

APPLICATION NOTE

APNUS031 How to Configure Cellular Router with
Auto APN
July 2023

Content

1. Glossary.....	3
2. Introduction.....	3
3. Installation Overview and Prerequisites	3
4. Auto APN Configuration architecture	4
5. Acksys Router Configuration	5
Configuration WAN Interface	5
Configuring LAN Interface (<i>Check if the predefined configuration suite your use case</i>)	8
6. Configuring Routing on WAN Interface (<i>Check if the predefined configuration suites your use case</i>)	10
Configuring the AP role on WIFI Interface	11
Configuring DHCP Server on WIFI Interface	13
7. Checking Cellular network STATUS	13
WAN Router: Cellular STATUS	13
WAN Router : Network STATUS.....	14
WAN Router: Wireless STATUS.....	14
8. TESTING	14
AIRBOX Router Internet Testing	15
TEST IN CLI.....	15
TEST IN GUI.....	15
AirLink Router (Wi-Fi end device) Internet Testing.....	16
TEST IN GUI.....	16
Windows Client (end device): Network Testing.....	17
TEST IN TERMINAL.....	17
IPCONFIG OUTPUT	17
9. ANNEX	18
GUI Password Policy Access	18

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.

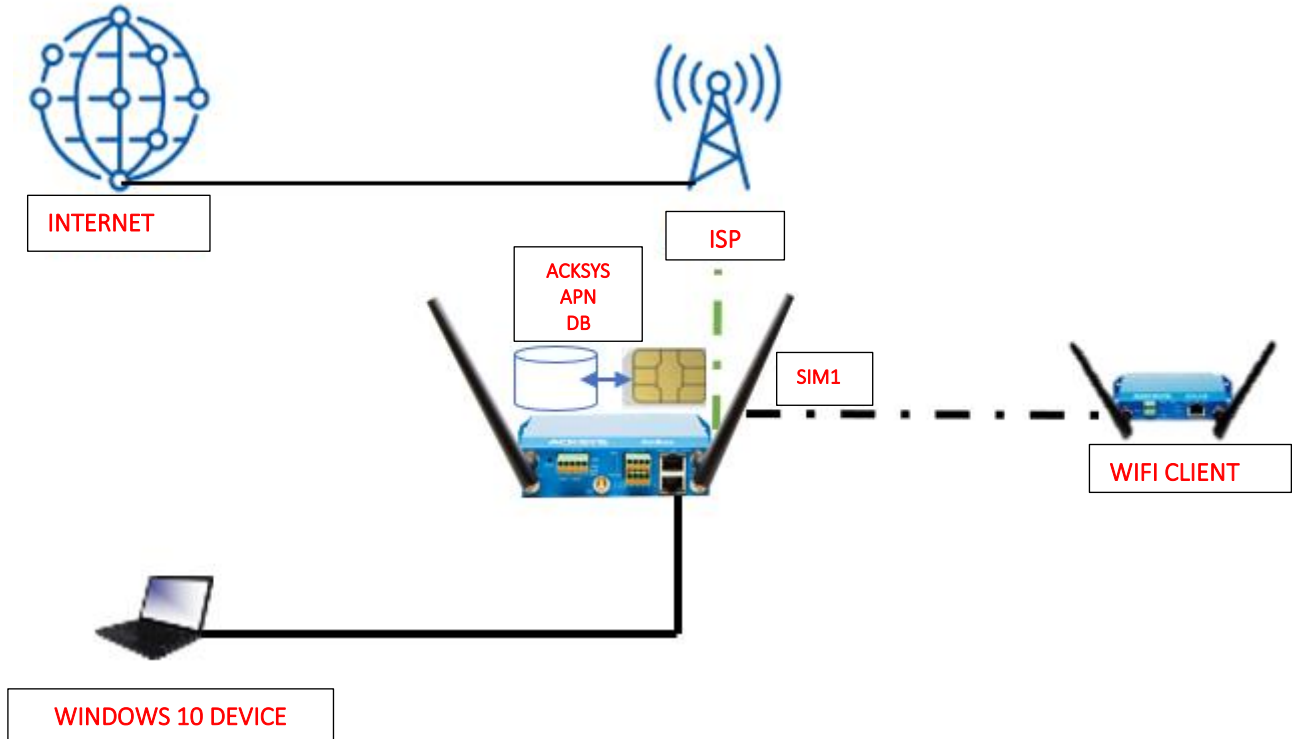
3. Installation Overview and Prerequisites

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.

