ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

APNUS031 How to Configure Cellular Router with Auto APN

July 2023

Content

1. Glossary

APN : Access Point Network
SIM: Subscriber Identify Module
MCC: Mobile Country Code
MNC: Mobile Network Code
PIN: Personal Identification Number
ICMP: Internet Control Management Protocol
DNS: Domain Name Service
DHCP: Dynamic Host Configuration Protocol
ISP: Internet Service Provider

2. Introduction

Auto APN allows to automatically configure the correct APN name based on the SIM card content.
Customers that need to deploy ACKSYS Cellular routers, don't need manual configuration to install need SIM cards with the Auto APN feature. This feature facilitates the installation of the product by non-technical users who might not be familiar with APN settings and lets very few parameters to configure before field deployment.

The aim of this application note is to configure a cellular router with AutoAPN capability and check if internet connectivity is then provided by the router for end devices.

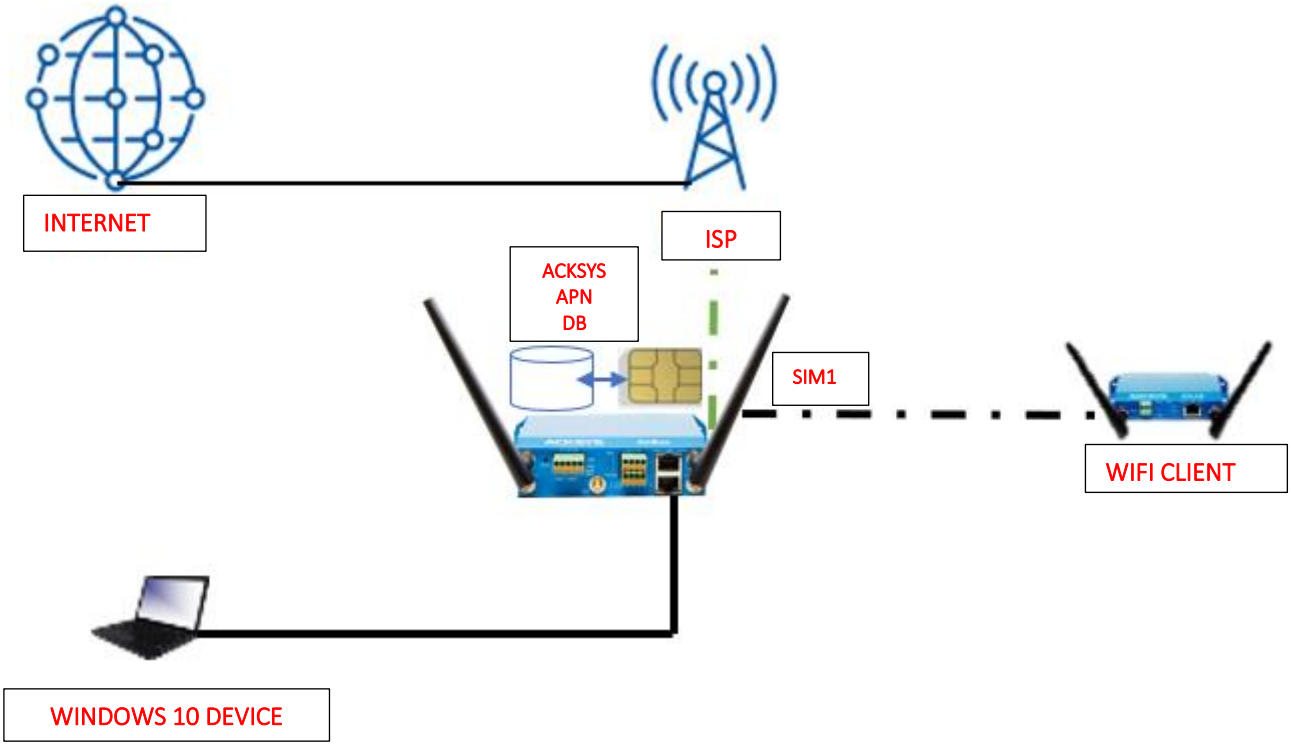
3. Installation Overview and Prerequesites

Before we begin, let's overview the configuration that we are attempting to achieve and the prerequisites that make it possible in this How-To note :

- One Cellular AirBox router or any type of Acksys Cellular Router
- WaveOs at least in release 4.22.0.1
- A valid SIM card from a known ISP
- Any devices connected in Wired or Wireless to test internet access
- Laptop to configure the router

4. Auto APN Configuration architecture

In this How-To, we will explain in detail how the APN is autoconfigured based on MCC and MCN information in the SIM card instead of manual configuration and the remaining configurations to allow the end devices to get internet access.



5. Acksys Router Configuration

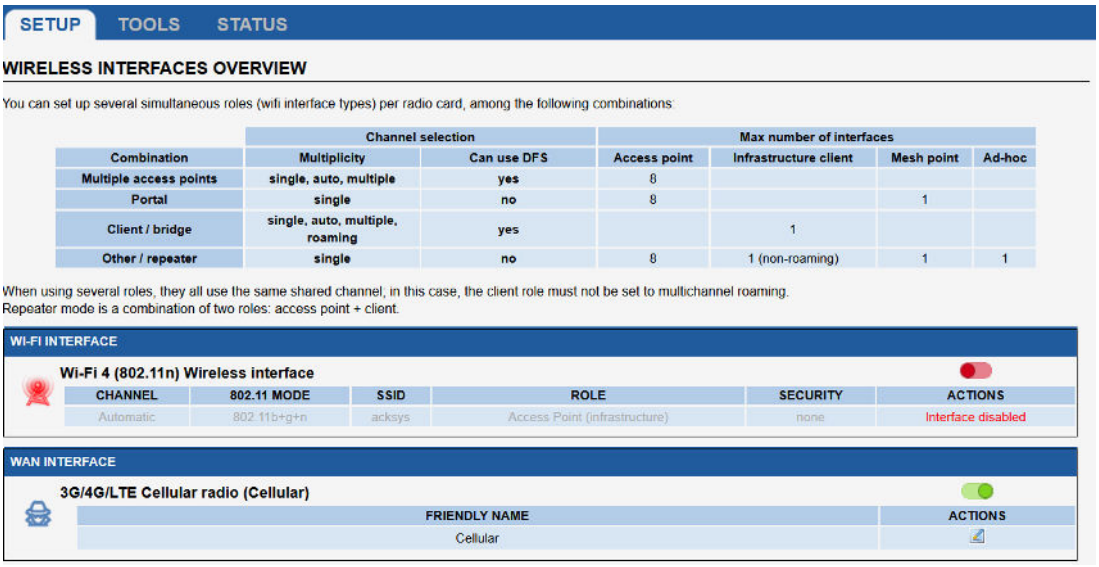
WaveOs release 4.22.0.1 comes with lot of keys features but only the Auto APN will be described here and the Password policy described in ANNEX.

Configuration WAN Interface

Note: the Cellular Interface is enabled by default, so we recommend you to configure the PINCODE before installing the simcard in the router to avoid simcard pinlock. If your simcard support multiple pincode retry, inserting the simcard before configuring the pincode, may consume one of the retry.

