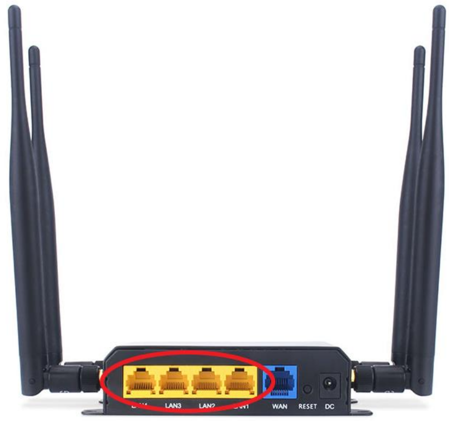
FE-W826-WD

User Manual

Table of content

1. Connecting the device

Carefully unpack the device. Plug in one side of the included Ethernet cable into one of the LAN Ports on the back side of the device, as shown in the picture below (LAN Ports circled in red).



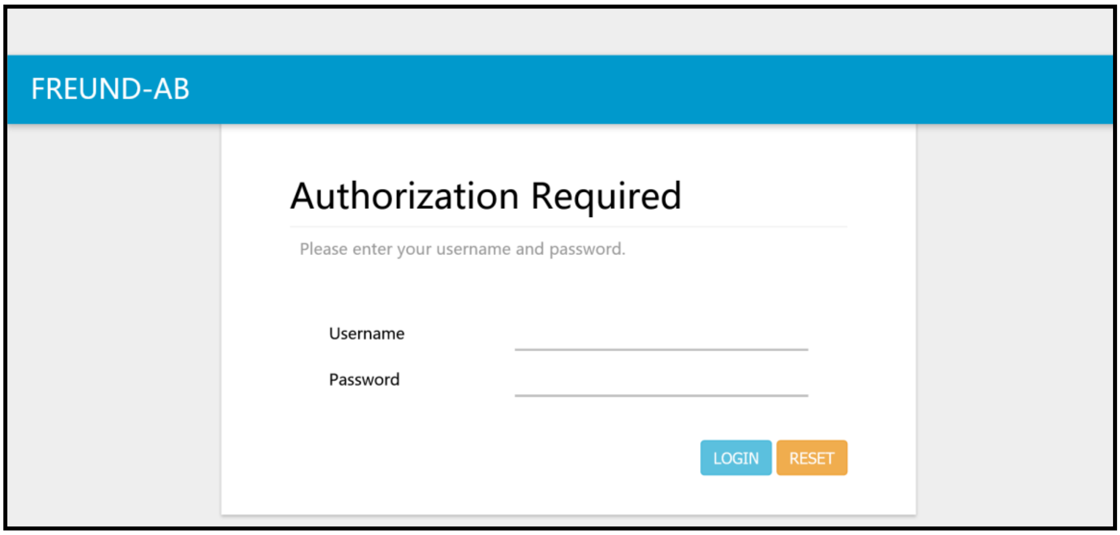
Connect the other end of the Ethernet cable into the Ethernet port of the Computer you are using to set up the device.

2. Authorization and Login page

In order to access the FE-W826-WD 4G router and configure it, you first need to open your web browser and type the default management address: **‘192.168.1.1’.**

If another device exists on the same network with the same IP address, the default management address will be automatically changed to ‘192.168.**2**.1’ and so on.

A following screen will be displayed:

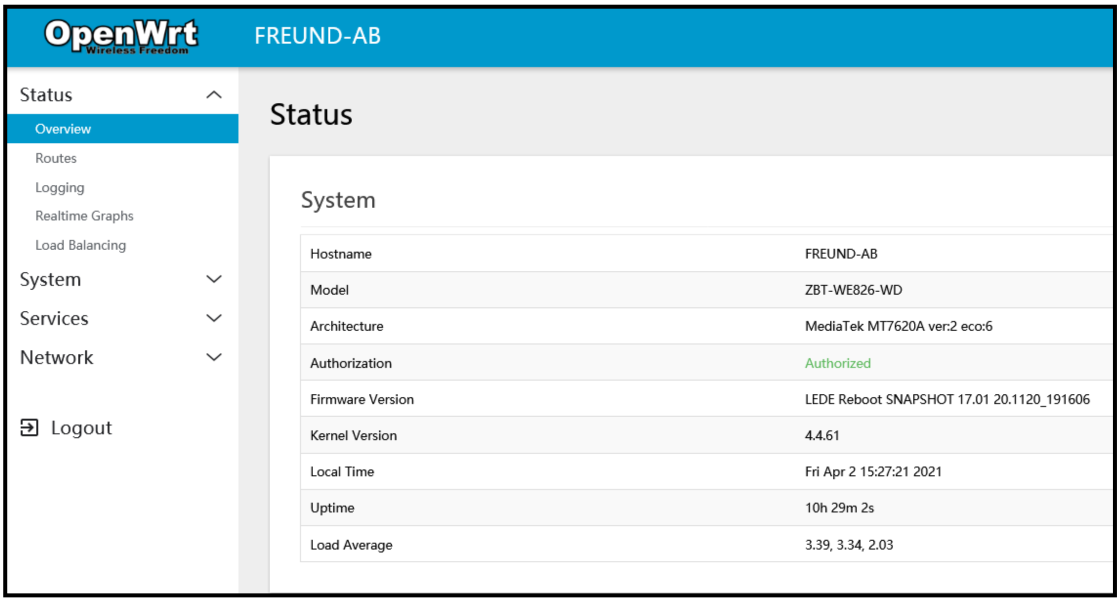


Authorization Required

Please enter your username and password.

The default username is ‘root’ and default password is ‘admin’.

After successfully typing in the credentials and clicking ‘**LOGIN’**, following screen will be shown.



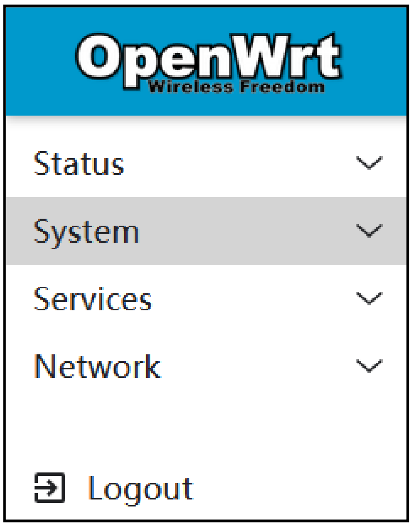
Status

System

Hostname	FREUND-AB
Model	ZBT-WE826-WD
Architecture	MediaTek MT7620A ver:2 eco:6
Authorization	Authorized
Firmware Version	LEDE Reboot SNAPSHOT 17.01 20.1120_191606
Kernel Version	4.4.61
Local Time	Fri Apr 2 15:27:21 2021
Uptime	10h 29m 2s
Load Average	3.39, 3.34, 2.03

3. Interface

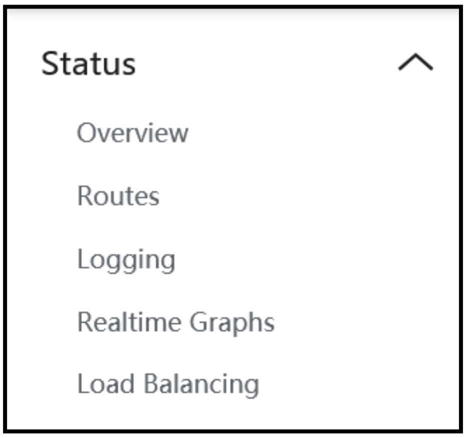
After successful login to device, on the left side of the interface we can see the menu that includes:



Status, System, Services, Network, Logout

3.1 Status

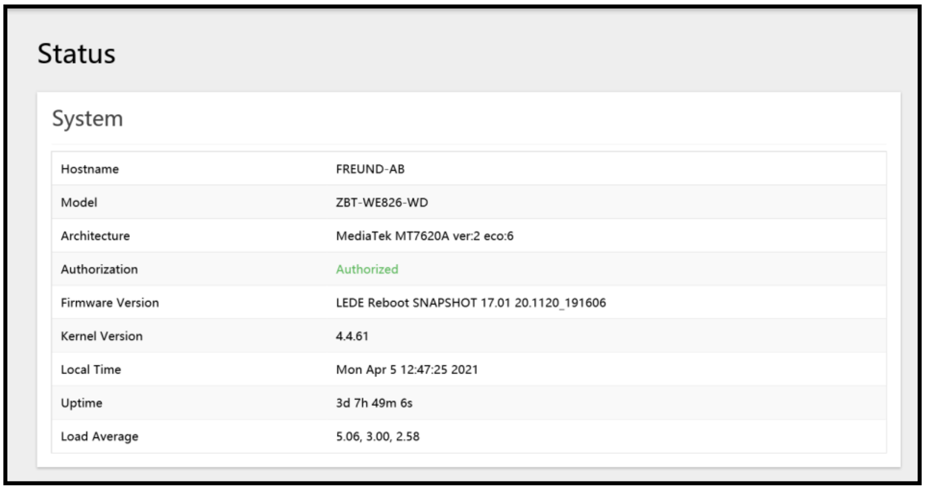
If we click on **Status**, we can see submenu containing:



Overview, Routes, Logging, Realtime Graphs, Load Balancing

3.1.1 Overview

Under **Overview** submenu, following information can be found: Hostname, Firmware version, Kernel Version, Local time, Uptime, and Average Load.