The screenshot shows the router's configuration interface. At the top, there are tabs for 'SETUP', 'TOOLS', and 'STATUS'. Below this is the 'WIRELESS INTERFACES OVERVIEW' section, which includes a table for channel selection and interface combinations. Below the table is a note about shared channels. The 'WI-FI INTERFACE' section shows a 'Wi-Fi 4 (802.11n) Wireless interface' that is currently disabled. The 'WAN INTERFACE' section shows a '3G/4G/LTE Cellular radio (Cellular)' that is currently enabled.

Combination	Channel selection		Max number of interfaces			
	Multiplicity	Can use DFS	Access point	Infrastructure client	Mesh point	Ad-hoc
Multiple access points	single, auto, multiple	yes	8			
Portal	single	no	8		1	
Client / bridge	single, auto, multiple, roaming	yes		1		
Other / repeater	single	no	8	1 (non-roaming)	1	1

When using several roles, they all use the same shared channel; in this case, the client role must not be set to multichannel roaming. Repeater mode is a combination of two roles: access point + client.

CHANEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11b+g+n	acksys	Access Point (infrastructure)	none	Interface disabled

FRIENDLY NAME	ACTIONS
Cellular	[Edit]

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

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

Network description

Default SIM card

SIM 1
 SIM 2

SIM slot selected at startup

IP Family

Protocol

Replace default route Replace the default route to use the cellular interface after successful connect

Default gateway metric

Gateway priority when several default gateways are configured, lowest is chosen. (Used only when a default gateway is defined on this interface)

Use peer DNS Configure the local DNS server to use the name servers advertised by the cellular peer

- 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

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

SIM card 1 PIN code

Enter the correct SLOT 1 PIN code or you might lock your sim card!

Auto APN APN inferred from SIM card data

Auto found APN

Authentication protocol

- 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

WAN SETTINGS - CELLULAR

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | SIM 2 | Advanced Settings

Always disabled at startup

State at startup

Default is 'up' except for networks with protocol 'none'. Use 'down' if this network should be brought up only by event rules.

Log AT transactions at "debug" level Use only at Support Service request, since it can flood the system log

Data count service The fields must be set in the SIMs tab.

Manual SIM switch Allow manual SIM switch with snmp.

Data connection Result of icmp echo requests sent through the cellular network

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

The screenshot shows the 'WAN SETTINGS - LTE' configuration page. Under the 'CELLULAR' section, there are tabs for 'General Setup', 'SIM 1', 'SIM 2', and 'Advanced Settings'. The 'SIM 1' tab is active. The 'SIM card 1 PIN code' field is masked with dots. Below it, the 'Auto APN' section is checked, and the 'Auto found APN' field is highlighted with a red box, showing the value 'sl2sfr'. The 'Authentication protocol' is set to 'SIM only'.

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

The screenshot shows the 'CELLULAR LOG SETTINGS (CELLULAR)' page. The 'Log level' dropdown menu is set to 'Debug'.

