ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

APNUS024
IPv6 routing over Cellular Network
IPv6-SLAAC/DHCPv6-NAT66

March 2023

Content

1. Glossary

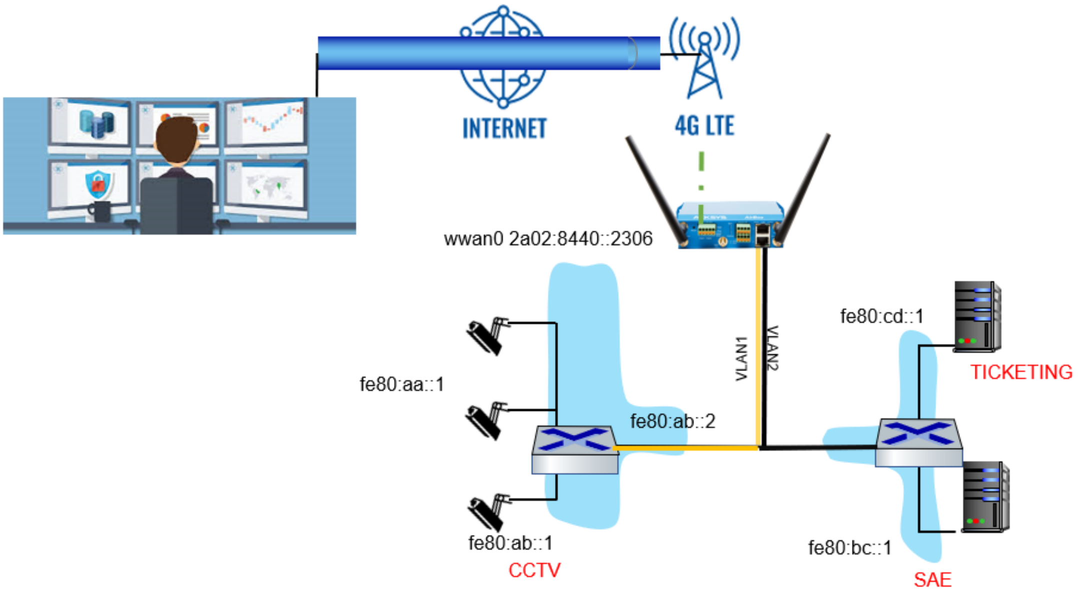
NDP :	Network Discovery Protocol
SLAAC :	Stateless Auto-Configuration
RA :	Router Advertisement server
DHCPv6 :	Dynamic Host Configuration Protocol version 6
RS :	Router Solicitation
DAD :	Duplicated Address Detection
NAT66 :	Network Address Translation IPv6_To_IPv6
ISP :	Internet Service Provider
ULA:	Unique Local Address
ISP:	Internet Service Provider

2. Introduction

Most of our end customers are in different category of activities specifically in transportation which need real time communication in motion.

They use several technology from management systems to provide even more information, comfort and safety to users to reduced traffic congestion results, less wasted time and reduced energy consumption. To improve fleet management, the number of on-board electronic equipment has considerably grown and WiFi Vs Cellular has quickly emerged amongst it.

For real time monitoring Mobile equipment switch WIFI to LTE but most of ISP move to IPv6 to easily manage their fleet in case they are out of WIFI coverage.



The assignment of an IPv6 address by the ISP to the cellular router imposes to have a network architecture that fits to the IPv6 address type, to allow the routing between the onboard network (or private network) and the internet network.

3. IPv6 address types

There are two different general classes of IPv6 addresses with 128-bit network layer identifier for a single interface of IPv6 node:

Routable address over Internet

GUA: stands for Global Unicast Address similar to IPv4 public address allocated by IANA from the prefix 2001::/3 to the regional providers.

Non routable address

ULA: stands for Unique Local Address used within a local site and not routed externally with reserved prefix. It allows sites to be interconnected without creating any address conflicts.

Link local: IPv6 link-local is a special type of unicast address unique on a subnet that is auto-configured on any interface using a combination of the link-local prefix FE80::/10 and the MAC address of the interface.

4. IPv6 address assignment method used by ISP

SLAAC

SLAAC stands for Stateless Address Autoconfiguration is a mechanism that enables each host on the network to auto-configure a unique IPv6 address without any device keeping track of which address is assigned to which node. **In general, the IP address autoconfigured via SLAAC is ULA address that is not routable via internet**

DHCPv6

DHCPv6 stands for Dynamic Host Configuration Protocol for IPv6 node similar as DHCPv4 with some exception and there are 4 DHCPv6 Server mode available in WaveOs:

SLAAC only mode: Client IPv6 autoconfiguration is based on RA server and DHCPv6 is Stopped
DHCPv6 Stateless: Based on SLAAC for client IPv6 addresses autoconfiguration
DHCPv6 Statefull: Same as DHCPv4, allocated addresses to clients without providing the gateway
DHCPv6 Statefull and Stateless: In this mode client can use SLAAC or request an address via DHCPv6 server
DHCPv6 Client: allow clients IPv6 to requests address from DHCPv6 server

In general, the IP address assigned via DHCPv6 is GUA address, the routing possibility over internet depends on the prefix length assigned by the ISP that shows if this prefix could be delegated to another subnet.

5. Overcome routing issue for non-routable IPv6 address assigned by ISP

ATTENTION:

- If DHCPv6 Prefix Delegation is configured but not working, then it is possible that the ISP **does not support this feature.**
  An indicator is that the Acksys router obtains an IPv6 address on the WAN interface, however clients behind the Acksys router **do not receive Ipv6 addresses**.

IPv6-to-IPv6 Network Prefix Translation (NPTv6), also known as NAT66, translates the internal IPv6 prefix in the IPv6 packet header to an external IPv6 prefix.