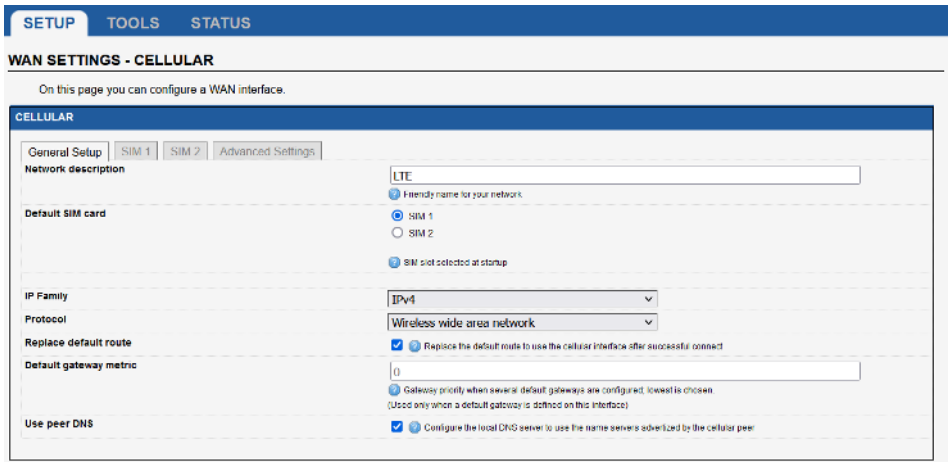
If you have familiarized yourself with the configuration scheme, we can start configuring the router using instructions provided in this section. In WaveOS 4.22.0.1 release, the Cellular Interface is enabled by default. In this note, only the SIM card 1 is configured.

In the GUI, go to Setup → Physical Interfaces → WAN Interface.

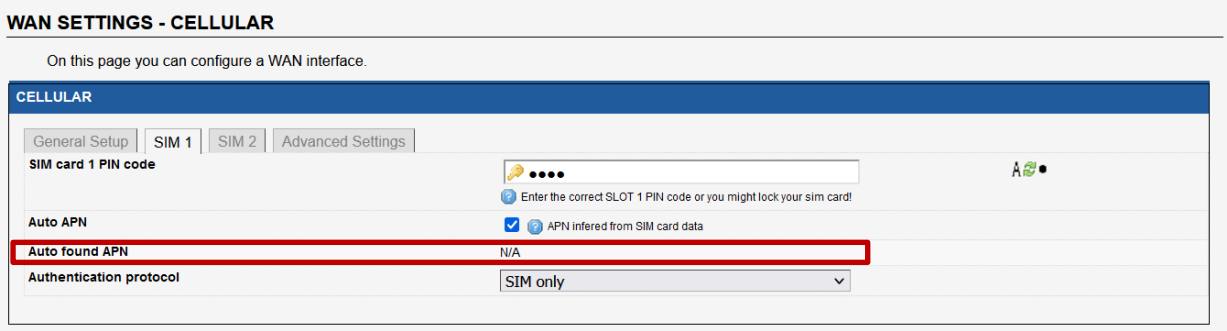


Click the "Edit" button located to the right and let configure WAN Interface.

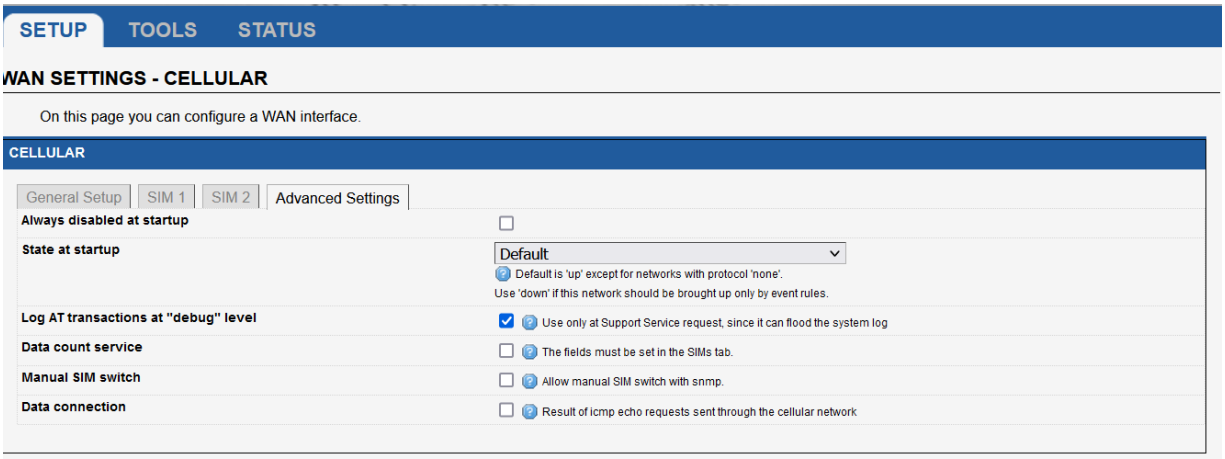
- General Setup : (*Check if the predefined configuration suite your use case*)
  - Network description :LTE (use your custom name)
  - Default SIM card:1
  - Select IPv4 in IP family
  - Check Replace default route
  - Set 0 as routing metric for default gateway
  - Check Use peer DNS to use the ISP DNS
  - Save



- SIM1
  - SIM card 1 PIN code: Your custom PIN code to avoid the SIM lock
  - Auto APN: Enable APN inferred from SIM card data (**Enabled by default**)
  - Auto found APN (): N/A until we have save and apply the configuration. Then it will automatically select the APN found in the database for this simcard.
  - Authentication protocol: SIM only



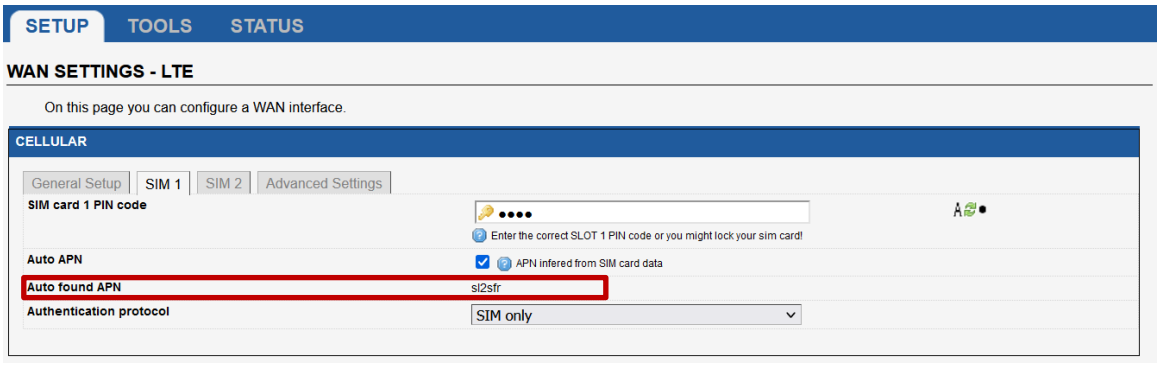
- Advanced Setting (*Check if the predefined configuration suite your use case*)
  - Enable AT transactions logs for better understanding in troubleshoot in case of issue.
  - Save and apply



NOTE: In this note the Data count service , Manual SIM switch and Data Connection sections will not be used, they are not part of this how-to.