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

NETWORK - LAN

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

COMMON CONFIGURATION

General Setup

Interfaces Settings

Advanced Settings

Enable interface	<input checked="" type="checkbox"/>
Network description	<input type="text" value="LAN"/> <small>📘 Friendly name for your network</small>
Protocol	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> static ▼ </div>
IPv6-Address	<input type="text"/>
Default IPv6 gateway	<input type="text"/>
Delegated prefix length	<input type="text" value="60"/> <small>📘 The assigned prefix(es) size for this interface</small>
Allowed prefix classes	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> all ▼ </div>
IPv4-Address	<input type="text" value="192.168.1.253"/>
IPv4-Netmask	<div style="border: 1px solid #ccc; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> 255.255.255.0 ▼ </div>
Default IPv4 gateway	<input type="text"/>
Default gateway metric	<input type="text" value="0"/> <small>📘 Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateway is defined on this interface)</small>
DNS server(s)	<input type="text"/> <small>📘 You can specify multiple IPv4 DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.</small>

- 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

NETWORK - LAN

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

COMMON CONFIGURATION

General Setup

Interfaces Settings

Advanced Settings

Bridge interfaces creates a bridge over specified interface(s)

Enable STP/RSTP Enables the Spanning Tree Protocol on this bridge
WARNING: Some cautions must be taken with wireless interfaces, please see user guide

Enable LLDP forwarding Enables the LLDP frame forwarding.

bridge VLAN Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)

Interface

- WiFi adapter: WiFi (currently disabled) - acksys (network: lan)
- Ethernet adapter: LAN1 (network: lan)
- Ethernet adapter: LAN2 (network: lan)

MTU

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

NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	<input checked="" type="checkbox"/>			192.168.1.253	255.255.255.0		Default	
LTE	<input checked="" type="checkbox"/>			DHCP		DHCP (0)	Default	WAN config.

Add 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 masquerading) 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.

NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
wan	"LTE"	-	<input checked="" type="checkbox"/>	All enabled	
lan	lan	wan	<input type="checkbox"/>	All enabled	

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

NETWORK ZONES - ZONE SETTINGS

ZONE "WAN"

This section defines common properties of "wan".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name wan

Enable IPv4/IPv6 Masquerading Only on public zones. Use for NAT/PAT routing
Warning: if using VRRP, the NATed network must be set to protocol NONE

MSS clamping

Default acceptance policy for local services All enabled
You can restrict or open the local services in the firewall section below

Covered networks

lan:

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).

NETWORK ZONES - ZONE SETTINGS

ZONE "LAN"

This section defines common properties of "lan".
Covered networks specifies which available networks are members of this zone.

General Settings | Advanced Settings

Name: lan

Enable IPv4/IPv6 Masquerading: Only on public zones. Use for NAT/PAT routing
Warning, if using VRRP, the NATed network must be set to protocol NONE

MSS clamping:

Default acceptance policy for local services: All enabled

Covered networks: lan, LTE

INTER-ZONE FORWARDING

Use this section only if IP Masquerading is disabled on this zone.
The options below control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from "lan". 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 forwarding to destination zones: wan, LTE

Configuring the AP role on WIFI Interface

By default, the WIFI interface is disabled 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.

CHANEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11b+g+n	acksys	Access Point (infrastructure)	none	Interface disabled

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

CHANEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11b+g+n	acksys	Access Point (infrastructure)	none	<input checked="" type="checkbox"/> Edit

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

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

DEVICE CONFIGURATION

General Setup | a/b/g Data Rates | 802.11n Mcs | **Advanced Settings**

802.11 mode 802.11b+g+n (2.4 GHz)
Changing the mode may affect the list in the 'a/b/g data rates' tab

HT mode 20MHz
Automatic 40MHz HT mode is not compatible with AP, Ad-hoc, Mesh and multi-interfaces

Automatic channel select Automatic channel select is not compatible with Ad-hoc, Mesh and multi-interfaces

Exclude DFS channels If checked, ACS will never select a DFS channel

The Max Tx Power mentioned above is the legal limit for the selected country, it may be higher than the effective maximum power that can be provided by the radio card

INTERFACE CONFIGURATION

General Setup | **Wireless Security** | Advanced Settings | MAC Filter | Frame filters

Role Access Point (Infrastructure)

ESSID ATTISOFT

Maximum simultaneous associations Max allowed by radio card (see documentation)
Specifies the maximum number of clients to connect

Hide ESSID In order to comply with the DFS regulation, clients might not associate if you check this option and select a DFS channel. See the user guide for more details.