- The NAT66 device is connected to an internal network and an external network therefore hosts in the internal network uses locally routed IPv6 prefixes. When an internal host sends packets to access the external network, the NAT66 device translates the source IPv6 address prefix in the packets to a global unicast address prefix.
- To allow external users to access internal servers, such as Wed server or FTP server, configure IPv6 destination prefix mappings on the interface connected to the external network

Therefore, with NAT66, we will be able to route ULA addresses assigned by the ISP to the internet.

5. Implementation in ACKSYS cellular router

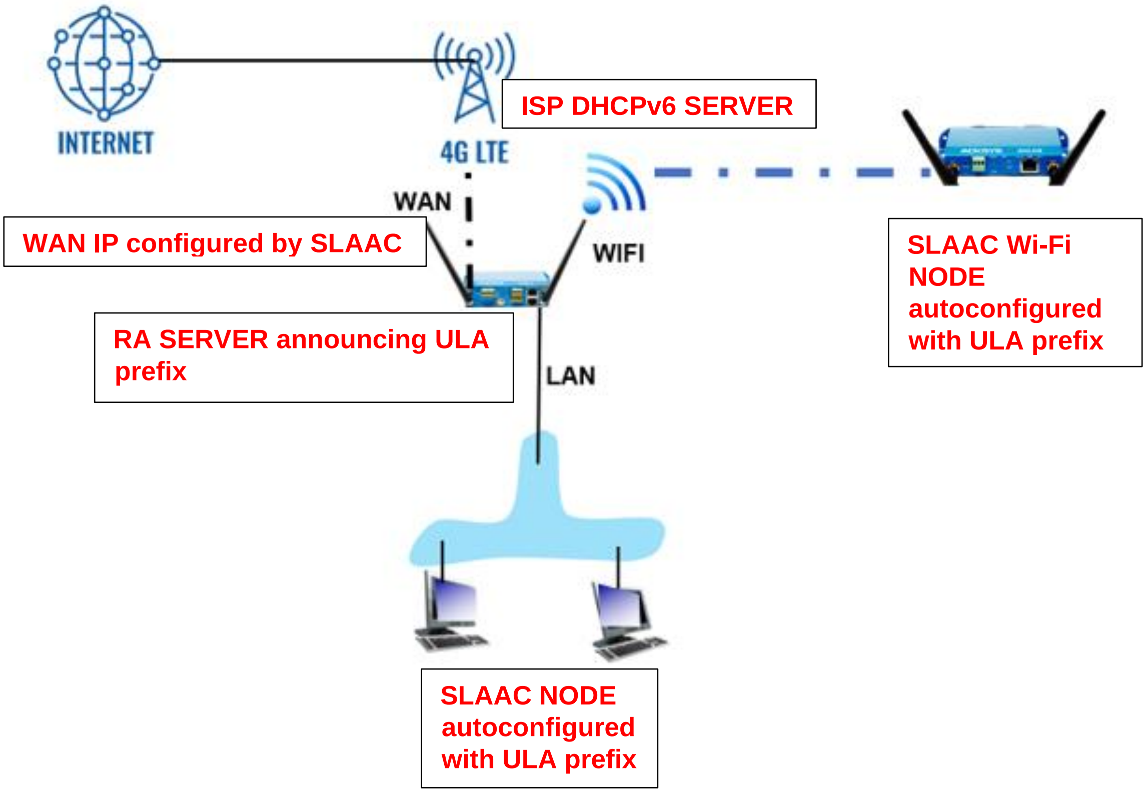
Configuration Overview and Prerequesites *in ACKSYS router*

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

- 1 Acksys AirBox cellular router in release 4.22.0.1 configured in NAT66 in routing mode
- A valid SIM card from an ISP with IPV6 features enabled
- An IPV6 client represented by an Acksys device: 1 Acksys Airlink in bridged mode or any device as dhcpv6 client supporting IPv6
- A PC to configure the Router

Configuration architecture

Just like below, the WAN Router stands as a Gateway of the local networks for internet access and will make a DHCPv6 solicitation to the ISP for a block of IPv6 addresses. The ISP in this use case, allocate /64 networks and therefore the WAN Router could not delegate this prefix to the IPV6 nodes on the local networks. So the local nodes must be autoconfigured with local address (ULA) vi RA server.


INTERNET
4G LTE
ISP DHCPv6 SERVER
WAN
WAN IP configured by SLAAC
WIFI
RA SERVER announcing ULA prefix
LAN
SLAAC Wi-Fi NODE autoconfigured with ULA prefix
SLAAC NODE autoconfigured with ULA prefix

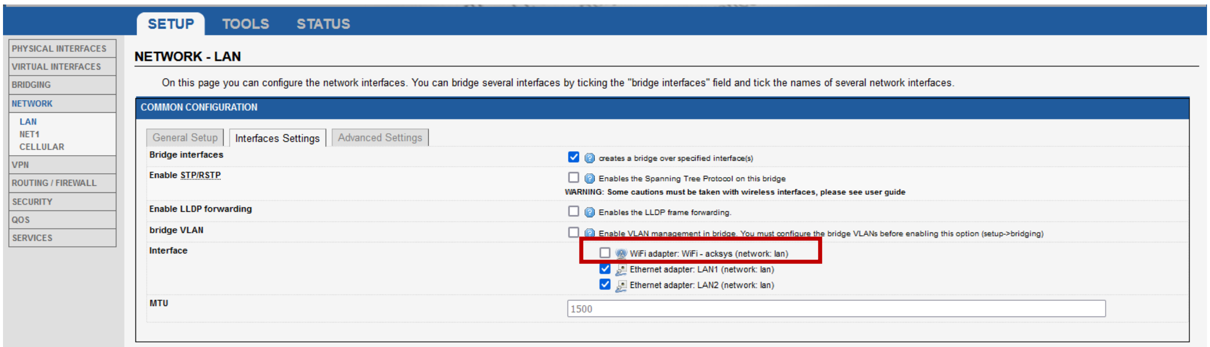
Devices configuration

If you have familiarized yourself with the configuration scheme and have all of the devices in order, we can start configuring the routers using instructions provided in this section.