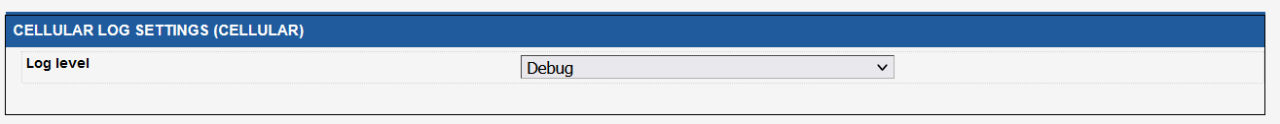
In order to check if the Auto APN has found automatically the appropriate APN, let go in GUI and go to Setup → Physical Interfaces → Cellular →SIM1

- Auto found APN field is populated with the correct ISP APN: example: sl2sfr



NOTE: The list of internal APN database embedded in WaveOs, with the most known ISP APN, can be found in the Android Open Source Depot available on this link: https://android.googlesource.com/device/sample/+/master/etc/apns-full-conf.xml

For troubleshoot purpose, let enable the Cellular debug. Go in Tools Logs Setting→ Cellular → Log Setting

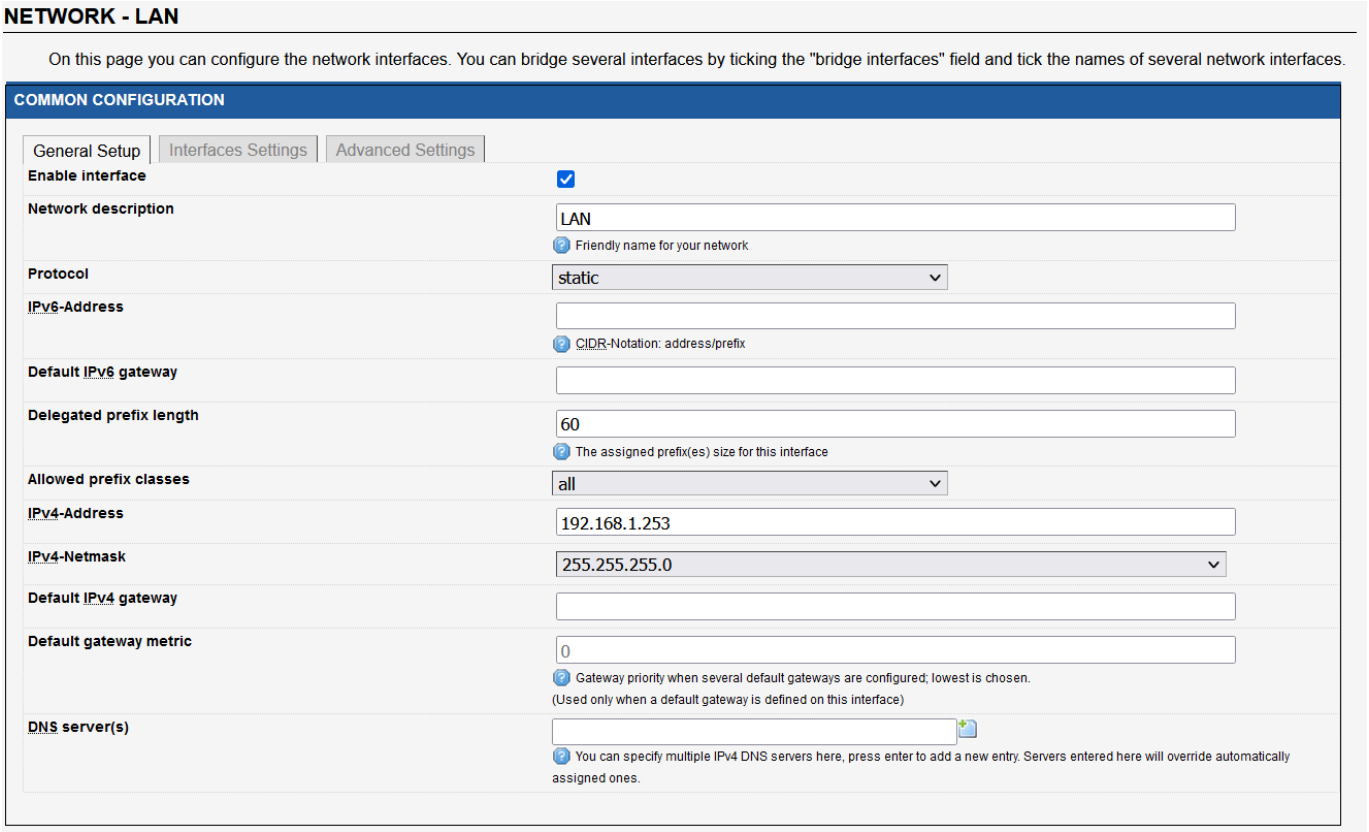


Configuring LAN Interface (*Check if the predefined configuration suites your use case*)

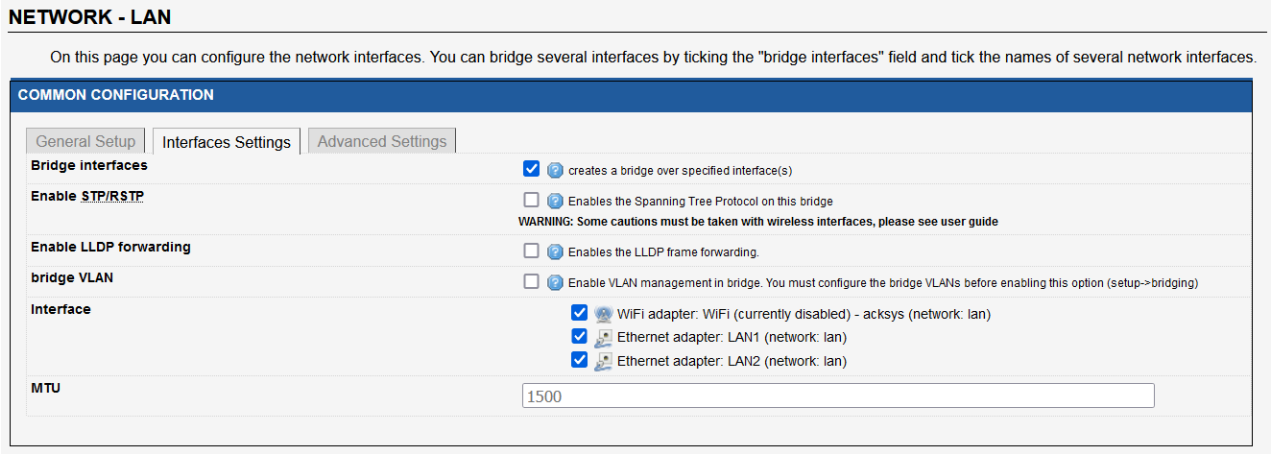
In this note, we will use the default IP address of the router 192.168.1.253 :

Go in GUI and go to Setup → Physical Interfaces → LAN setting Interface:

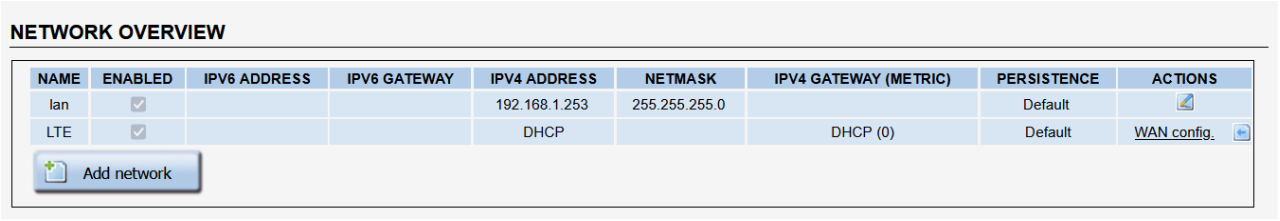
- General Setup
  - Enable Interface: Check
  - Network description: LAN (you could use your custom name)
  - Protocol: static
  - IPv4 address: 192.168.1.253
  - IPv4 Netmask: 255.255.255.0



