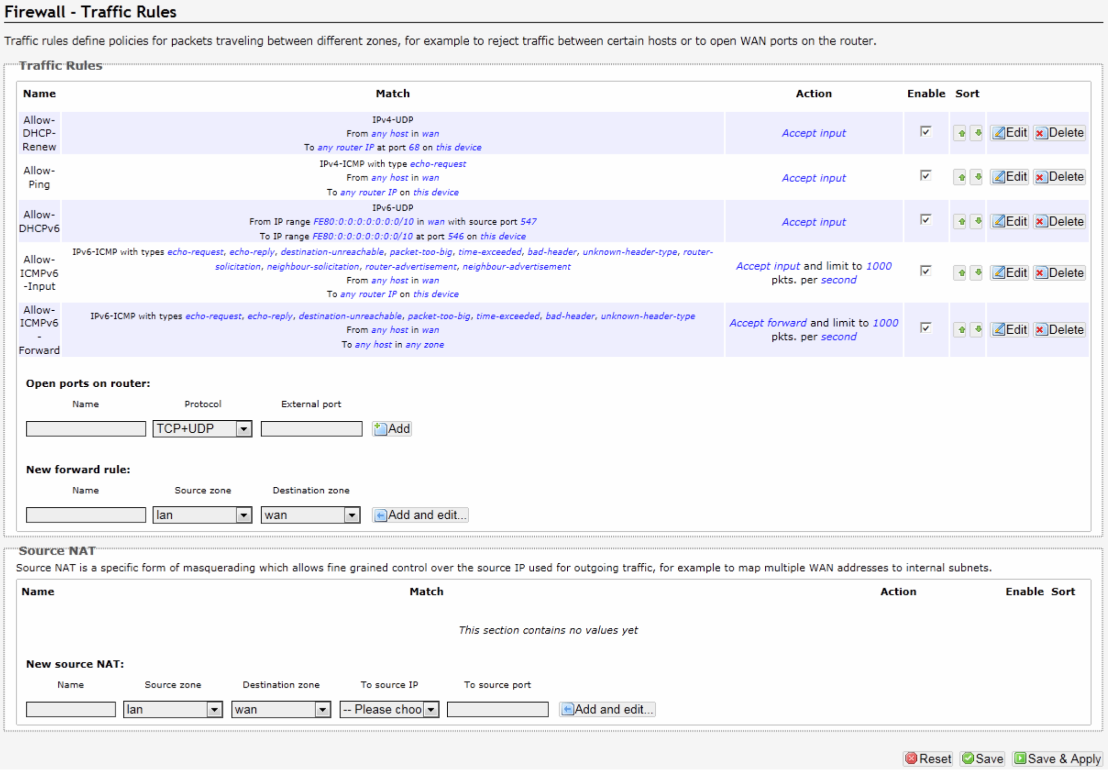
Internet port: Port services provided by the server within the network used. Please refer to the "common ports and services table".

common ports and services table

Network Services	Agreement	Port
ftp	TCP	21
Ssh	TCP	22
telnet	TCP	23
Smtp	TCP	25
Time	TCP	37
DNS	UDP	53
www	TCP	80
POP3	TCP	110
Snmp	UDP	161
CS server	TCP	27015

4.4.7.3 Traffic Rules

Click on the "Network>Firewall>Traffic Rules" option, you can see the following interface.



Firewall - Traffic Rules

Traffic rules define policies for packets traveling 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

Open ports on router:

Name	Protocol	External port	
	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	
	lan	wan	Add and edit...

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

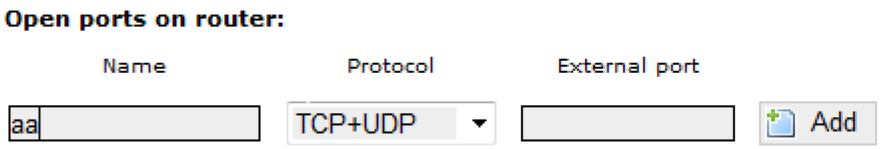
This section contains no values yet

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
	lan	wan	-- Please choo		Add and edit...

Communication rules define the traffic transmitted between different regions, for example: some refuse to communications between the host and open to the WAN port.