Configuring WAN Router with NAT66: Airbox device

LAN interface configuration:

By default the LAN1and LAN2 interfaces are bridged with WIFI interface in case of dual LAN interfaces (Acksys Airbox or AirWan) and in this test, the WIFI Adapter will be associated to the IPv6 interface we will create later.



NETWORK - LAN

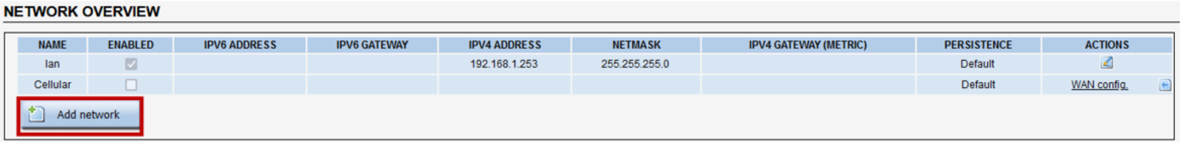
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

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 - acksys (network: lan) ☑ Ethernet adapter: LAN1 (network: lan) ☑ Ethernet adapter: LAN2 (network: lan)
MTU	1500

Wi-Fi IPV6 interface configuration (used by the RA server to distribute the ULA prefix):

Let configure Networks by login to the router's GUI and go to **Setup** → **Network**→ **Add Network**. Enter a name for the network and click the "Add" button.

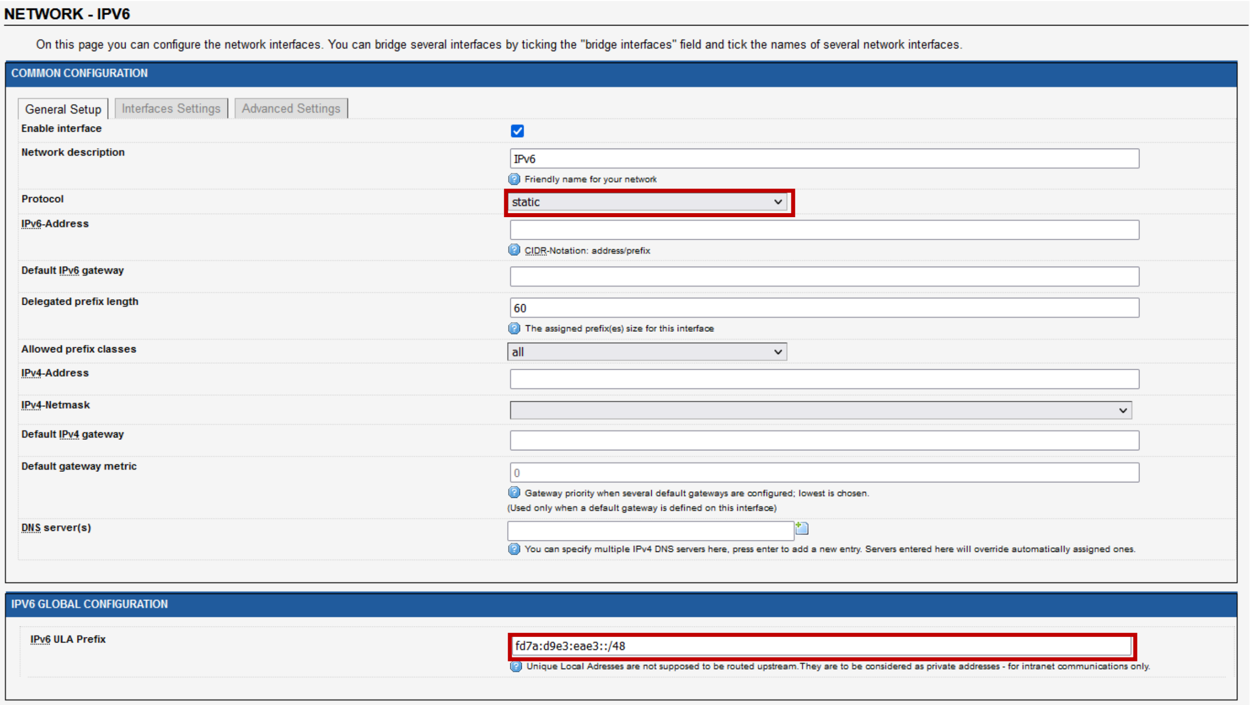


NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	☑			192.168.1.253	255.255.255.0		Default	
Cellular	☐						Default	WAN config.

You will be redirected to the Network settings window where you can add additional network IPv6. Below is screenshot of configurations IPv6 Network:

- Description interface: IPv6
- Protocol: static (to Use NAT66, the protocol must be in static with an ULA Prefix)
- Delegated prefix length: 60
- Allowed prefix classes: all
- IPv6 ULA Prefix: fd7a:dee3:eae3::/48
- Click on Save



NETWORK - IPV6

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.