- Interface Setting
  - Bridge interfaces: Check
  - Interface: WIFI adapter, LAN1 & LAN2 are bridged
  - Protocol: static
  - IPv4 address: 192.168.1.253
  - IPv4 Netmask: 255.255.255.0



Let have an overview on Network, Go in Setup → Network

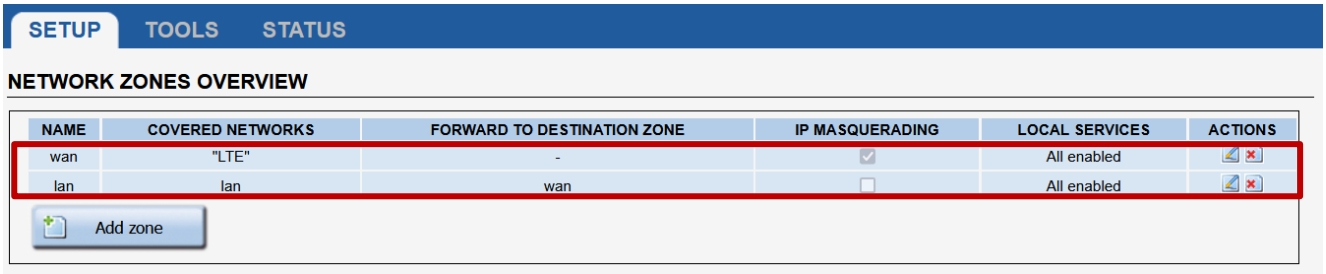


6. Configuring Routing on WAN Interface (*Check if the predefined configuration suites your use case*)

WaveOs release 4.22.0.1 comes with some features by default but we are interesting in this note on these features below and which will perform automatically the routing configuration:

- By default the WAN interface is enabled
- By default Routing/Firewall →Network Zones are created
- NAT (IP masquering) is enabled on the WAN zone
- IP forward is allowed from the LAN to the WAN
- By default Auto APN is enable on the SIM

Login to the router's WebUI and go to Setup → Routing/Firewall →Network Zones.

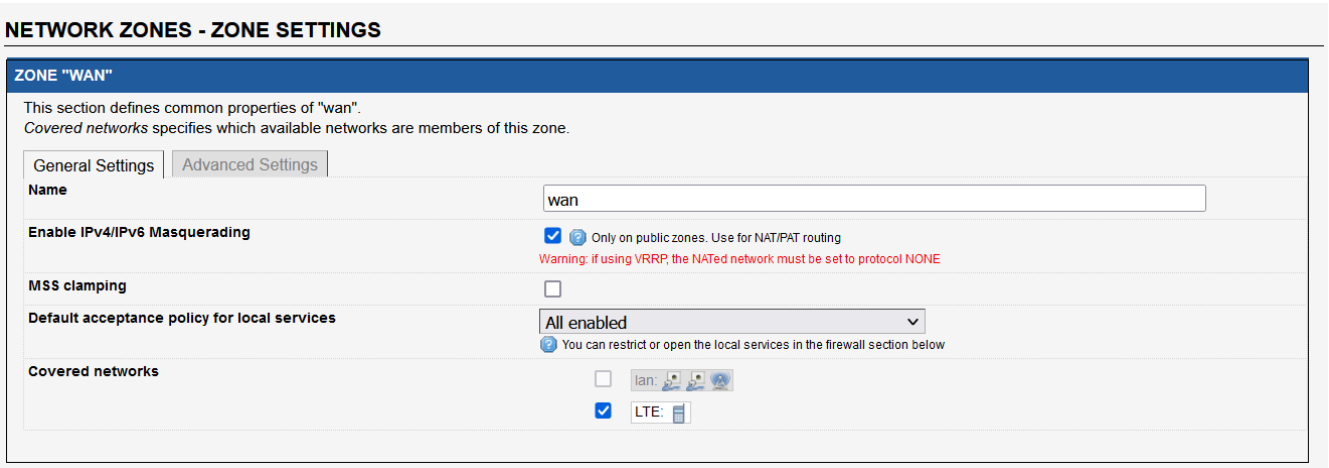


The 2 Networks Zones are created and associated to the 2 Network Interfaces (LAN and WAN) with NAT enabled on WAN.

WAN Zone Overview

In the router's WebUI and go to Setup → Routing/Firewall →Network Zones→ edit WAN Zone to see the configuration:

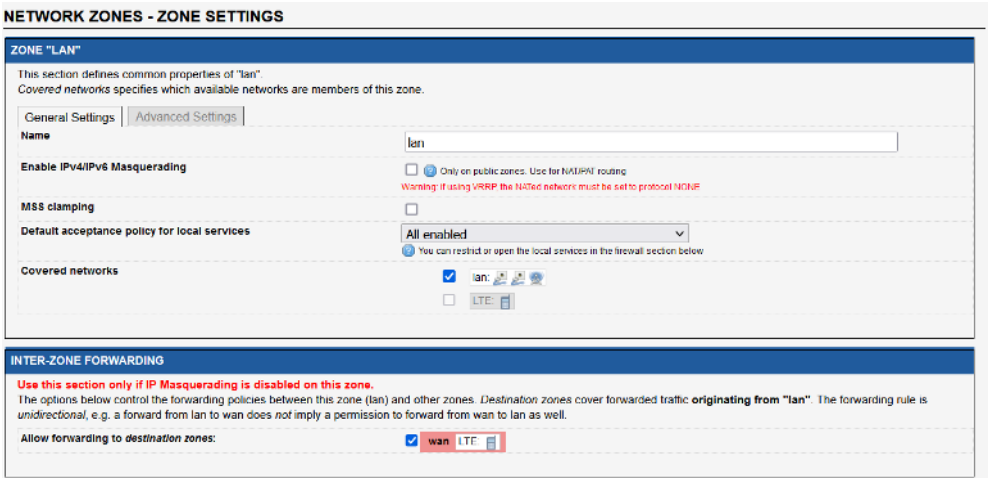
- Name: WAN (you could use your custom name)
- Enable IPv4/IPv6 Masquerading: checked
- Covered networks: LTE



LAN Zone Overview

In the router's WebUI and go to Setup → Routing/Firewall →Network Zones→ edit LAN Zone to see the configuration:

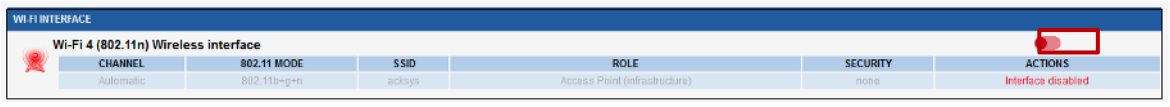
- Name: LAN (you could use your custom name)
- Enable IPv4/IPv6 Masquerading: Not checked
- Covered networks: LAN
- Allow Forwarding to destination zones: WAN (to allow devices connected to the LAN interface to get internet access.