Status

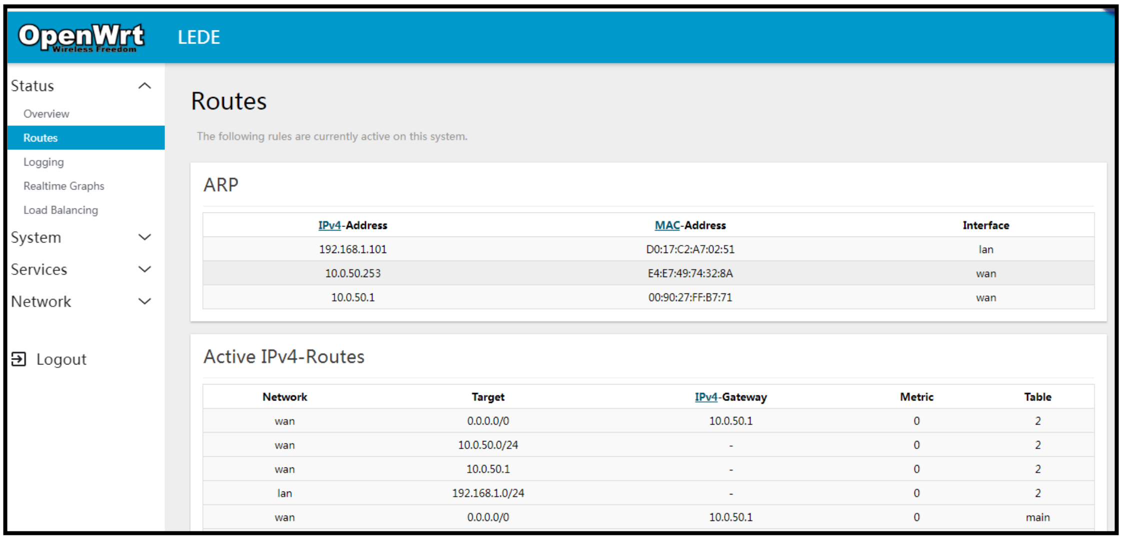
System

Hostname	FREUND-AB
Model	ZBT-WE826-WD
Architecture	MediaTek MT7620A ver:2 eco:6
Authorization	Authorized
Firmware Version	LEDE Reboot SNAPSHOT 17.01 20.1120_191606
Kernel Version	4.4.61
Local Time	Mon Apr 5 12:47:25 2021
Uptime	3d 7h 49m 6s
Load Average	5.06, 3.00, 2.58

Overview

3.1.2 Routes

Under **Routes** submenu, we can see information about Active IPv4 and IPv6 Routes.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.168.1.101	D0:17:C2:A7:02:51	lan
10.0.50.253	E4:E7:49:74:32:8A	wan
10.0.50.1	00:90:27:FF:B7:71	wan

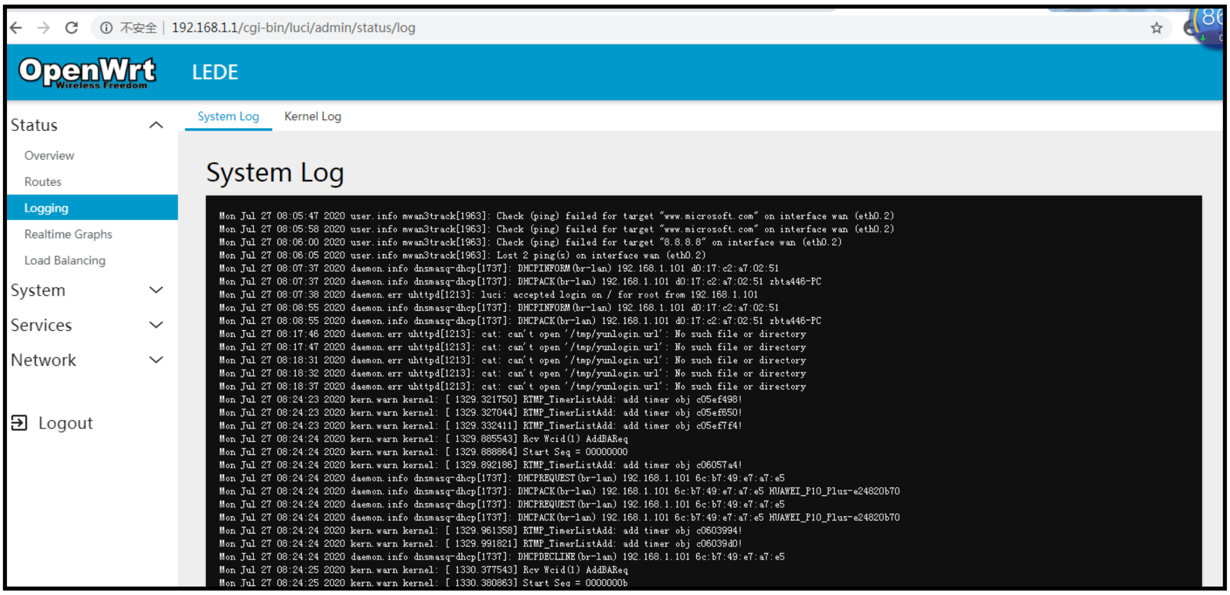
Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	10.0.50.1	0	2
wan	10.0.50.0/24	-	0	2
wan	10.0.50.1	-	0	2
lan	192.168.1.0/24	-	0	2
wan	0.0.0.0/0	10.0.50.1	0	main

Routes

3.1.3 Logging

Under **Logging** submenu, we can see two additional submenus: System Log and Kernel Log.



System Log

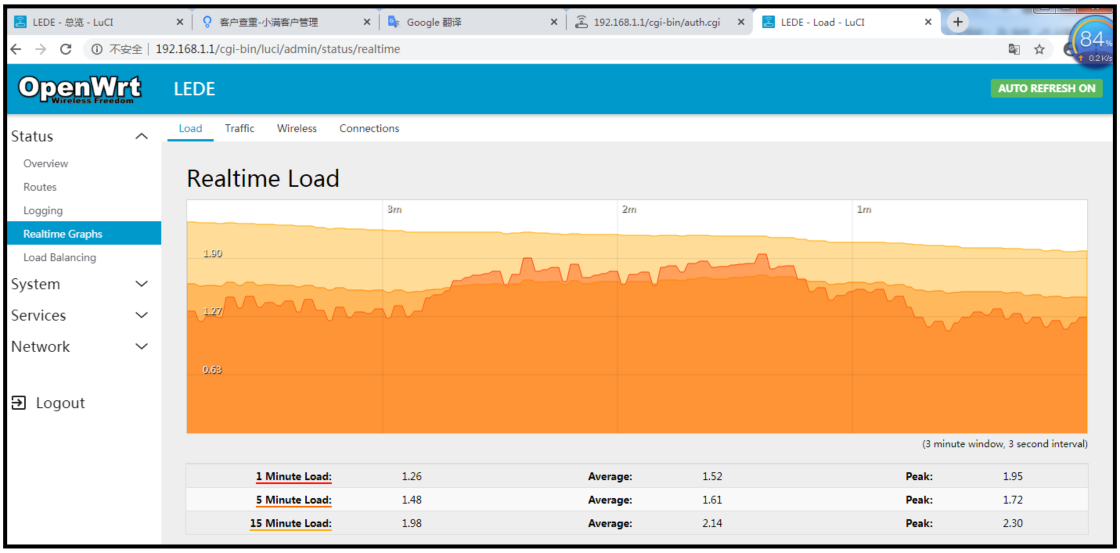
```
Mon Jul 27 08:05:47 2020 user.info mwan3track[1963]: Check (ping) failed for target "www.microsoft.com" on interface wan (eth0.2)
Mon Jul 27 08:05:58 2020 user.info mwan3track[1963]: Check (ping) failed for target "www.microsoft.com" on interface wan (eth0.2)
Mon Jul 27 08:06:00 2020 user.info mwan3track[1963]: Check (ping) failed for target "8.8.8.8" on interface wan (eth0.2)
Mon Jul 27 08:06:05 2020 user.info mwan3track[1963]: Lost 2 ping(s) on interface wan (eth0.2)
Mon Jul 27 08:07:37 2020 daemon.info dnsmasq-dhcp[1737]: DHCPINFORM(br-lan) 192.168.1.101 d0:17:c2:a7:02:51
Mon Jul 27 08:07:37 2020 daemon.info dnsmasq-dhcp[1737]: DHCPACK(br-lan) 192.168.1.101 d0:17:c2:a7:02:51 zbta446-PC
Mon Jul 27 08:07:38 2020 daemon.err uhttpd[1213]: luci: accepted login on / for root from 192.168.1.101
Mon Jul 27 08:08:55 2020 daemon.info dnsmasq-dhcp[1737]: DHCPINFORM(br-lan) 192.168.1.101 d0:17:c2:a7:02:51
Mon Jul 27 08:08:55 2020 daemon.info dnsmasq-dhcp[1737]: DHCPACK(br-lan) 192.168.1.101 d0:17:c2:a7:02:51 zbta446-PC
Mon Jul 27 08:17:46 2020 daemon.err uhttpd[1213]: cat: can't open '/tmp/yunlogin.url': No such file or directory
Mon Jul 27 08:17:47 2020 daemon.err uhttpd[1213]: cat: can't open '/tmp/yunlogin.url': No such file or directory
Mon Jul 27 08:18:31 2020 daemon.err uhttpd[1213]: cat: can't open '/tmp/yunlogin.url': No such file or directory
Mon Jul 27 08:18:32 2020 daemon.err uhttpd[1213]: cat: can't open '/tmp/yunlogin.url': No such file or directory
Mon Jul 27 08:18:37 2020 daemon.err uhttpd[1213]: cat: can't open '/tmp/yunlogin.url': No such file or directory
Mon Jul 27 08:24:23 2020 kern.warn kernel: [ 1329.321750] RTMP_TimerListAdd: add timer obj c05ef498!
Mon Jul 27 08:24:23 2020 kern.warn kernel: [ 1329.327044] RTMP_TimerListAdd: add timer obj c05ef650!
Mon Jul 27 08:24:23 2020 kern.warn kernel: [ 1329.332411] RTMP_TimerListAdd: add timer obj c05ef7f4!
Mon Jul 27 08:24:24 2020 kern.warn kernel: [ 1329.885543] Rcv Wcid(1) AddBAReq
Mon Jul 27 08:24:24 2020 kern.warn kernel: [ 1329.888864] Start Seq = 00000000
Mon Jul 27 08:24:24 2020 kern.warn kernel: [ 1329.892186] RTMP_TimerListAdd: add timer obj c06057a4!
Mon Jul 27 08:24:24 2020 daemon.info dnsmasq-dhcp[1737]: DHCPREQUEST(br-lan) 192.168.1.101 6c:b7:49:e7:a7:e5
Mon Jul 27 08:24:24 2020 daemon.info dnsmasq-dhcp[1737]: DHCPACK(br-lan) 192.168.1.101 6c:b7:49:e7:a7:e5 HUAWEI_P10_Plus-e24820b70
Mon Jul 27 08:24:24 2020 daemon.info dnsmasq-dhcp[1737]: DHCPREQUEST(br-lan) 192.168.1.101 6c:b7:49:e7:a7:e5
Mon Jul 27 08:24:24 2020 daemon.info dnsmasq-dhcp[1737]: DHCPACK(br-lan) 192.168.1.101 6c:b7:49:e7:a7:e5 HUAWEI_P10_Plus-e24820b70
Mon Jul 27 08:24:24 2020 kern.warn kernel: [ 1329.961358] RTMP_TimerListAdd: add timer obj c0603994!
Mon Jul 27 08:24:24 2020 kern.warn kernel: [ 1329.991821] RTMP_TimerListAdd: add timer obj c06039d0!
Mon Jul 27 08:24:24 2020 daemon.info dnsmasq-dhcp[1737]: DHCPDECLINE(br-lan) 192.168.1.101 6c:b7:49:e7:a7:e5
Mon Jul 27 08:24:25 2020 kern.warn kernel: [ 1330.377543] Rcv Wcid(1) AddBAReq
Mon Jul 27 08:24:25 2020 kern.warn kernel: [ 1330.380863] Start Seq = 0000000b
```