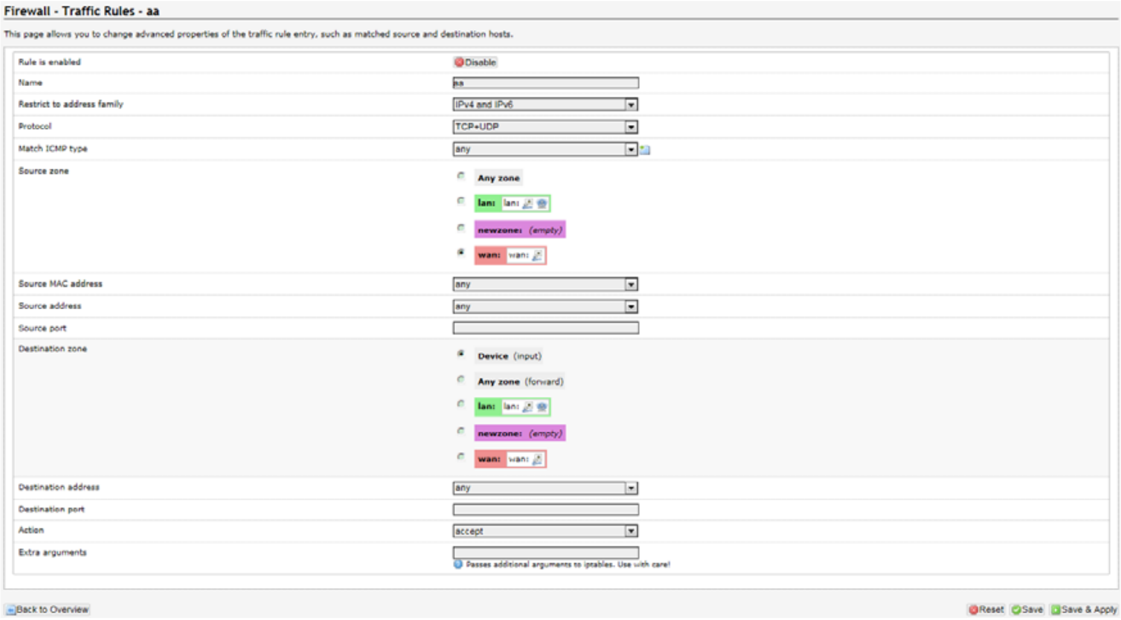
For example, you want to add the name of aa traffic rules, follow these steps to configure.



Open ports on router:

Name	Protocol	External port	
aa	TCP+UDP		Add

Fill in the information according to the map, click on the "Add" button, you can enter the following interface configuration.



Firewall - Traffic Rules - aa

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	Disable
Name	aa
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ○ lan: lan: ○ newzone: (empty) ● wan: wan:
Source MAC address	any
Source address	any
Source port	
Destination zone	● Device (input) ○ Any zone (forward) ○ lan: lan: ○ newzone: (empty) ○ wan: wan:
Destination address	any
Destination port	
Action	accept
Extra arguments	Passes additional arguments to iptables. Use with care!

Name: corresponds to add your name, such as aa.

Restrict to address family: IPv4 and IPv6, only IPv4, only IPv6, any for you to choose, according to the traffic rules you want to add to choose.

Protocol: Select the protocol based on your intranet server.

Match ICMP type: You can select the type of ICMP packet, if you are unsure type, you can choose "any"

Source zone: You can select lan, wan or all areas.

Source MAC address: Here you can customize the source MAC address.

Source address: Here you can customize the source IP address.

Source Port: Port of services provided by the source server is used.

Destination Zone: You can select lan, wan or all areas.

Destination address: You can customize the destination IP address here.