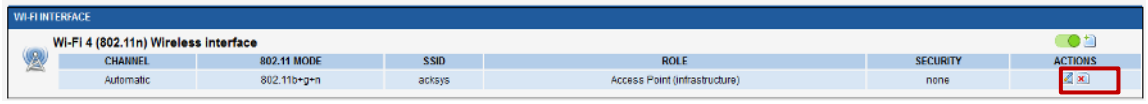
Configuring the AP role on WIFI Interface

By default, the WIFI interface is disable and need to be enabled before configuring the AP and for this note, we will configure the Access Point with the following information:

- In GUI and go to Setup → Physical Interfaces →Enable the WIFI Interface.

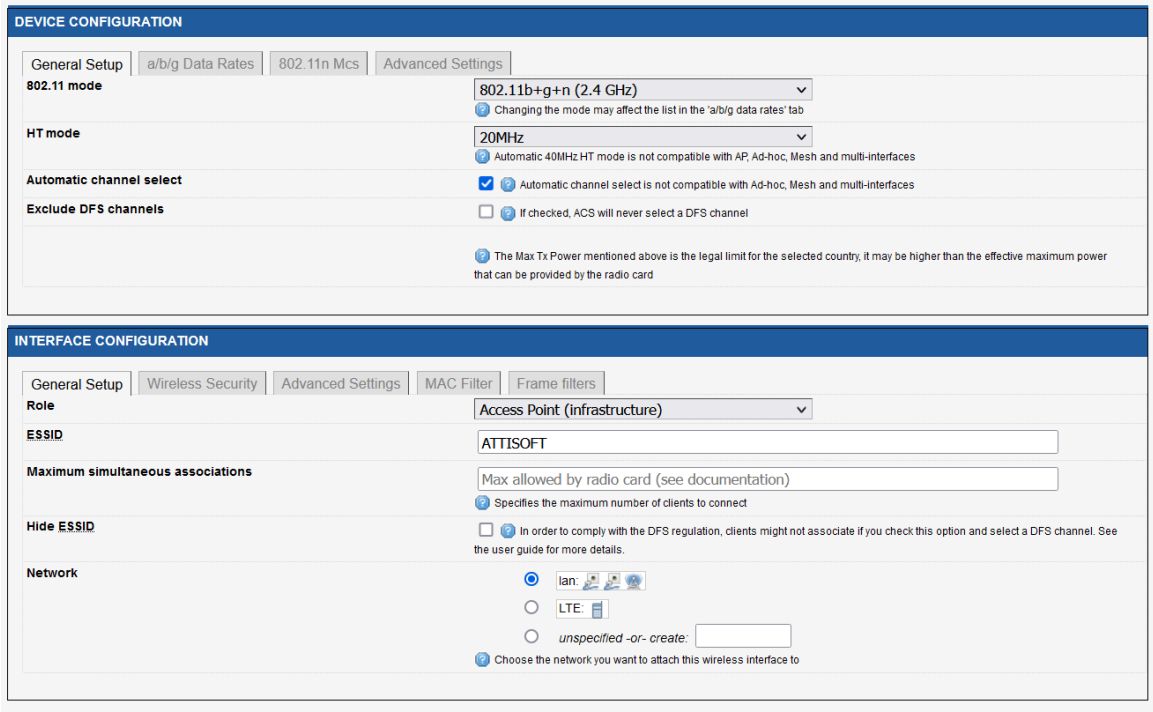


- Click the "Edit" button located to the right and configure your WIFI SSID.

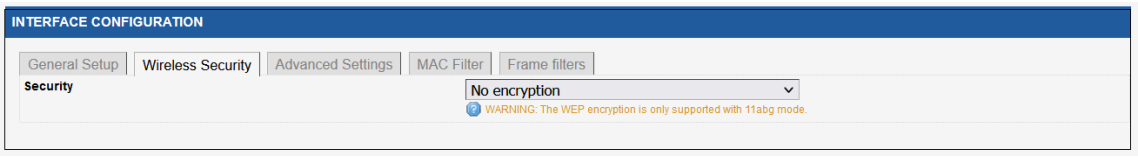


You will be redirected to the settings window where you can start configuring

- Role: Access Point
- ESSID: ATTISOFT
- Network: Lan
- Click on Save



- Security: No encryption (only in this note but we invite partner to set a strong password)

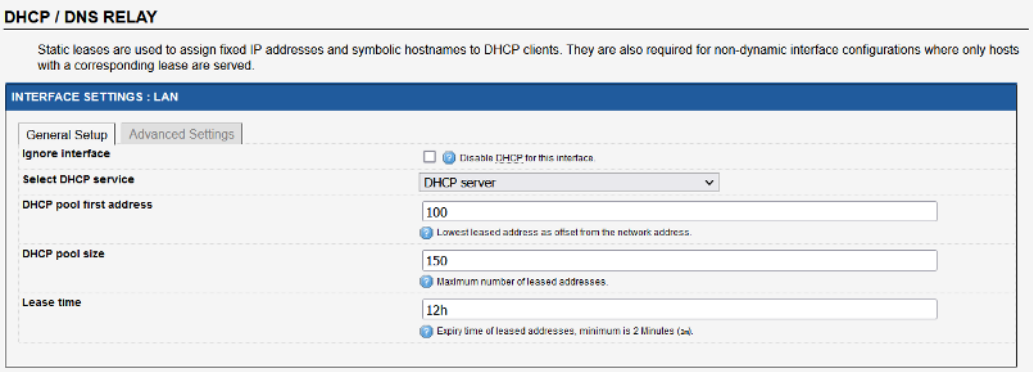


Configuring DHCP Server on WIFI Interface

Note: In this example, we use IPV4 protocol family for the ISP and the WiFi connection, so the DHCP server and the ip connectivity will be performed in IPV4. In case your change the default config from IPV4 to IPV6, you have to adapt according to your configuration.
By default, the DHCP server is disabled and to allow end devices to receive IP address, we will configure the DHCP server with the default following information:

In GUI and go to Setup → Services →DHCP/DNS RELAY

- LAN Interface is enable DHCP
- Select DHCP service: DHCP server
- Save and Apply

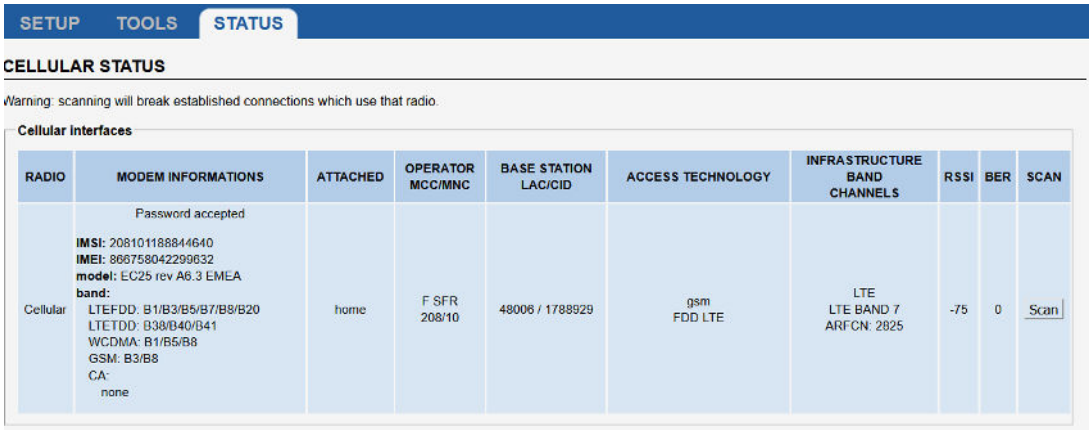


7. Checking Cellular network STATUS

If you've followed all the steps presented above, your configuration should be finished and let have an overview on status of the Cellular and Network.