System Log

3.1.4 Realtime Graphs

Under **Realtime Graphs**, we can see Load as well as Traffic, Wireless and Connections submenus.

- **Load** submenu gives information about Peak and Average load in 1 minute, 5 minute and 15 minute load(and 3 minute window Graph with 3 seconds interval).
- **Traffic** shows Realtime Traffic for every specific ethernet port as well as WAN. It shows inbound and outbound traffic speed(and 3 minute window Graph with 3 seconds interval).
- **Realtime Wireless** shows information about Signal and Noise, with Peak and Average information as well as physical layer rate.



Realtime Load

(3 minute window, 3 second interval)

1 Minute Load:	1.26	Average:	1.52	Peak:	1.95
5 Minute Load:	1.48	Average:	1.61	Peak:	1.72
15 Minute Load:	1.98	Average:	2.14	Peak:	2.30

Realtime Load (Load, Traffic, Wireless, and Connections)

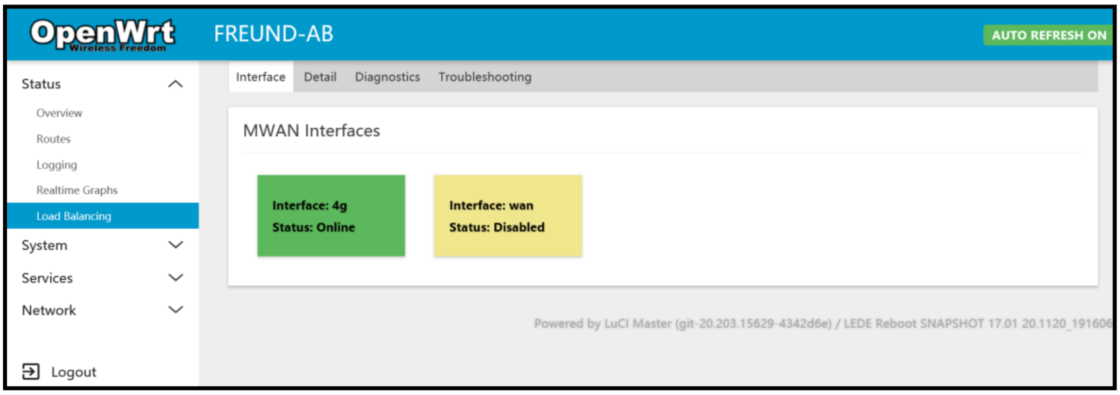
3.1.5 Load Balancing

Under Load Balancing submenu, we can see which interface is online (4G and WAN).

Clicking on Detail will show additional information (connected networks, active rules).

Diagnostics tab gives us several options:

- Ping default gateway
- Ping tracking IP
- Check IP rules
- Check routing table
- Hotplug



MWAN Interfaces

Interface: 4g
Status: Online

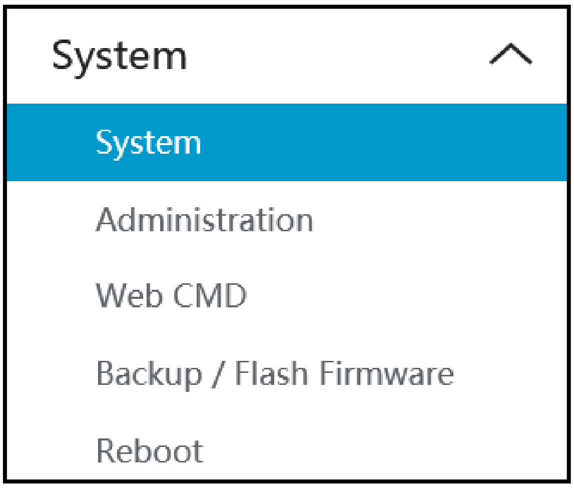
Interface: wan
Status: Disabled

Powered by LuCI Master (git-20.203.15629-4342d6e) / LEDE Reboot SNAPSHOT 17.01 20.1120_191606

Load Balancing (Interface, Detail, Diagnostics, Troubleshooting)

3.2 System

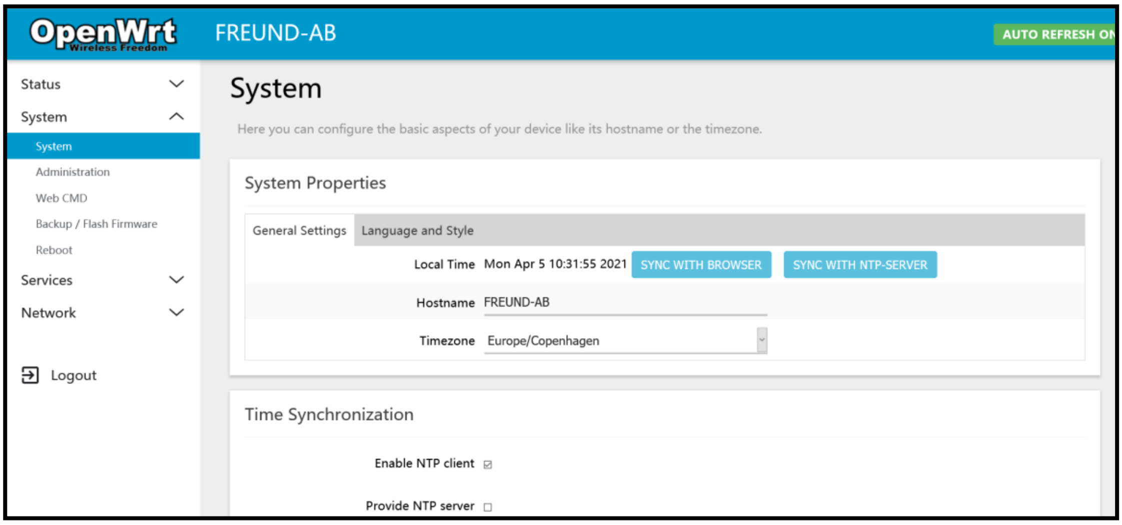
If we click on **System**, we can see submenu containing:



System, Administration, Web CMD, Backup/Flash Firmware, Reboot

3.2.1 System

System submenu offers options to change Time and Time Zone, Hostname, Language and Theme.



System

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

System Properties

Local Time Mon Apr 5 10:31:55 2021

Hostname FREUND-AB

Timezone Europe/Copenhagen

Time Synchronization

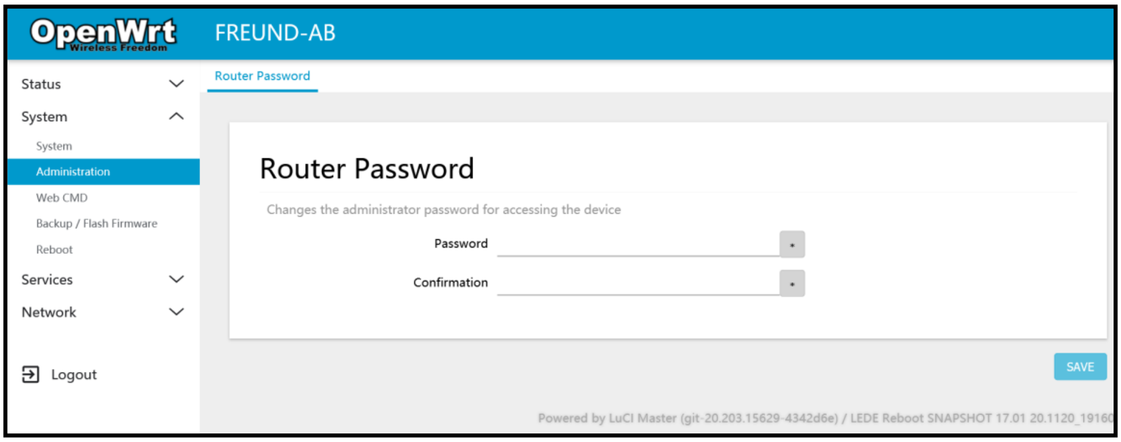
Enable NTP client ☑

Provide NTP server □

System (General settings, Language and Style)

3.2.2 Administration

Administration submenu allows us to change the password of the device.