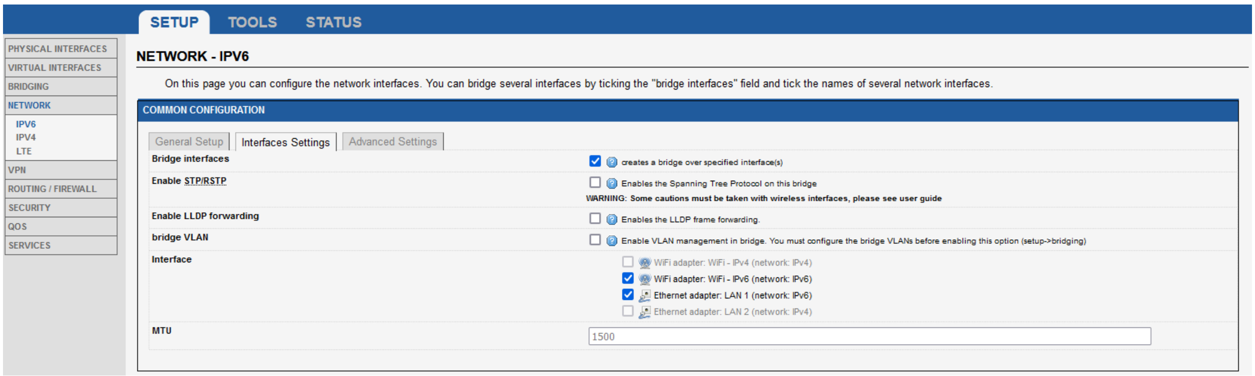
COMMON CONFIGURATION

Enable interface	☑
Network description	IPv6 Friendly name for your network
Protocol	static
IPv6-Address	 CIDR-Notation: address/prefix
Default IPv6 gateway	
Delegated prefix length	60 The assigned prefix(es) size for this interface
Allowed prefix classes	all
IPv4-Address	
IPv4-Netmask	
Default IPv4 gateway	
Default gateway metric	0 Gateway priority when several default gateways are configured; lowest is chosen. (Used only when a default gateway is defined on this interface)
DNS server(s)	 You can specify multiple IPv4 DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.

IPV6 GLOBAL CONFIGURATION

IPv6 ULA Prefix	fd7a:d9e3:eae3::/48 Unique Local Adresses are not supposed to be routed upstream. They are to be considered as private addresses - for intranet communications only.

- Edit the IPv6 network created and associated its to the WIFI adapter:



NETWORK - IPV6

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

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 - IPv4 (network: IPv4) ☑ WiFi adapter: WiFi - IPv6 (network: IPv6) ☑ Ethernet adapter: LAN 1 (network: IPv6) ☐ Ethernet adapter: LAN 2 (network: IPv4)
MTU	1500

NOTE:

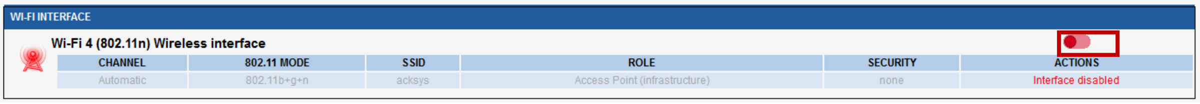
Delegated prefix length: 60 as delegated prefix length is applicable to subscriber-hosts with IPv6 Prefix assigned by the **DHCPv6 Server in SLAAC Only** (**RA server**). An IPv6 prefix is more similar to a route than it is to an IP address. The length of the prefix plays crucial role in forwarding decisions and prefix assignment through DHCPv6 pools in the local DHCPv6 server.

IPv6 ULA Prefix: Global unique prefix similar to global unicast address. Range in DHCPv6 pools IPv6 address to each device from the Router Advertisement Server and each subnet in the device will be allocated a /64 IPv6 address range from this /48 ULA range.

Configuring the AP role on the 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**.

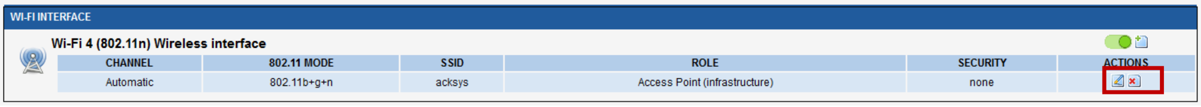


WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	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.



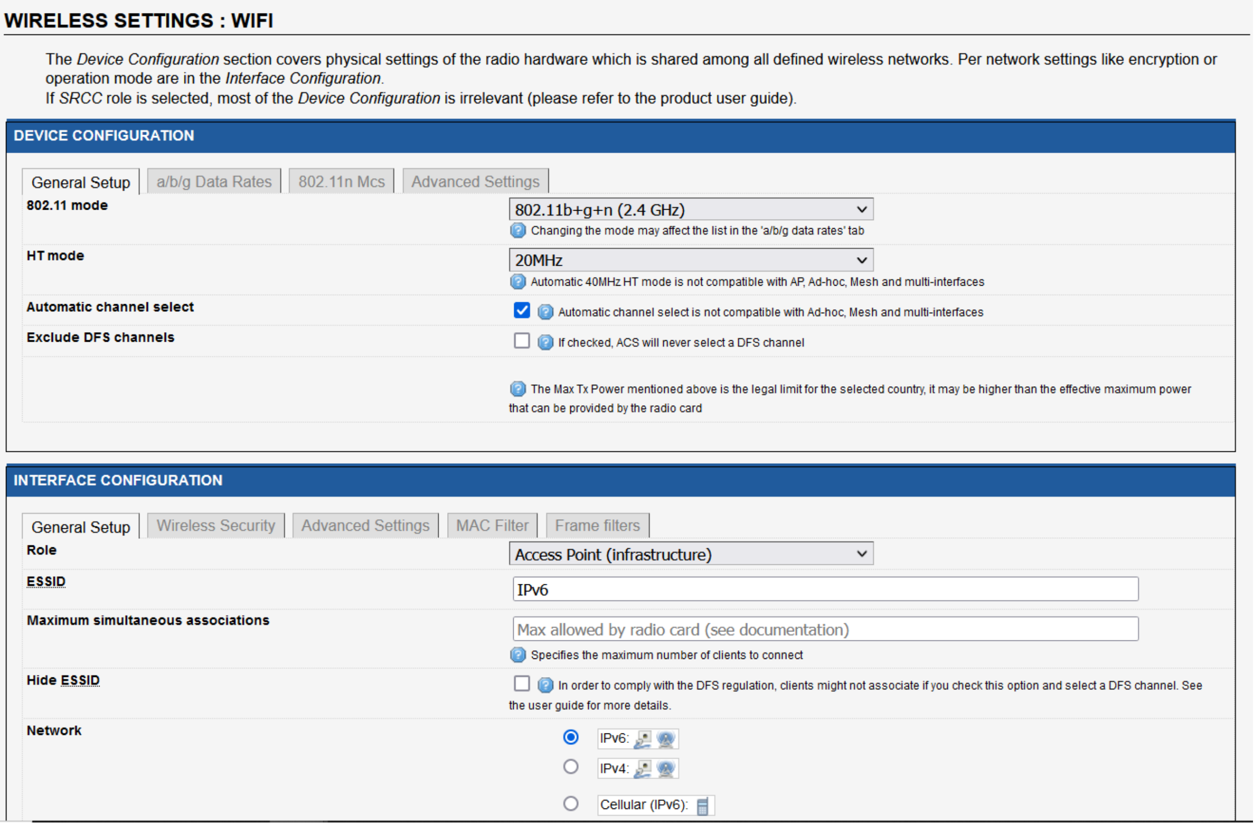
WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