Network
 lan: 📶 🌐 🌐 🌐
 LTE: 📶
 unspecified -or- create: _____
Choose the network you want to attach this wireless interface to

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

INTERFACE CONFIGURATION

General Setup | **Wireless Security** | Advanced Settings | MAC Filter | Frame filters

Security No encryption
WARNING: The WEP encryption is only supported with 11abg mode.

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

DHCP / DNS RELAY

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.

INTERFACE SETTINGS : LAN

General Setup | **Advanced Settings**

Ignore interface Disable DHCP for this interface

Select DHCP service: DHCP server

DHCP pool first address: 100
Lowest leased address as offset from the network address.

DHCP pool size: 150
Maximum number of leased addresses.

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

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

SETUP TOOLS STATUS									
CELLULAR STATUS									
Warning: scanning will break established connections which use that radio.									
Cellular interfaces									
RADIO	MODEM INFORMATIONS	ATTACHED	OPERATOR MCC/MNC	BASE STATION LAC/CID	ACCESS TECHNOLOGY	INFRASTRUCTURE BAND CHANNELS	RSSI	BER	SCAN
Cellular	Password accepted IMSI: 208101188844640 IMEI: 866758042299632 model: EC25 rev A6.3 EMEA band: LTEFDD: B1/B3/B5/B7/B8/B20 LTEFDD: B38/B40/B41 WCDMA: B1/B5/B8 GSM: B3/B8 CA: none	home	F SFR 208/10	48006 / 1788929	gsm FDD LTE	LTE LTE BAND 7 ARFCN: 2825	-75	0	Scan

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.

NETWORK UTILITIES

LINK DIAGNOSTIC

Ping

Ping IPv6

Traceroute

Traceroute IPv6

BANDWIDTH TEST

MODE	PROTOCOL	DELAY (S)	DISPLAY (S)
Server	TCP	1	1

Run Test

DNS TEST

Query

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=114 time=30.230 ms
64 bytes from 8.8.8.8: seq=1 ttl=114 time=48.745 ms
64 bytes from 8.8.8.8: seq=2 ttl=114 time=35.674 ms
64 bytes from 8.8.8.8: seq=3 ttl=114 time=28.521 ms
64 bytes from 8.8.8.8: seq=4 ttl=114 time=36.716 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 28.521/35.977/48.745 ms
    
```

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.

NETWORK UTILITIES

LINK DIAGNOSTIC

Ping

Ping IPv6

Traceroute

Traceroute IPv6

BANDWIDTH TEST

MODE	PROTOCOL	DELAY (S)	DISPLAY (S)
Server	TCP	1	1

Run Test

DNS TEST

Query

```

PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=114 time=33.920 ms
64 bytes from 8.8.8.8: seq=1 ttl=114 time=27.625 ms
64 bytes from 8.8.8.8: seq=2 ttl=114 time=33.147 ms
64 bytes from 8.8.8.8: seq=3 ttl=114 time=42.822 ms
64 bytes from 8.8.8.8: seq=4 ttl=114 time=31.665 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 27.625/33.835/42.822 ms
    
```


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

```

ping 8.8.8.8

Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=58 ms TTL=113
Réponse de 8.8.8.8 : octets=32 temps=33 ms TTL=113
Réponse de 8.8.8.8 : octets=32 temps=72 ms TTL=113
Réponse de 8.8.8.8 : octets=32 temps=39 ms TTL=113

Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 33ms, Maximum = 72ms, Moyenne = 50ms
    
```

IPCONFIG OUTPUT

```

Carte réseau sans fil Wi-Fi :