Router Password

Changes the administrator password for accessing the device

Password

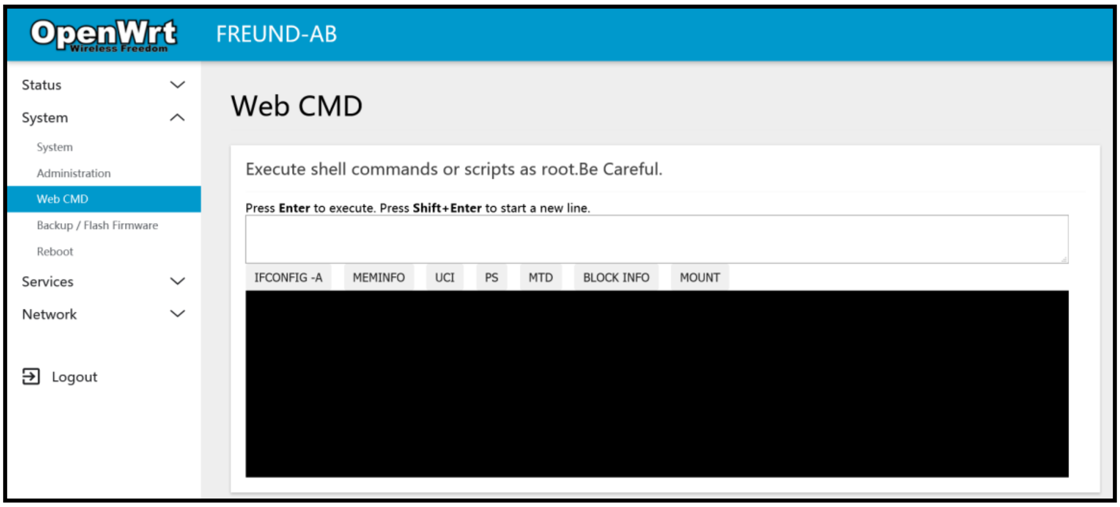
Confirmation

Powered by LuCI Master (git-20.203.15629-4342d6e) / LEDE Reboot SNAPSHOT 17.01 20.1120_19160

Administration

3.2.3 Web CMD

Web CMD submenu allows usage of the CMD by entering commands into the shell. Use with caution.



Web CMD

Execute shell commands or scripts as root.Be Careful.

Press **Enter** to execute. Press **Shift+Enter** to start a new line.

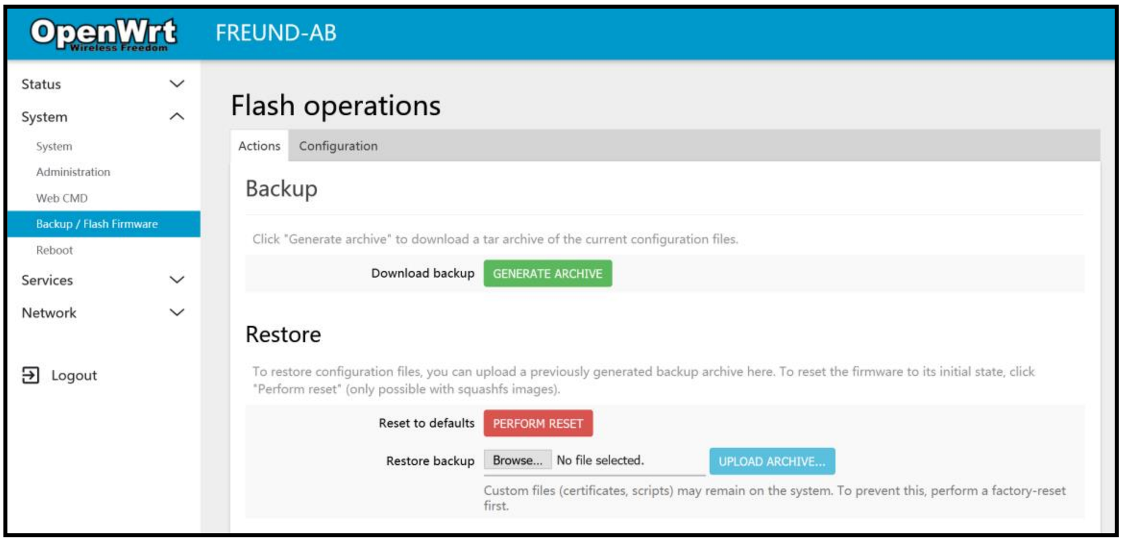
Web CMD

3.2.4 Backup / Flash Firmware

Under **Actions** tab, it allows backing up and download of the current config files as well as restoring backed up configuration.

It is also possible to upgrade the Firmware version of the device from the same tab. To do that, click Browse button and select file in File Browser. You can check the box ‘Keep settings’ if you want to retain the current configuration (compatible firmware image required).

Clicking on **Configuration** tab, backed up file list will be shown.



Flash operations

Backup

Click "Generate archive" to download a tar archive of the current configuration files.

Download backup

Restore

To restore configuration files, you can upload a previously generated backup archive here. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Reset to defaults

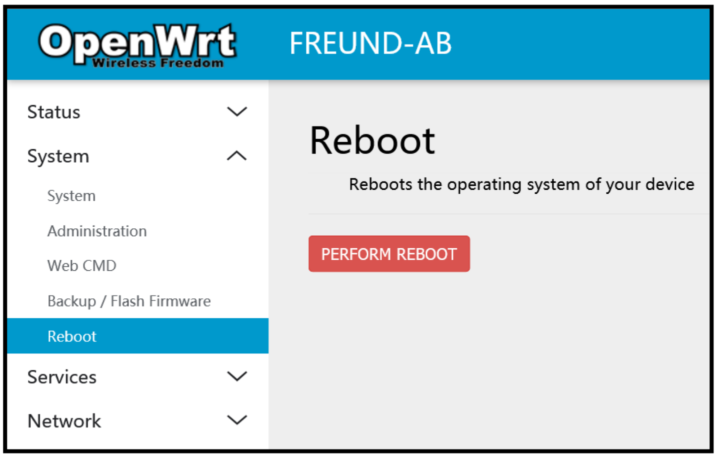
Restore backup No file selected.

Custom files (certificates, scripts) may remain on the system. To prevent this, perform a factory-reset first.

Backup / Flash Firmware(Actions, Configuration)

3.2.5 Reboot

Reboot submenu allows manual reboot of the device.



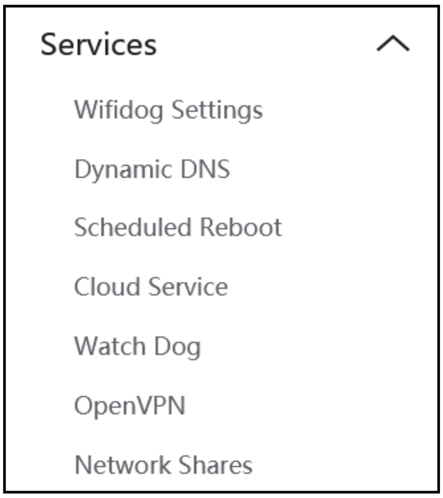
Reboot

Reboots the operating system of your device

Reboot

3.3 Services

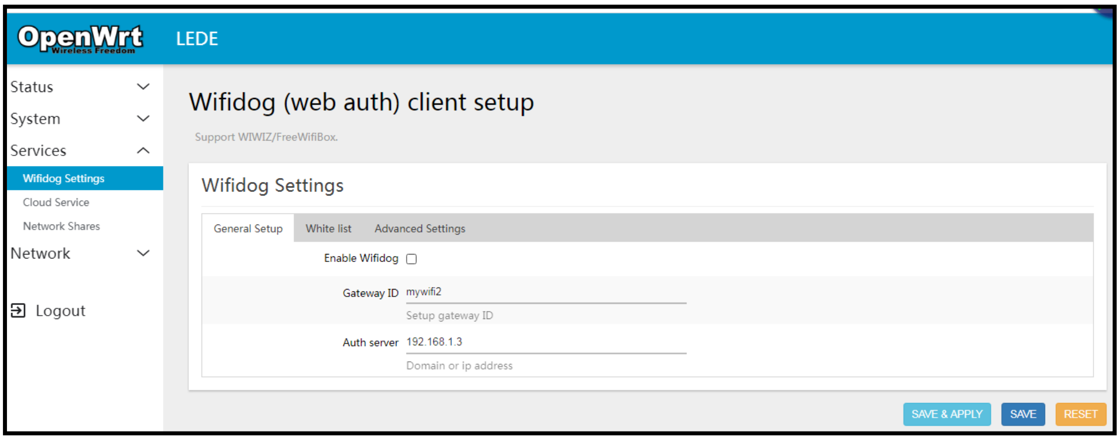
If we click on **Services**, we can see submenu containing:



Wifidog Settings, Dynamic DNS, Scheduled Reboot, Cloud Service, Watch Dog, OpenVPN, Network shares

3.3.1 WiFiDog

WiFiDog Settings submenu allows enabling the Wifidog, Setting up the gateway ID, Domain name or IP Address. Also, you can whitelist URL as well as MAC addresses, enable SSL certificates, Change the Ports used, etc.