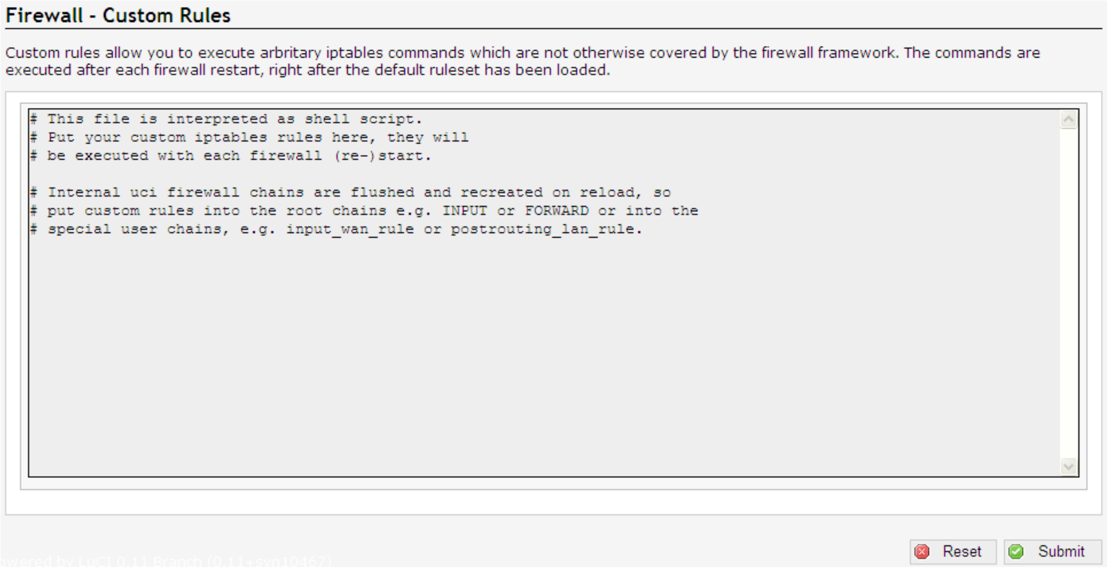
Destination port: Enter the port services provided by the target server being used.

Action: You can choose to discard , accept, reject , or no action .

Extra arguments: Additional parameters passed to iptables, careful to use!

4.4.7.4 Custom Rules

Click on the "Network>Firewall>Custom Rules" option, you can see the following interface.



Firewall - Custom Rules

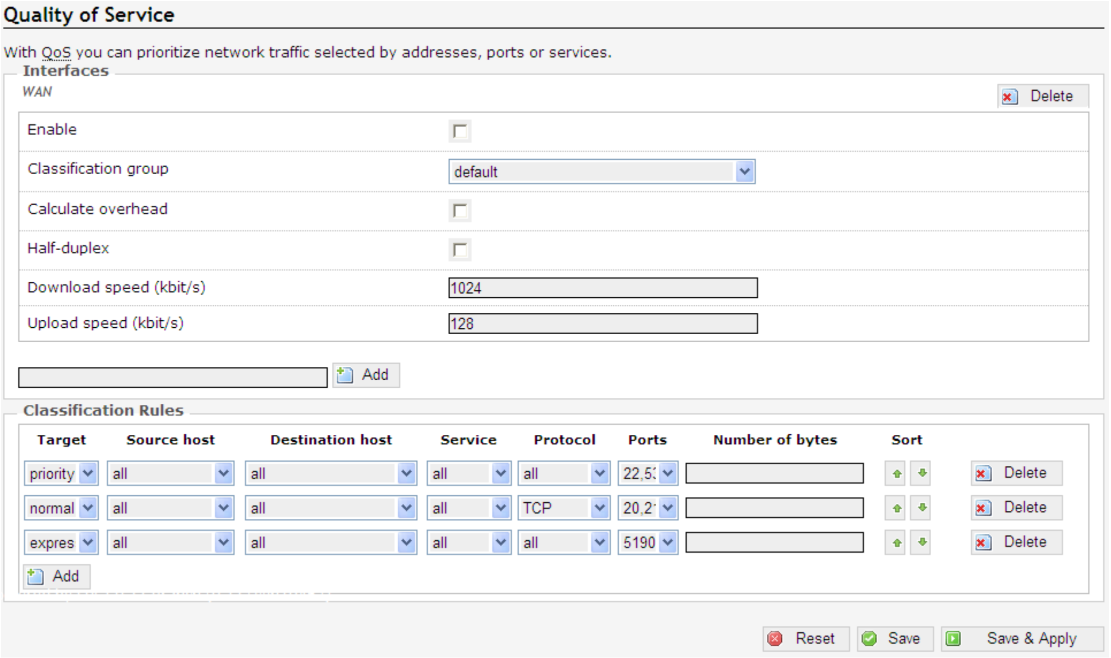
Custom rules allow you to execute arbritary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

In this interface you can define some functions not included in the firewall so that the AP can play against the computer maximum protection.