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

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

- Role: Access Point
- ESSID: IPv6
- Network: IPv6
- Click on Save



WIRELESS SETTINGS : WIFI

The *Device Configuration* section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the *Interface Configuration*.
If *SRCC* role is selected, most of the *Device Configuration* is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION

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

Role: Access Point (infrastructure)

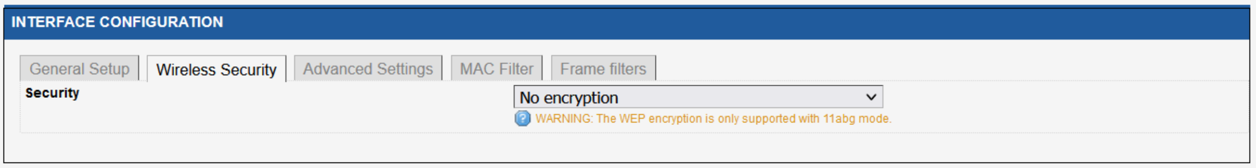
ESSID: IPv6

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:
● IPv6:
○ IPv4:
○ Cellular (IPv6):

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



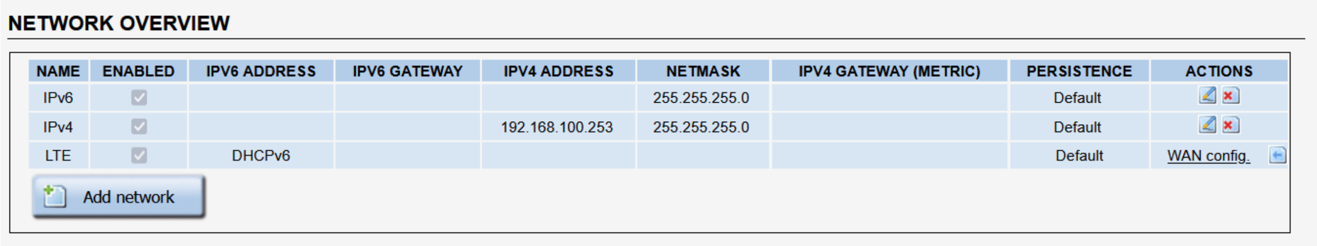
INTERFACE CONFIGURATION

Security: No encryption

WARNING: The WEP encryption is only supported with 11abg mode.

AirBox Cellular Router Network Overview:

Let have a look on the network where the WAN cellular interface is not yes configured and please do not consider in this note the network IPv4 in the screenshot below during the test.



NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
IPv6	☑				255.255.255.0		Default	
IPv4	☑			192.168.100.253	255.255.255.0		Default	
LTE	☑	DHCPv6					Default	WAN config.

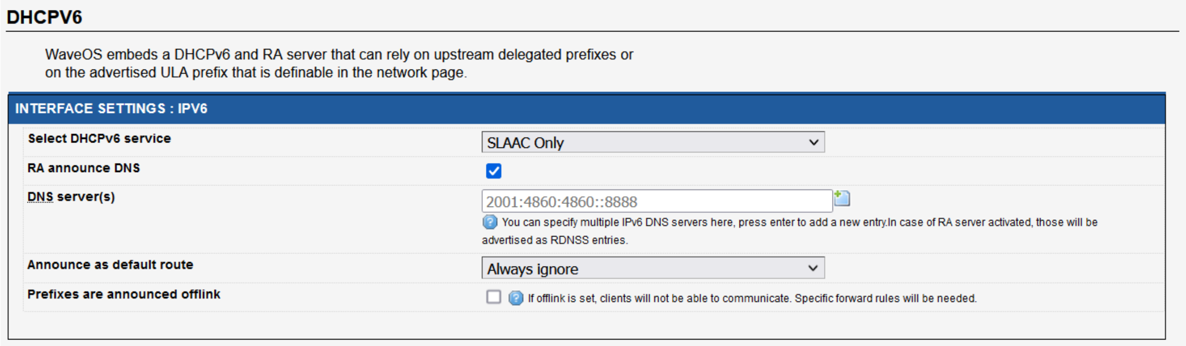
Configuring the RA server on the WAN device:

The Acksys Cellular router AirBox in AP role have different type of DHCPv6 server and in this note, DHCPv6 server is configured in SLAAC ONLY.DHCPv6 Server in SLAAC Only works as Router Advertising Server in charge of IPv6 addresses in SLAAC for End devices.