Wifidog (web auth) client setup

Support WIWIZ/FreeWifiBox.

Wifidog Settings

Enable Wifidog ☐

Gateway ID mywifi2

Setup gateway ID

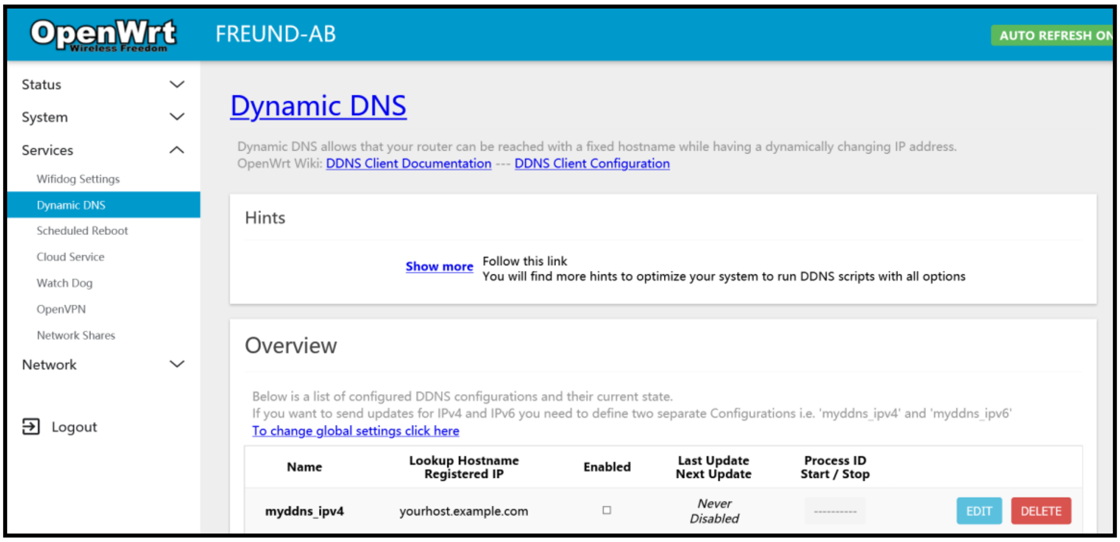
Auth server 192.168.1.3

Domain or ip address

WiFiDog Settings (General Setup, Whitelist, Advanced Settings)

3.3.2 Dynamic DNS

Dynamic DNS allows you to access your devices from the internet via a simple to remember domain name while still having a dynamically changing IP address.



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.
OpenWrt Wiki: DDNS Client Documentation --- DDNS Client Configuration

Hints

Show more Follow this link
You will find more hints to optimize your system to run DDNS scripts with all options

Overview

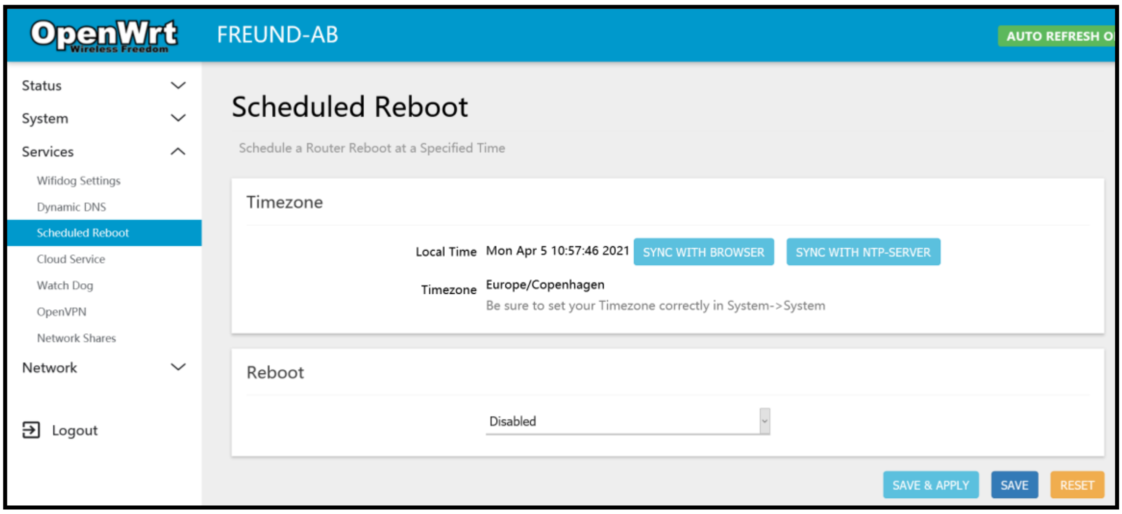
Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
To change global settings click here

Name	Lookup Hostname Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop
myddns_ipv4	yourhost.example.com	□	Never Disabled	----------

Dynamic DNS

3.3.3 Scheduled Reboot

Allows you to enable **Scheduled Reboot** and set up Reboot time.



Scheduled Reboot

Schedule a Router Reboot at a Specified Time

Timezone

Local Time Mon Apr 5 10:57:46 2021

Timezone Europe/Copenhagen
Be sure to set your Timezone correctly in System->System

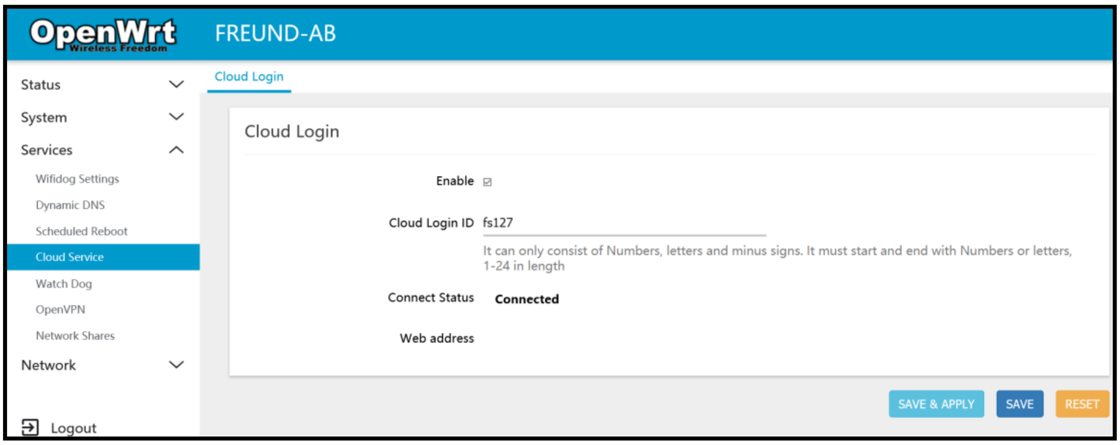
Reboot

Disabled

Scheduled Reboot

3.3.4 Cloud Service

It is possible to log in to the device remotely. To turn it on, you need to click on the Services button, and then Cloud Service. Following screen will show.



Cloud Login

Enable ☑

Cloud Login ID fs127

It can only consist of Numbers, letters and minus signs. It must start and end with Numbers or letters, 1-24 in length

Connect Status **Connected**

Web address

Cloud Service

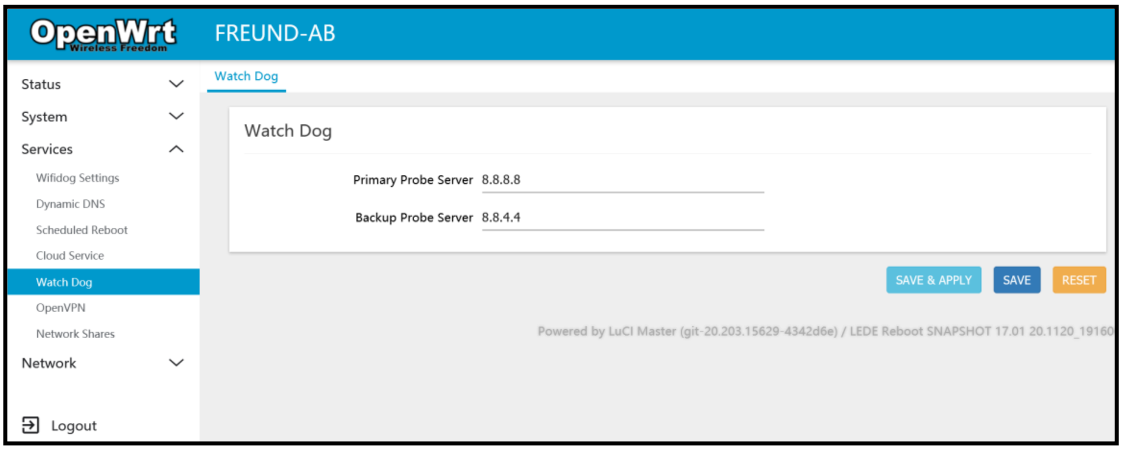
Tick the box ‘Enable’ and create your own Login ID.

The login ID can only consist of numbers, letters, and minus signs. It must start and end with numbers or letters, 1-24 characters in length.

3.3.5 Watchdog

Under Watchdog submenu, you can select Primary and Backup DNS Server.

If the device lose connection to both servers, Watchdog will reset the device in attempt to restore the connection.