WAN Router: Cellular STATUS

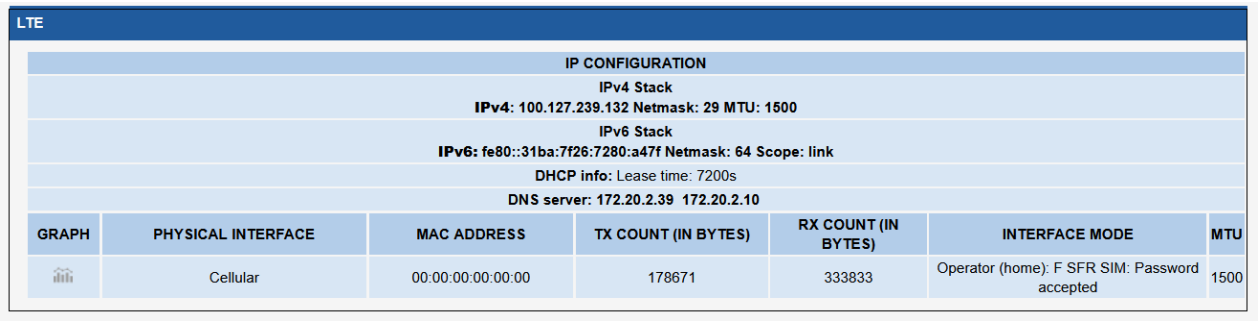
In GUI and go to Status → Cellular



WAN Router : Network STATUS

To verify the connection, click in Status→Network as shown in the screenshot below where the WAN interface receive Internet IP address from the ISP.

In GUI and go to **Status → Network**



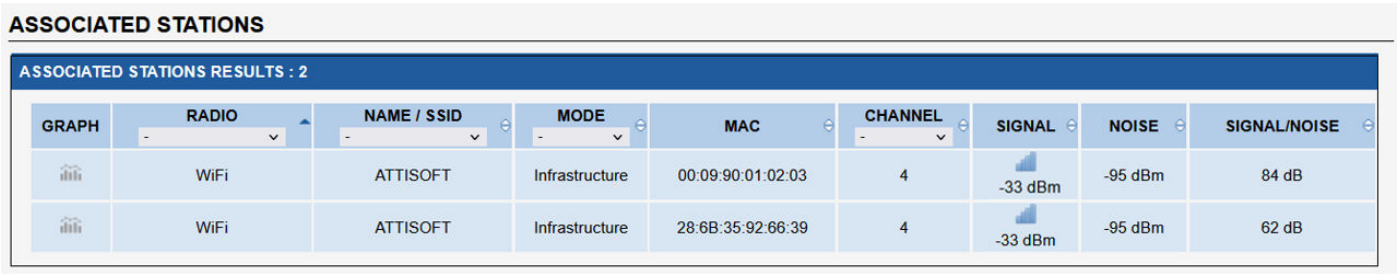
LTE

IP CONFIGURATION
IPv4 Stack **IPv4: 100.127.239.132 Netmask: 29 MTU: 1500**
IPv6 Stack **IPv6: fe80::31ba:7f26:7280:a47f Netmask: 64 Scope: link**
DHCP info: Lease time: 7200s
DNS server: 172.20.2.39 172.20.2.10

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	Cellular	00:00:00:00:00:00	178671	333833	Operator (home): F SFR SIM: Password accepted	1500

WAN Router: Wireless STATUS

As expected, the Both End devices (Airlink and Windows WIFI clients) are connected to the WAN routeur in GUI and go to **Status → Wireless**



ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 2

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WiFi	ATTISOFT	Infrastructure	00:09:90:01:02:03	4	-33 dBm	-95 dBm	84 dB
	WiFi	ATTISOFT	Infrastructure	28:6B:35:92:66:39	4	-33 dBm	-95 dBm	62 dB

8. TESTING

If you've followed all the steps presented above, your configuration should be finished as expected therefore we can test internet access with an internet ICMP connectivity.

AIRBOX Router Internet Testing

Let us ping Google DNS address which works as shown below. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly.

TEST IN CLI

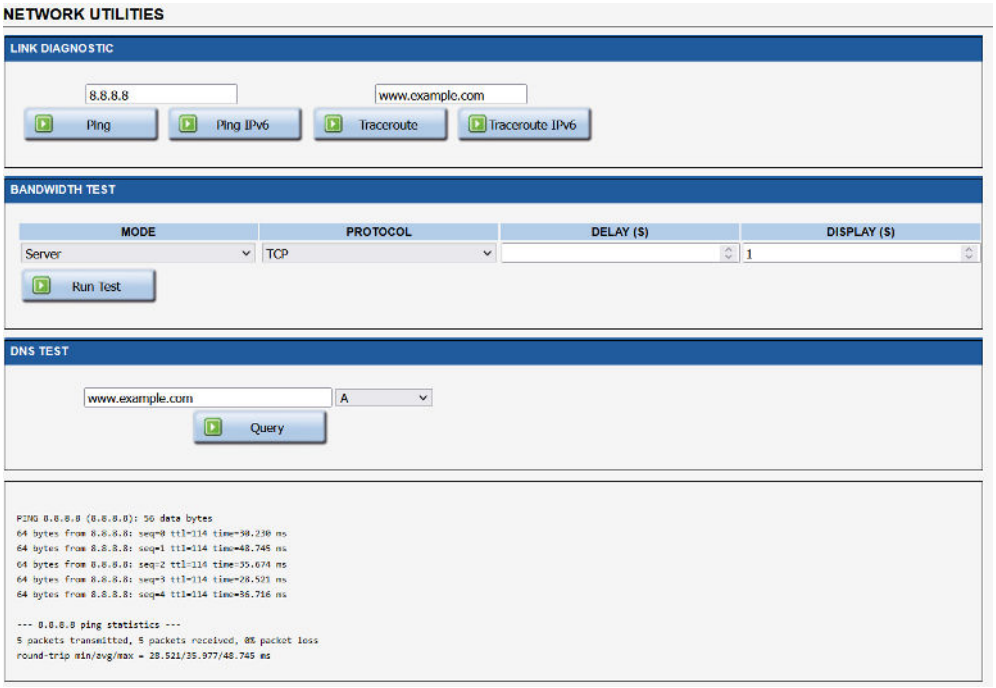
In GUI , Setup → Service →Enable SSH Server to access CLI for ICMP Test.

```
root@AutoAPN:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=115 time=57.072 ms
64 bytes from 8.8.8.8: seq=1 ttl=115 time=49.039 ms
64 bytes from 8.8.8.8: seq=2 ttl=115 time=48.816 ms
64 bytes from 8.8.8.8: seq=3 ttl=115 time=28.601 ms
64 bytes from 8.8.8.8: seq=4 ttl=115 time=28.768 ms
64 bytes from 8.8.8.8: seq=5 ttl=115 time=29.675 ms
64 bytes from 8.8.8.8: seq=6 ttl=115 time=47.956 ms
64 bytes from 8.8.8.8: seq=7 ttl=115 time=55.116 ms
64 bytes from 8.8.8.8: seq=8 ttl=115 time=28.897 ms
64 bytes from 8.8.8.8: seq=9 ttl=115 time=28.684 ms
64 bytes from 8.8.8.8: seq=10 ttl=115 time=28.224 ms
64 bytes from 8.8.8.8: seq=11 ttl=115 time=38.379 ms
64 bytes from 8.8.8.8: seq=12 ttl=115 time=47.814 ms

--- 8.8.8.8 ping statistics ---
13 packets transmitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 28.224/39.772/57.072 ms
```

TEST IN GUI

In GUI, Setup → Network →Link diagnostic for ICMP Test.