Let configure DHCPv6 Server in SLAAC Only therefore node can configure their address in SLAAC

Login to the router's WebUI **Setup** → **Services**→**DHCPv6** and enter the following information below:

- SLAAC only
- Enable RA announce DNS
- DNS Server: not to configure in order to use ISP DNS
- Announce as default route: "always ignore Always "to inform RA server not to push default gateway



DHCPV6

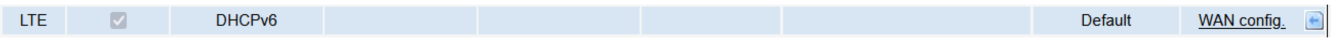
WaveOS embeds a DHCPv6 and RA server that can rely on upstream delegated prefixes or on the advertised ULA prefix that is definable in the network page.

INTERFACE SETTINGS : IPV6

Select DHCPv6 service	SLAAC Only
RA announce DNS	☑
DNS server(s)	2001:4860:4860::8888 You can specify multiple IPv6 DNS servers here, press enter to add a new entry.In case of RA server activated, those will be advertised as RDNSS entries.
Announce as default route	Always ignore
Prefixes are announced offlink	□ If offlink is set, clients will not be able to communicate. Specific forward rules will be needed.

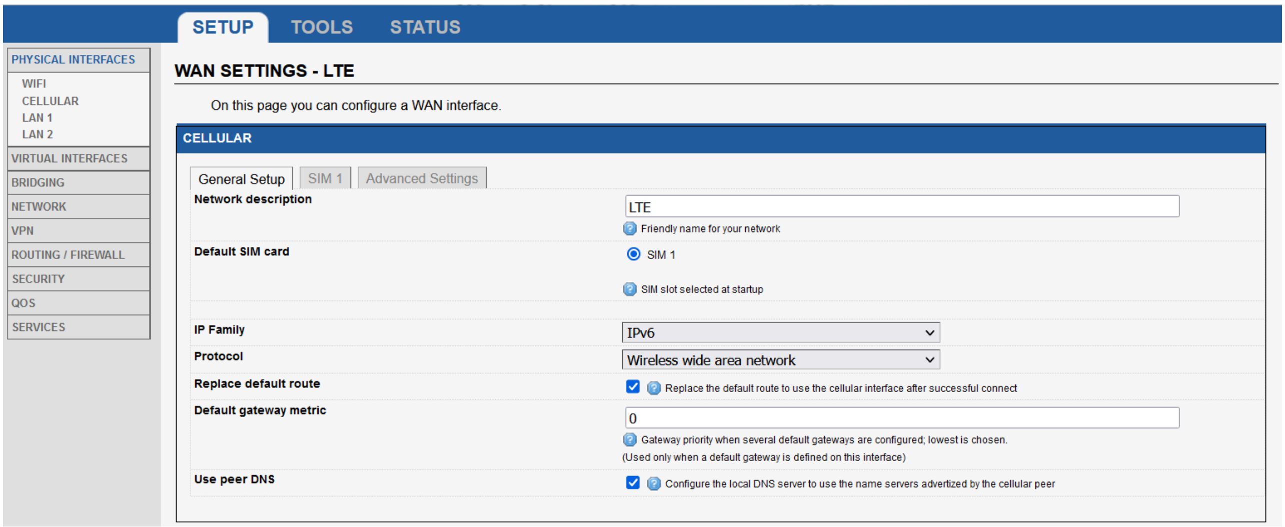
Configuring the Cellular interface:

The AirBox router is configured in AP role in router mode and by default the WAN (Cellular Interface) is in DHCPv6 node function only and dynamically will obtain IPv6 address and other configuration parameters from the ISP settings through DHCPv6 server.



LTE	☑	DHCPv6				Default	WAN config.	⇦

- Login to the router's WebUI and go to Setup →Physical Interfaces → Cellular.
  - General Setup
    - Select IPv6 in IP family
    - Check Replace default route
    - Set 0 as routing metric 0 for default gateway
    - Check Use peer DNS in case DNS is on the LAN to use the ISP DNS
    - Save



WAN SETTINGS - LTE

On this page you can configure a WAN interface.

CELLULAR

Network description: LTE
Friendly name for your network

Default SIM card: ● SIM 1
SIM slot selected at startup

IP Family: IPv6

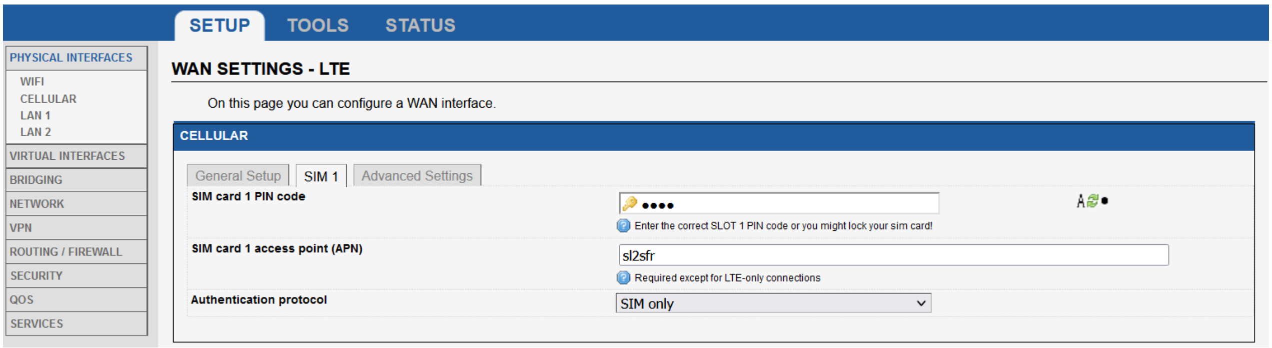
Protocol: Wireless wide area network

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

Default gateway metric: 0
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 advertized by the cellular peer

- Select the correct SIM slot (in case of dual SIM) and fill out APN with the connection information provided by the ISP (in this case sfr SIM card is used): sl2sfr



WAN SETTINGS - LTE

On this page you can configure a WAN interface.