Watch Dog

Primary Probe Server 8.8.8.8

Backup Probe Server 8.8.4.4

Powered by LuCI Master (git-20.203.15629-4342d6e) / LEDE Reboot SNAPSHOT 17.01 20.1120_19160

Watchdog

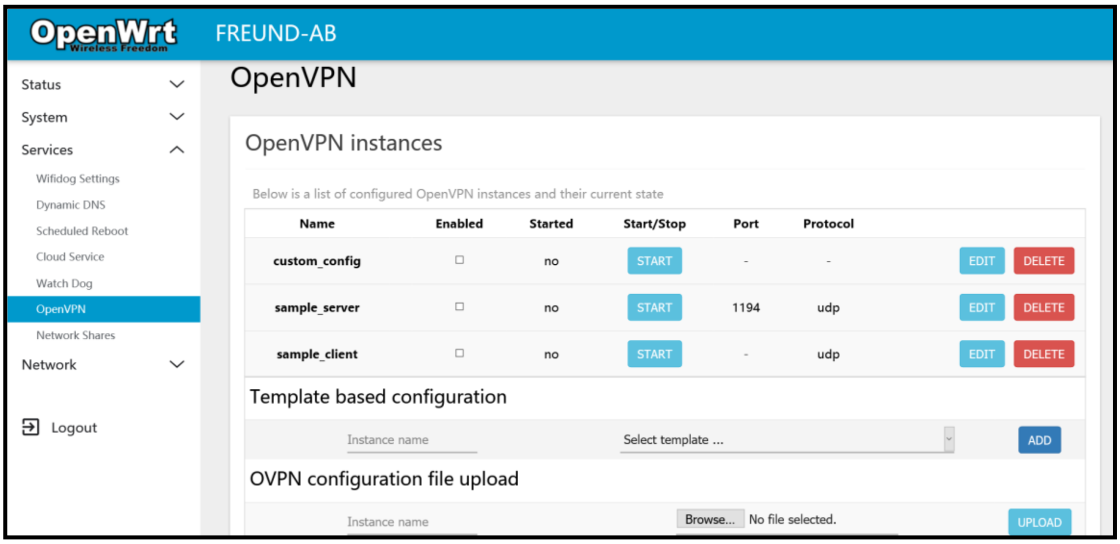
Watchdog **ON**	Primary Probe Server	8.8.8.8
	Backup Probe Server	8.8.4.4
Watchdog **OFF**	Primary Probe Server	127.0.0.1
	Backup Probe Server	192.168.1.1

To enable or disable Watchdog, enter the information above into the corresponding fields under Services – Watchdog submenu.

3.3.6 OpenVPN

Allows accessing the list of configured OpenVPN instances. Also allows configuration through a template.

You can upload an OpenVPN configuration file by clicking on the Browse button and selecting the wanted file in the File Browser and submit by clicking the Upload button.



OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Name	Enabled	Started	Start/Stop	Port	Protocol		
custom_config	☐	no	START	-	-	EDIT	DELETE
sample_server	☐	no	START	1194	udp	EDIT	DELETE
sample_client	☐	no	START	-	udp	EDIT	DELETE

Template based configuration

Instance name Select template ... ADD

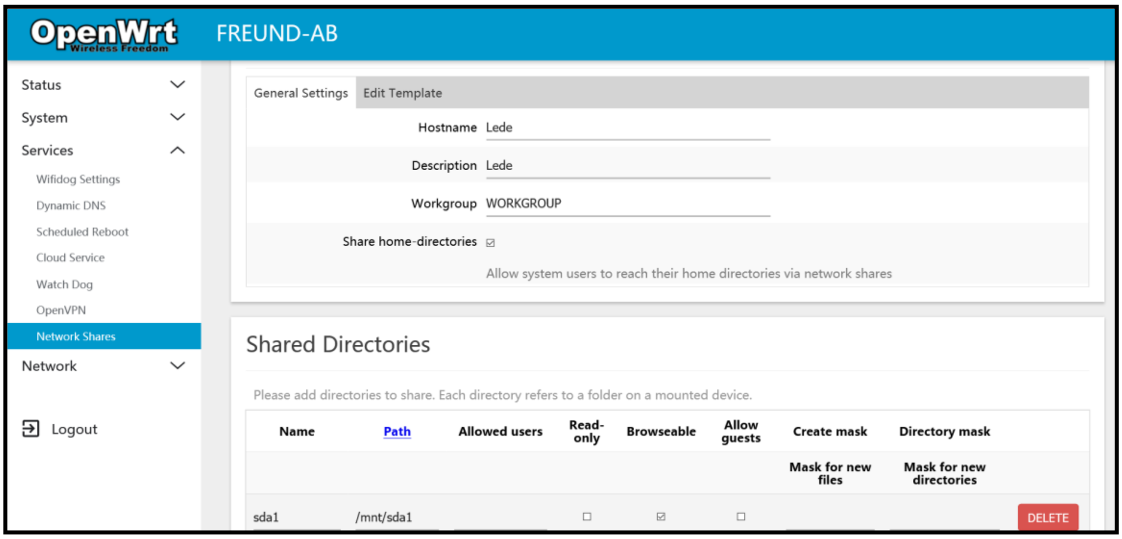
OVPN configuration file upload

Instance name Browse... No file selected. UPLOAD

OpenVPN

3.3.7 Network Sharing

Allows system users to reach their home directives via Network Sharing.



Hostname Lede

Description Lede

Workgroup WORKGROUP

Share home-directories ☑

Allow system users to reach their home directories via network shares

Shared Directories

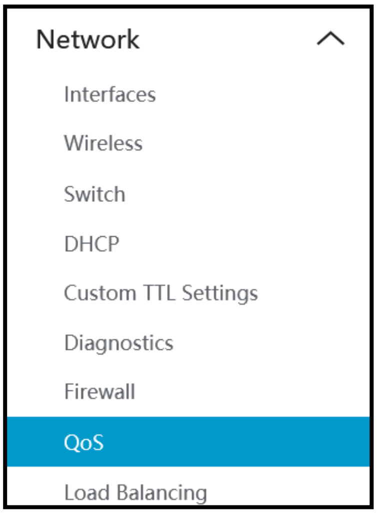
Please add directories to share. Each directory refers to a folder on a mounted device.

Name	Path	Allowed users	Read-only	Browseable	Allow guests	Create mask	Directory mask	
						Mask for new files	Mask for new directories	
sda1	/mnt/sda1		□	☑	□			DELETE

Network Shares

3.4 Network

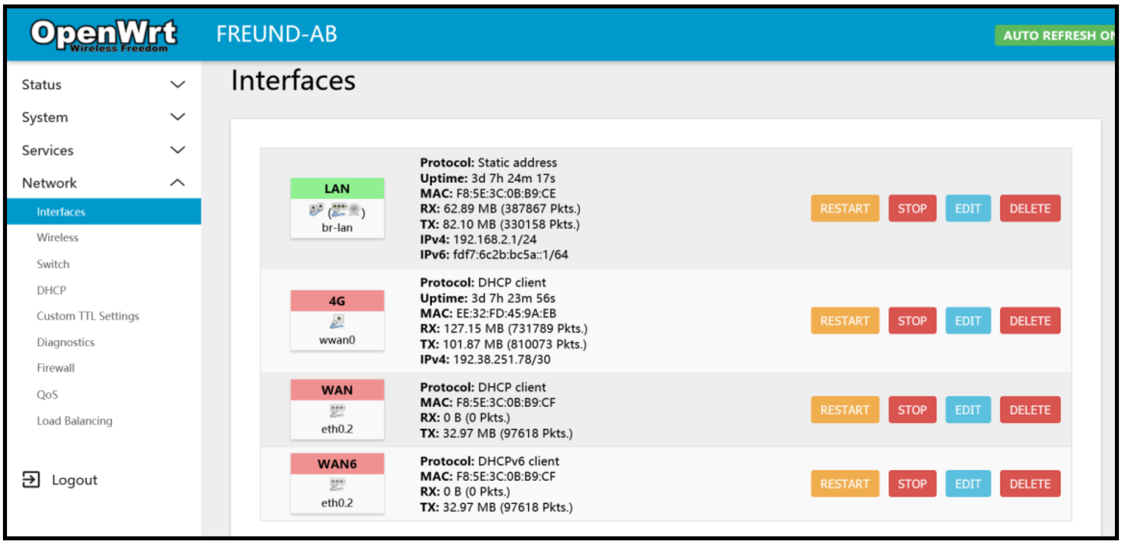
If we click on **Network**, we can see submenu containing:



Interfaces, Wireless, Switch, DHCP, Custom TTL, Diagnostics, Firewall, QoS, Load Balancing

3.4.1 Interfaces

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and entering the names of several network interfaces separated by spaces.



Interfaces

LAN
br-lan

Protocol: Static address
Uptime: 3d 7h 24m 17s
MAC: F8:5E:3C:0B:B9:CE
RX: 62.89 MB (387867 Pkts.)
TX: 82.10 MB (330158 Pkts.)
IPv4: 192.168.2.1/24
IPv6: fdf7:6c2b:bc5a::1/64

4G
wwan0

Protocol: DHCP client
Uptime: 3d 7h 23m 56s
MAC: EE:32:FD:45:9A:EB
RX: 127.15 MB (731789 Pkts.)
TX: 101.87 MB (810073 Pkts.)
IPv4: 192.38.251.78/30

WAN
eth0.2

Protocol: DHCP client
MAC: F8:5E:3C:0B:B9:CF
RX: 0 B (0 Pkts.)
TX: 32.97 MB (97618 Pkts.)

WAN6
eth0.2

Protocol: DHCPv6 client
MAC: F8:5E:3C:0B:B9:CF
RX: 0 B (0 Pkts.)
TX: 32.97 MB (97618 Pkts.)