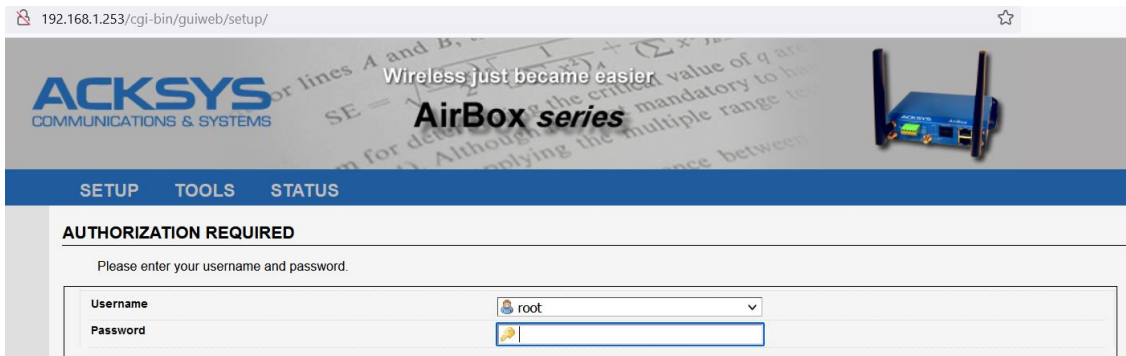
    Suffixe DNS propre à la connexion. . . : lan
    Description. . . . . : Intel(R) Wi-Fi 6E AX211 160MHz
    Adresse physique . . . . . : 28-6B-35-92-66-39
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6. . . . . : fde8:4c50:eb14::ba3(préfééré)
    Bail obtenu. . . . . : mardi 18 avril 2023 09:42:29
    Bail expirant. . . . . : vendredi 25 mai 2159 16:10:56
    Adresse IPv6. . . . . : fde8:4c50:eb14:0:ebe:6f93:152c:bb5d(préfééré)
    Adresse IPv6 temporaire . . . . . : fde8:4c50:eb14:0:4cc0:df91:9cfd:26ad(préfééré)
    Adresse IPv6 de liaison locale. . . . : fe80::ed67:f6c6:a214:86ea%19(préfééré)
    Adresse IPv4. . . . . : 192.168.1.159(préfééré)
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : mardi 18 avril 2023 09:42:34
    Bail expirant. . . . . : mardi 18 avril 2023 21:42:31
    Passerelle par défaut. . . . . : 192.168.1.253
    Serveur DHCP . . . . . : 192.168.1.253
    IAID DHCPv6 . . . . . : 254307125
    DUID de client DHCPv6. . . . . : 00-01-00-01-2B-15-E0-55-C4-CB-E1-06-E6-F3
    Serveurs DNS. . . . . : fde8:4c50:eb14::1
    192.168.1.253
    fde8:4c50:eb14::1
    NetBIOS sur Tcpip. . . . . : Activé
    