AirLink Router (Wi-Fi end device) Internet Testing

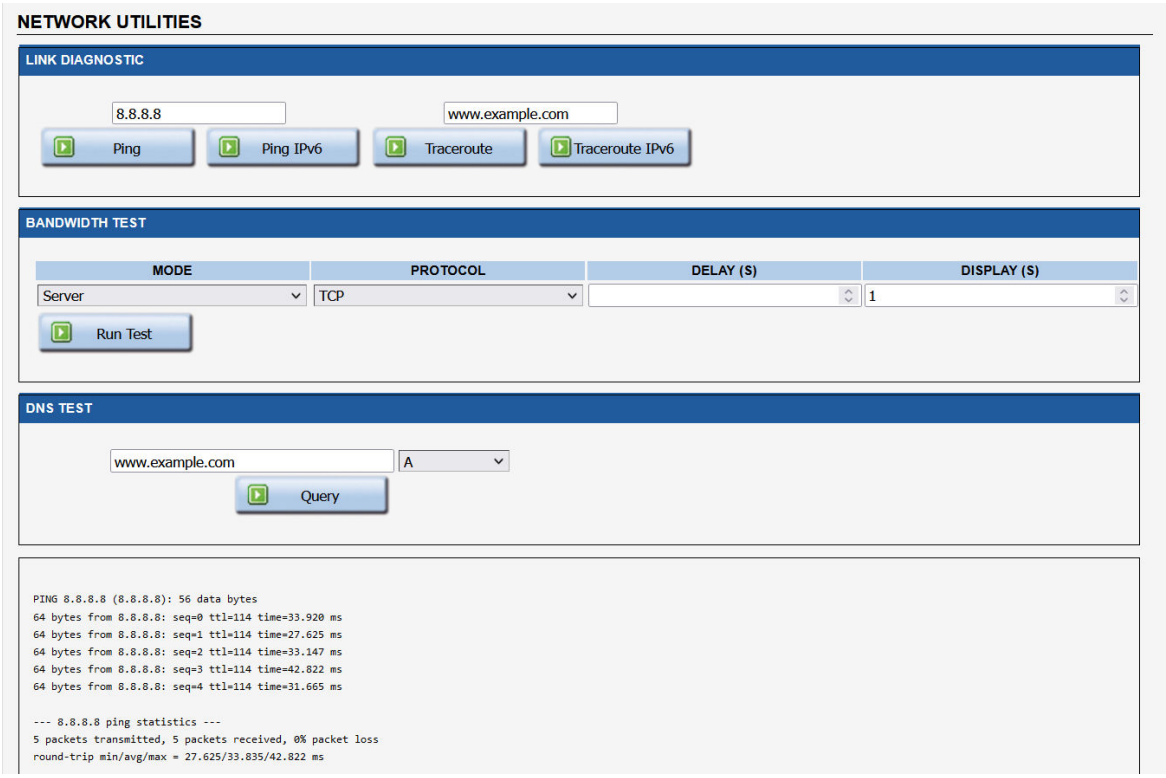
In this note the configuration of AirLink router is not described but the router is in its default configuration with 192.168.1.250 as IP address and in Client role. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. Internet access is ok as shown the response of Google DNS

```
root@CLIENT-WIFI:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=114 time=21.423 ms
64 bytes from 8.8.8.8: seq=1 ttl=114 time=30.038 ms
64 bytes from 8.8.8.8: seq=2 ttl=114 time=29.396 ms
64 bytes from 8.8.8.8: seq=3 ttl=114 time=49.810 ms
64 bytes from 8.8.8.8: seq=4 ttl=114 time=29.248 ms
64 bytes from 8.8.8.8: seq=5 ttl=114 time=35.095 ms
64 bytes from 8.8.8.8: seq=6 ttl=114 time=27.939 ms
64 bytes from 8.8.8.8: seq=7 ttl=114 time=28.327 ms
64 bytes from 8.8.8.8: seq=8 ttl=114 time=28.761 ms
64 bytes from 8.8.8.8: seq=9 ttl=114 time=26.547 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 21.423/30.658/49.810 ms
```

TEST IN GUI

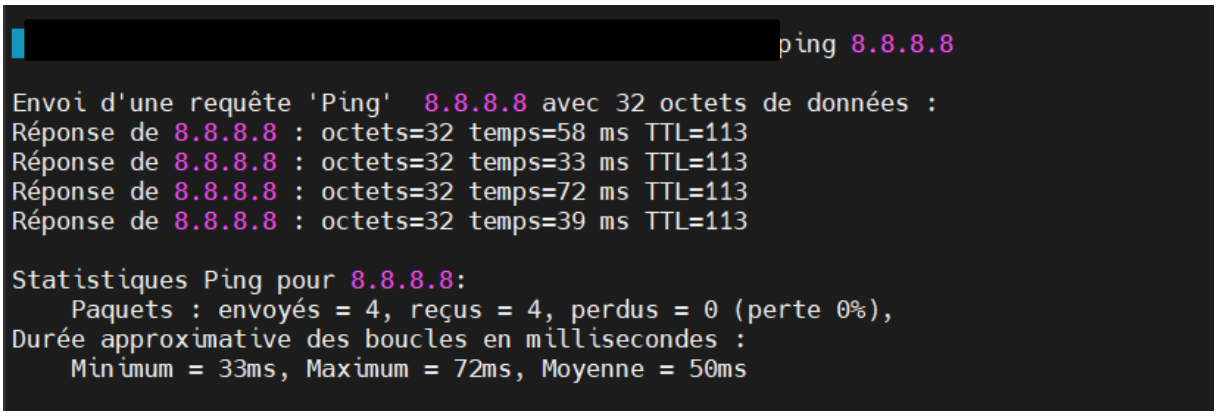
In GUI, Setup → Network →Link diagnostic for ICMP Test.