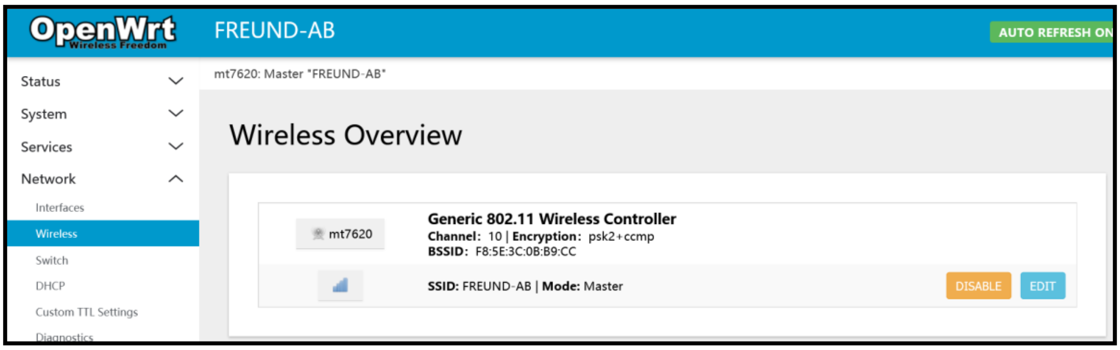
Interfaces

3.4.2 Wireless

Under Wireless, you have overview of your device Controller. Clicking on 'Edit' button, Device Configuration page will open.

The **Device Configuration** section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are 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.

You can also manage Security settings, such as encryption or cipher.



mt7620: Master "FREUND-AB"

Wireless Overview

mt7620

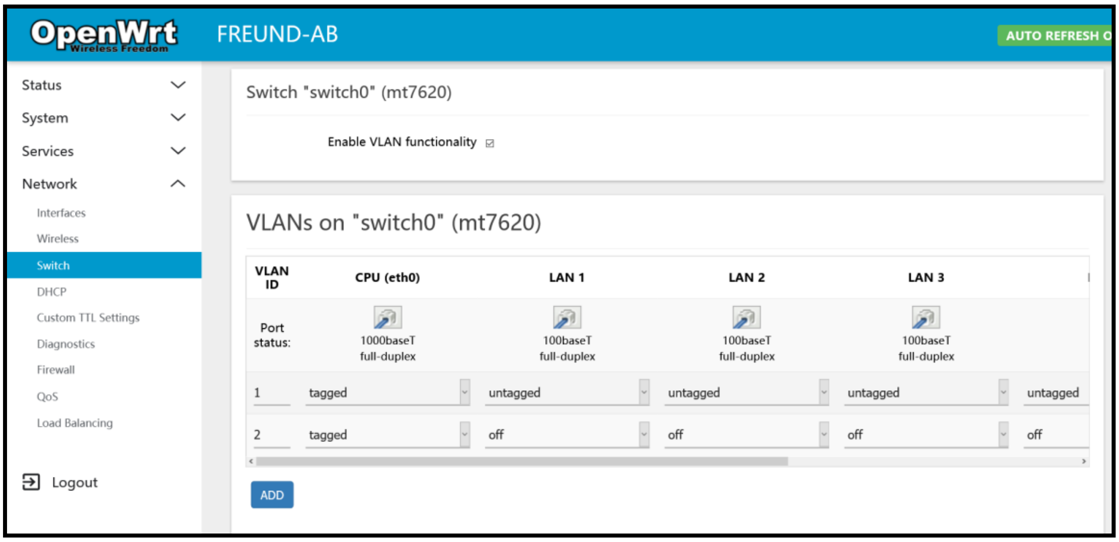
Generic 802.11 Wireless Controller
Channel: 10 | **Encryption:** psk2+ccmp
BSSID: F8:5E:3C:0B:B9:CC

SSID: FREUND-AB | **Mode:** Master

Wireless

3.4.3 Switch

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



Switch "switch0" (mt7620)

Enable VLAN functionality ☑

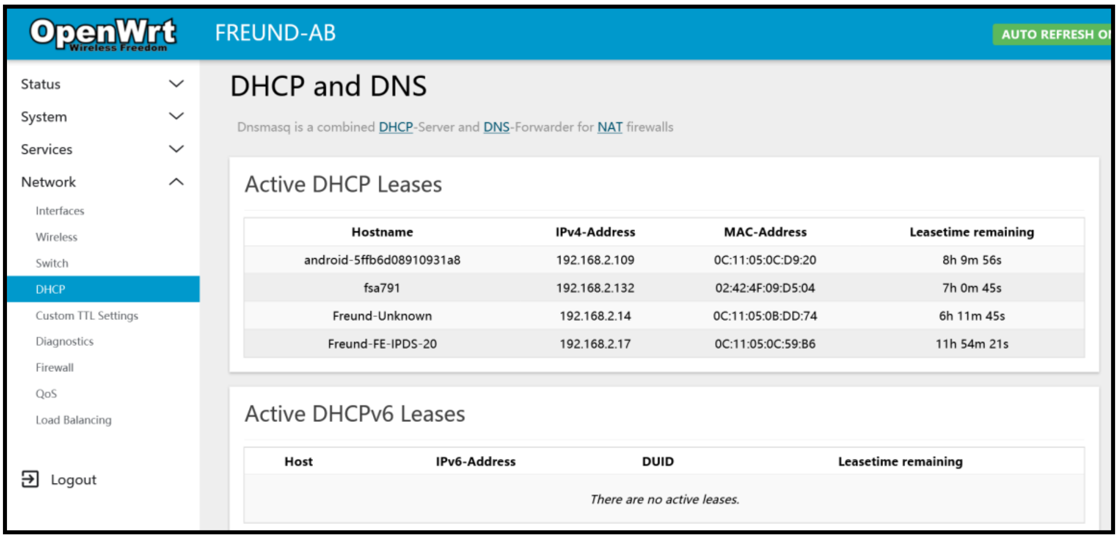
VLANs on "switch0" (mt7620)

VLAN ID	CPU (eth0)	LAN 1	LAN 2	LAN 3
Port status:	1000baseT full-duplex	100baseT full-duplex	100baseT full-duplex	100baseT full-duplex
1	tagged	untagged	untagged	untagged	untagged
2	tagged	off	off	off	off

Switch

3.4.4 DHCP

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



DHCP and DNS

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

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-5ffb6d08910931a8	192.168.2.109	0C:11:05:0C:D9:20	8h 9m 56s
fsa791	192.168.2.132	02:42:4F:09:D5:04	7h 0m 45s
Freund-Unknown	192.168.2.14	0C:11:05:0B:DD:74	6h 11m 45s
Freund-FE-IPDS-20	192.168.2.17	0C:11:05:0C:59:B6	11h 54m 21s

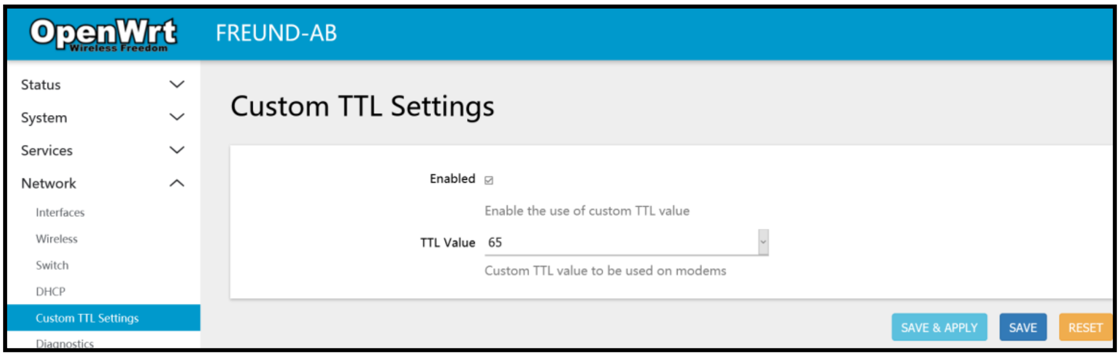
Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

DHCP and DNS

3.4.5 TTL Settings

Time to live (**TTL**) or **hop limit** is a mechanism which limits the lifespan or lifetime of data in a computer or network.