```

9. ANNEX

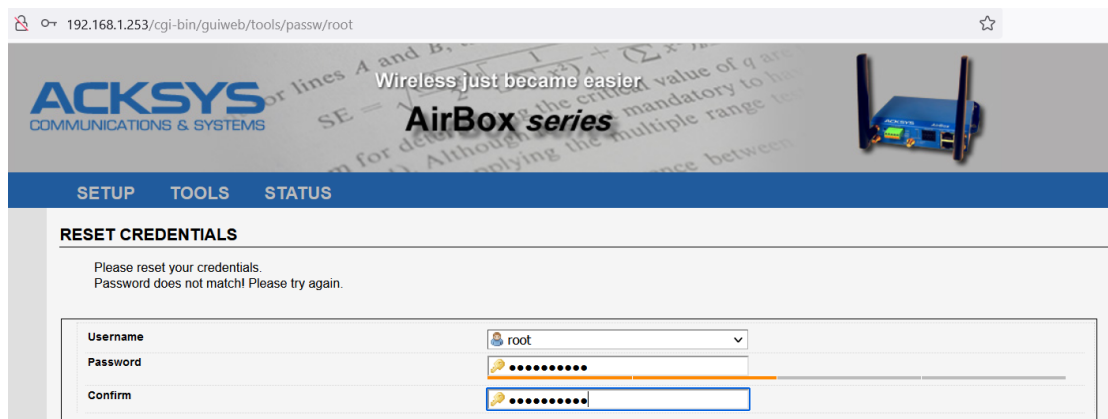
GUI Password Policy Access

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.

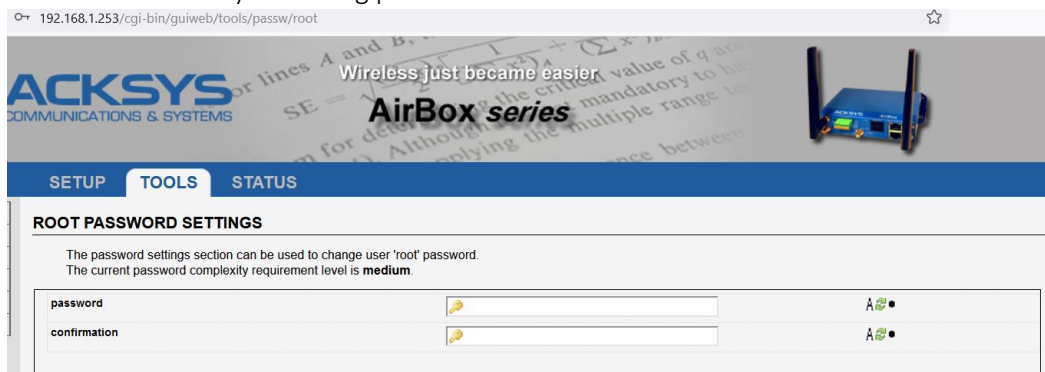
From factory setting, in GUI and enter the default login and password (by default no password):



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



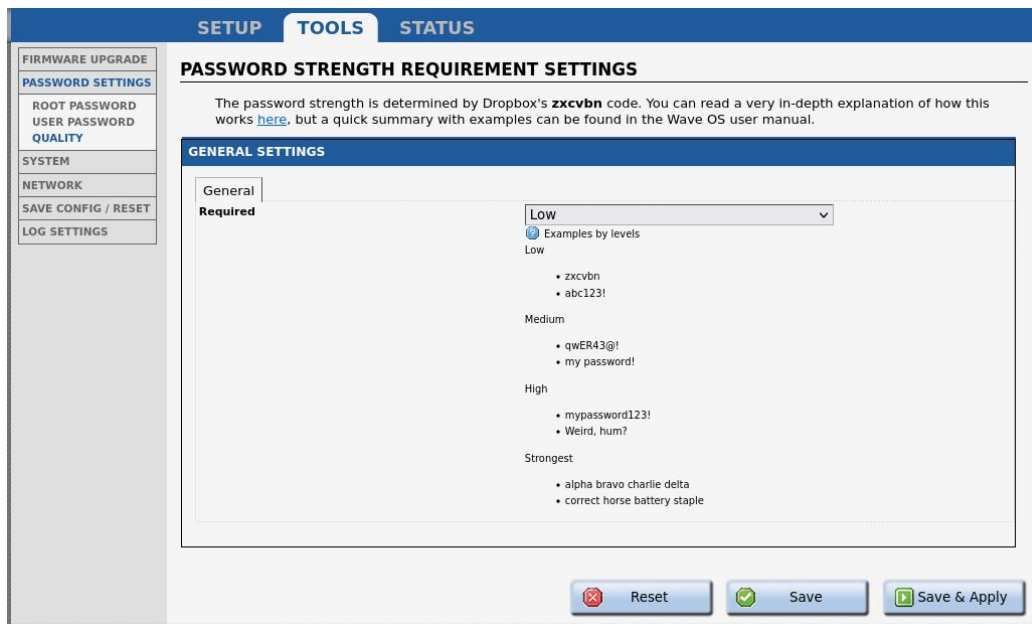
The new defined password is well saved and therefore we could continue the configuration on WAN router.

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>