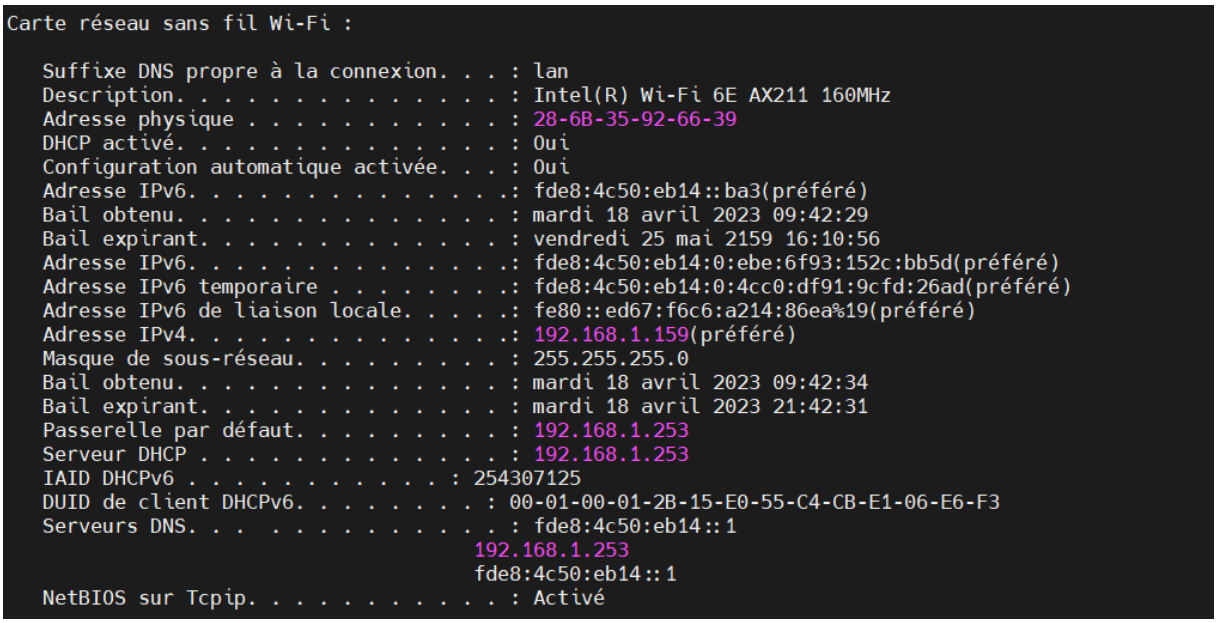
Windows Client (end device): Network Testing

If you've followed all the steps presented above, your configuration should be finished. But as with any other configuration, it is always wise to test the setup in order to make sure that it works properly. Internet access is ok as shown the response of Google DNS

TEST IN TERMINAL



IPCONFIG OUTPUT

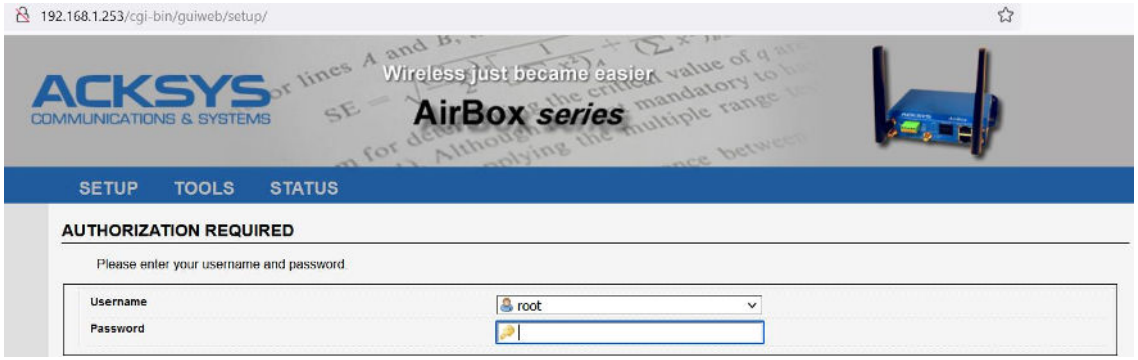


9. ANNEX

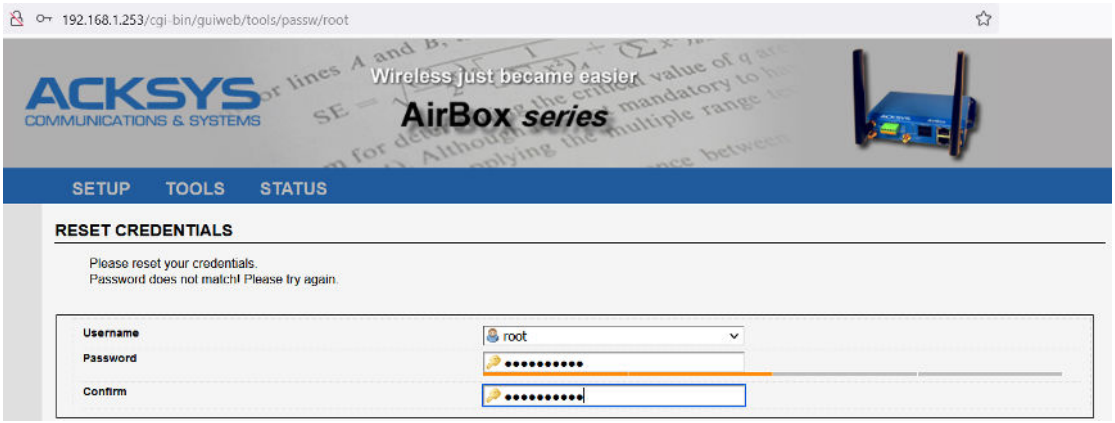
GUI Password Policy Access

WaveOs release 4.22.0.1 doesn't have only Auto APN feature but also Password policies where before access GUI, a strong password need to be configured.

From factory setting, in GUI and enter the default login and password (by default no password):



You will be redirected to the settings window where you can define the password with a minimum of 8 characters by pay attention to avoid dictionary password:

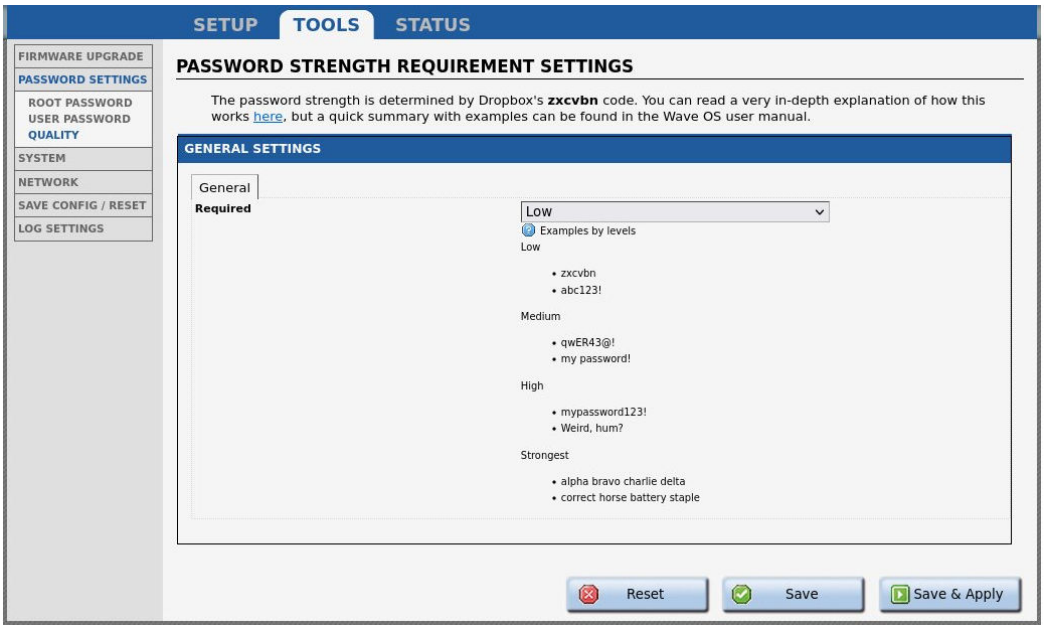


- Password: your strong password
- Confirm: confirm your strong password

The new defined password is well saved and therefore we could continue the configuration on WAN router.

> NOTE:
> We lock and unlock **SSH and GUI** accounts after reaching a certain failed number of login attempts (3) with unlock_time=1200 seconds.
> **To reset the authentication token in RAM, it is necessary to reboot the router.**

EXAMPLE OF PASSWORD Per Level



Support : https://support.acksys.fr