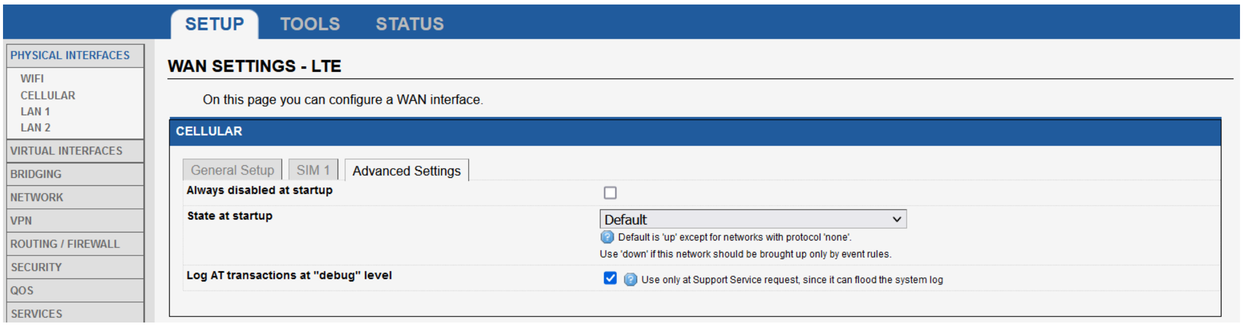
CELLULAR

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

SIM card 1 access point (APN): sl2sfr
Required except for LTE-only connections

Authentication protocol: SIM only

- Enable AT transactions logs for better understanding in troubleshoot in case of issue.
- Save and apply the config



WAN SETTINGS - LTE

On this page you can configure a WAN interface.

CELLULAR

General Setup | SIM 1 | Advanced Settings

Always disabled at startup ☐

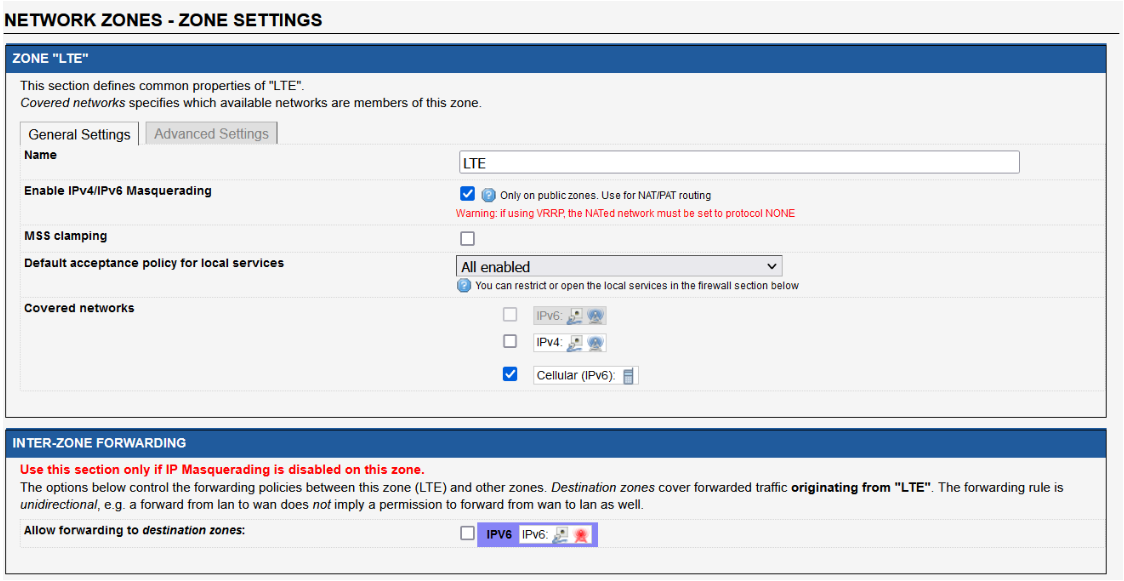
State at startup: Default
Default is 'up' except for networks with protocol 'none'.
Use 'down' if this network should be brought up only by event rules.

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

Configuring routing + NAT66 on the WAN interface:

In this note, we will configure 2 Network Zone covering 2 Network (IPv6 and LTE).
To avoid IPv6 clients node behind the Acksys Cellular router which receive IPv6 addresses but do not have Internet access, we need to enable NAT66 configured on WAN interface (cellular) to help clients to have Internet access.