Custom TTL Settings

Enabled ☑

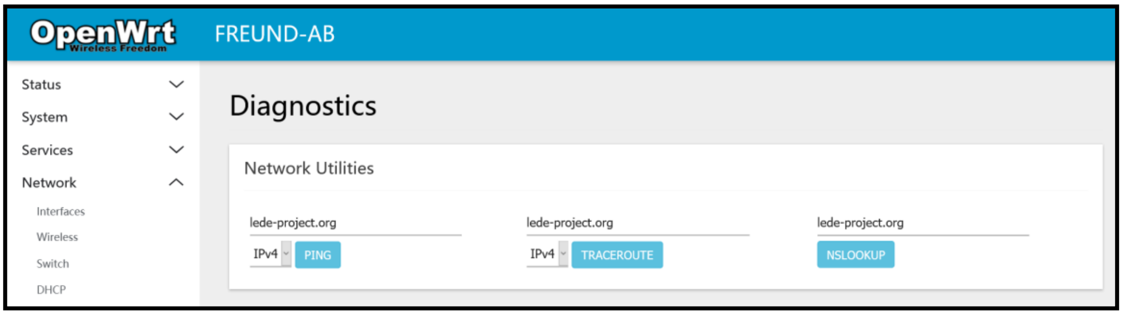
Enable the use of custom TTL value

TTL Value 65

Custom TTL value to be used on modems

Time-to-live Settings

3.4.6 Diagnostics



Diagnostics

Network Utilities

lede-project.org | lede-project.org | lede-project.org

Diagnostics

3.4.7 Firewall

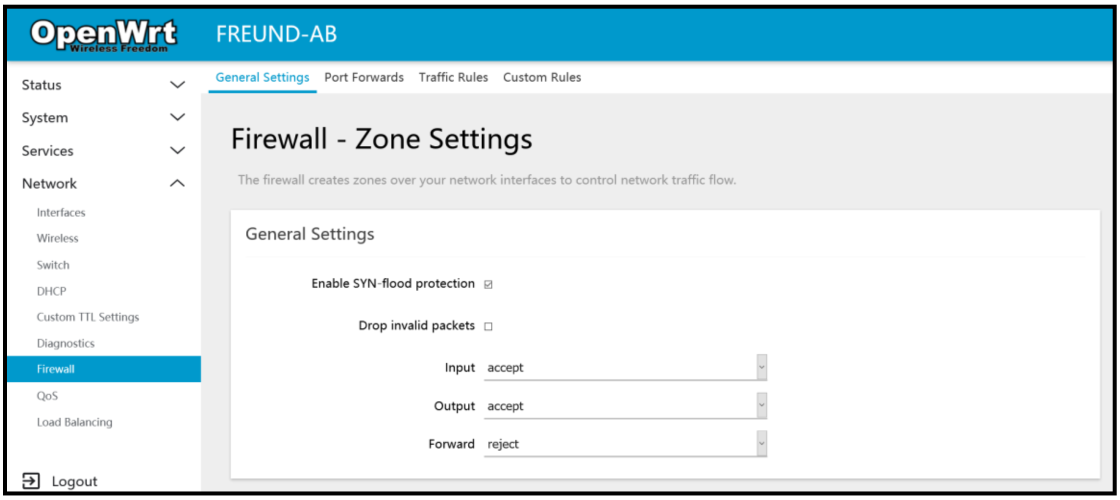
Under **Firewall** submenu, there are following tabs:

General Settings - The firewall creates zones over network interfaces to control network traffic flow.

Port Forwarding - Allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

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.

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



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

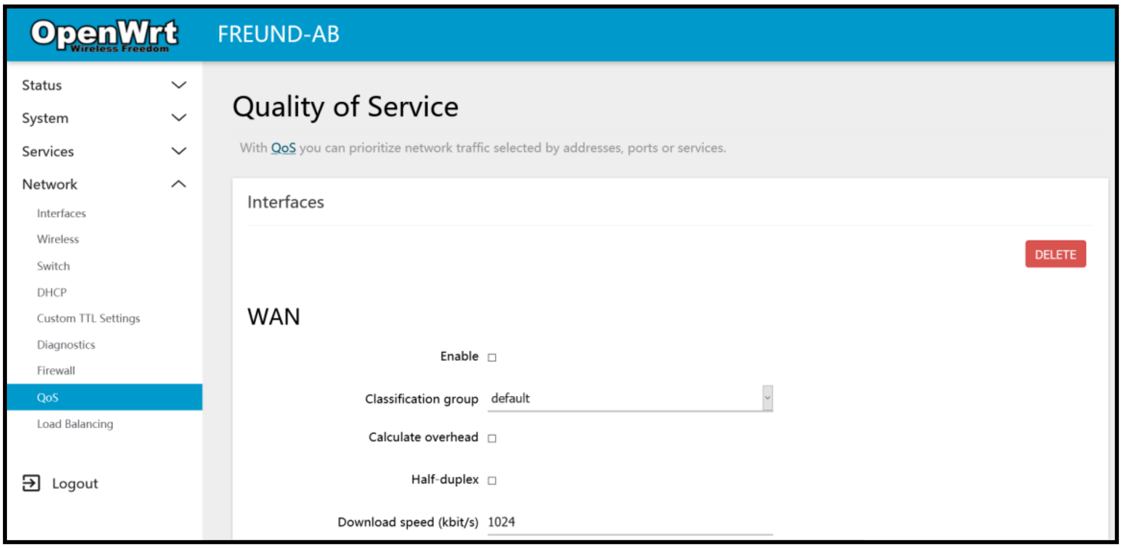
Output: accept

Forward: reject

Firewall

3.4.8 Quality of Service

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



Quality of Service

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

Interfaces

WAN

Enable □

Classification group: default

Calculate overhead □

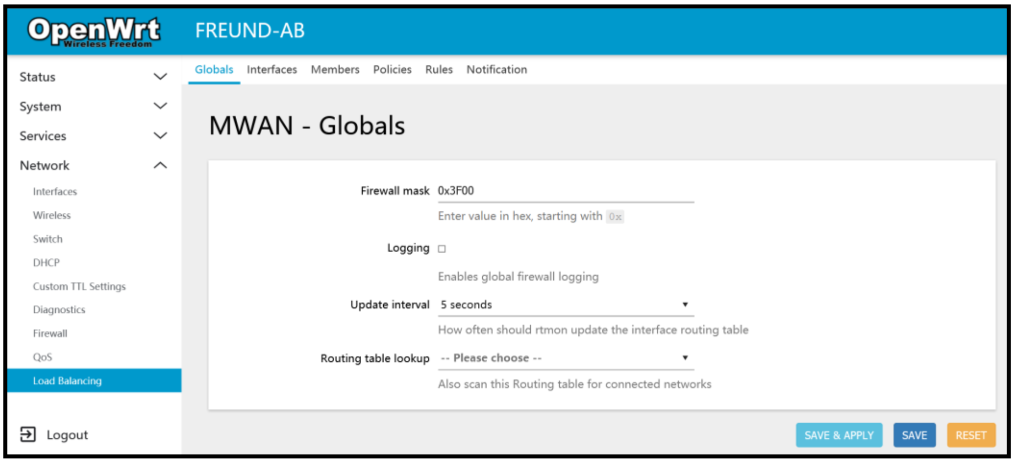
Half-duplex □

Download speed (kbit/s): 1024

Quality of Service

3.4.9 Load Balancing

With load balancing, traffic is distributed across a number of connections. Unlike bonding, these connections remain separate, and you do not need a hub in a Data Centre to bond these connections together.



MWAN - Globals

Firewall mask: 0x3F00

Enter value in hex, starting with 0x

Logging □

Enables global firewall logging

Update interval: 5 seconds

How often should rtmon update the interface routing table

Routing table lookup: -- Please choose --

Also scan this Routing table for connected networks

Load Balancing

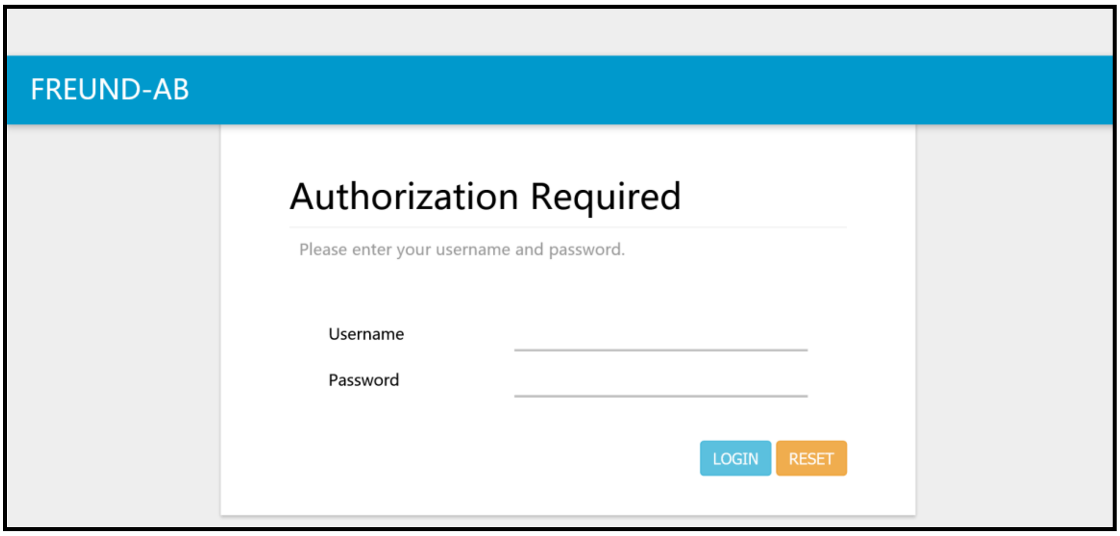
MWAN3 uses normal Linux policy routing to balance outgoing traffic over multiple WAN connections.

Linux outgoing network traffic load-balancing is performed on a per-IP connection basis – it is not channel-bonding, where a single connection (e.g. a single download) will use multiple WAN connections simultaneously.

As such load-balancing will help speed multiple separate downloads or traffic generated from a group of source PCs all accessing different sites but it will not speed up a single download from one PC (unless the download is spread across multiple IP streams such as by using a download manager).

3.5 Logout

After Clicking on Logout, you will be taken to the following Login Screen.



FREUND-AB

Authorization Required

Please enter your username and password.

Username

Password

Freund Elektronik A/S, in cooperation with our sister company Freund Elektronika D.O.O. Sarajevo, is developing an IP-Based Intercoms, Audio Systems, Access Control and Smart Home solutions.

As a developer, manufacturer, and reseller, we have been self-improving and perfecting ourselves for over 30 years.

In the industry, we negotiate the most advanced and innovative solutions regarding the building communication. Our daily focus is on the development and user friendliness of our high quality and pleasantly designed products.

As a developer and manufacturer of our own IP-INTEGRA system, we have made a top-of-the-line products for Door Telephony, Public Audio, and Access Control solution.

Our development department, together with our partners, has created elegant and robust door phones, SIP-Centrals, Terminals, IP-Speakers, ACC Controllers, and applications with intelligent features using the most advanced technologies when available, and creating new technologies when they are not while keeping it simple for our customers.