4.4.8 QoS

Click on the "Network>QoS" option, you can see the following interface.



Quality of Service

With QoS you can prioritize network traffic selected by addresses, ports or services.

Interfaces

WAN

Enable	□
Classification group	default
Calculate overhead	□
Half-duplex	□
Download speed (kbit/s)	1024
Upload speed (kbit/s)	128

Classification Rules

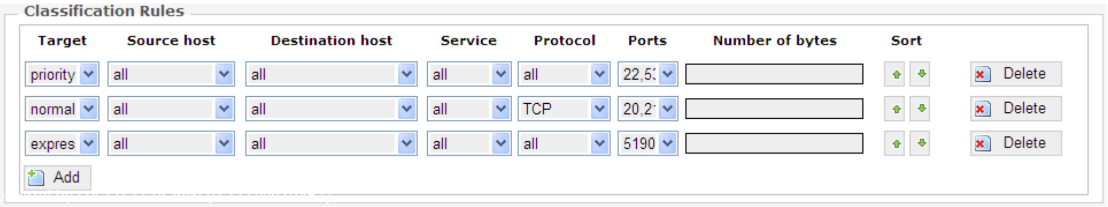
Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Sort
priority	all	all	all	all	22,5		
normal	all	all	all	TCP	20,2		
expres	all	all	all	all	5190		

Download speed/Upload speed: To modify according to their actual broadband.

Classification Rules: Here the program allows you to specify the port column graded, according to the rules of what you want to do.

Example: You want to play the game, you want the port at the most laid-back, to prevent gaming card machine dropped. Game port: 12701, then do the following.

Click the "Add" button, make the following configuration, the configuration is completed, click "Save&Apply" button.



Classification Rules

Target	Source host	Destination host	Service	Protocol	Ports	Number of bytes	Sort	
priority	all	all	all	all	22,5:			Delete
normal	all	all	all	TCP	20,2			Delete
expres	all	all	all	all	5190			Delete

Target: There are the "priority", "express", "normal", "low" four options to choose from. In this example select "priority".

Source host: Fill the local IP address.

Destination host: Fill the destination IP to be controlled.

Service: Choose one of your own network.

Protocol: Protocol used by the service provided by the server. If not clear what kind of agreement, you can choose "TCP+UDP" protocol.

Ports: Port services provided by the server within the network used. In this example 12701.

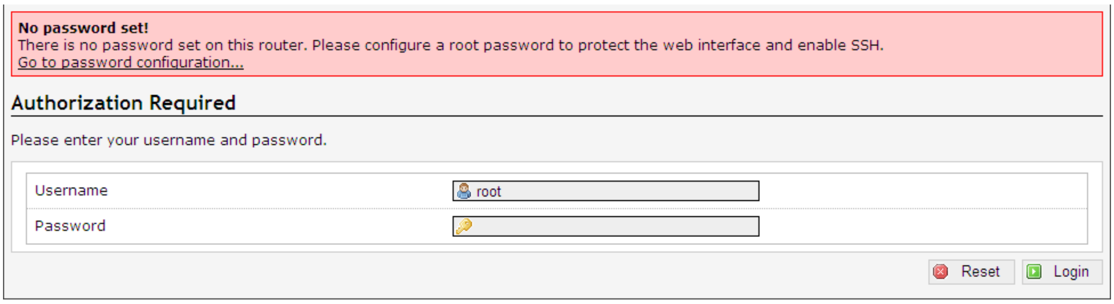
Number of bytes: That is the amount of how many bytes of data through your AP has.

Sort: If you add two more goals, you can press this button to select their order.

Note: Be sure to fill out the total bandwidth of the actual bandwidth carriers, the only way to be precise limit network speed.

4.5 Logout

Click the “Logout”, you can exit the Web management interface, back to the landing interface.



No password set!
There is no password set on this router. Please configure a root password to protect the web interface and enable SSH.
Go to password configuration...

Authorization Required

Please enter your username and password.

Username	root
Password	

4.6 FCC Statement

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

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

FCC Radiation Exposure Statement

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

Federal Communications Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environ ment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, hum an proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.