- Login to the router's WebUI and go to Setup →Routing/Firewall → Network Zone → Add Network Zone.
  - LTE
    - Enable IPv6 Enable IPv4/IPv6 Masquerading
    - Save



NETWORK ZONES - ZONE SETTINGS

ZONE "LTE"

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

General Settings | Advanced Settings

Name: LTE

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

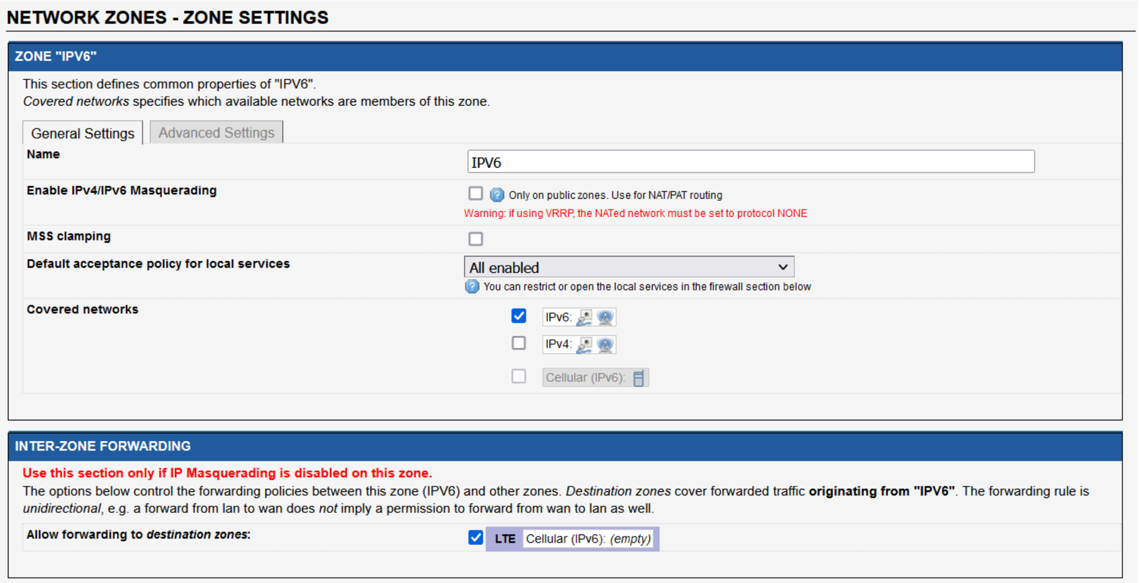
Covered networks
☐ IPv6:
☐ IPv4:
☑ Cellular (IPv6):

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 (LTE) and other zones. *Destination zones* cover forwarded traffic **originating from "LTE"**. 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*: ☐ IPV6 IPv6:

- Setup →Routing/Firewall → Network Zone → Add Network Zone.
  - IPv6
    - Do not enable IPv4/IPv6 Masquerading
    - Allow IPv6 zone to forward to LTE zone
    - Save



NETWORK ZONES - ZONE SETTINGS

ZONE "IPV6"

This section defines common properties of "IPV6".
Covered networks specifies which available networks are members of this zone.

Name	IPV6
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	☑ IPv6: □ IPv4: □ Cellular (IPv6):

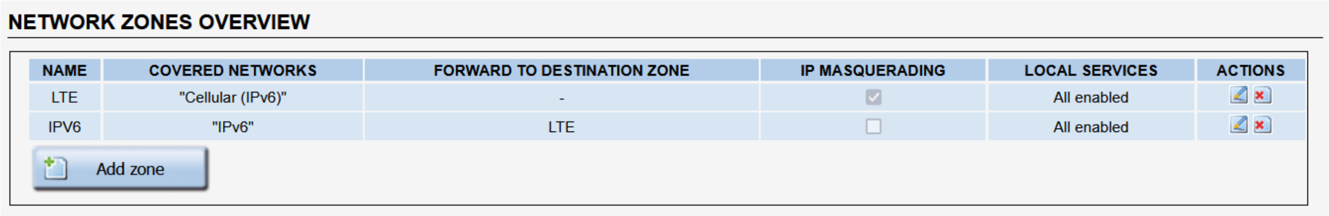
INTER-ZONE FORWARDING

Use this section only if IP Masquerading is disabled on this zone.
The options below control the forwarding policies between this zone (IPV6) and other zones. *Destination zones* cover forwarded traffic **originating from "IPV6"**. 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*: ☑ LTE Cellular (IPv6): *(empty)*

Network Zones Overview:

Let having an overview of Network zone created, LTE and IPv6.



NETWORK ZONES OVERVIEW

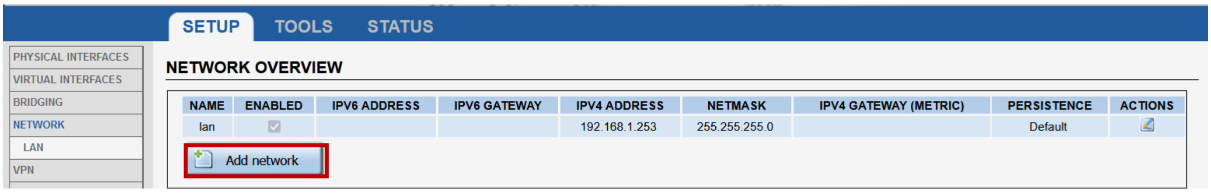
NAME	COVERED NETWORKS	FORWARD TO DESTINATION ZONE	IP MASQUERADING	LOCAL SERVICES	ACTIONS
LTE	"Cellular (IPv6)"	-	☑	All enabled	
IPV6	"IPv6"	LTE	□	All enabled	

Configuring SLAAC Wi-Fi node: Airlink

To fully understand how the IPv6 auto-addressing work, we are going to configure the client (Airlink) therefore it can be configured via SLAAC. Stateless address autoconfiguration (SLAAC) as the IPv6 type makes the operating system attempt to configure the IPv6 address for the interface from router advertisements (RA) that advertise the prefix and related information

Configuring Wi-Fi interface in SLAAC mode:

Let configure Networks by login to the router's GUI and go to **Setup → Network→ Add Network**. Enter a name for the network and click the "Add" button.



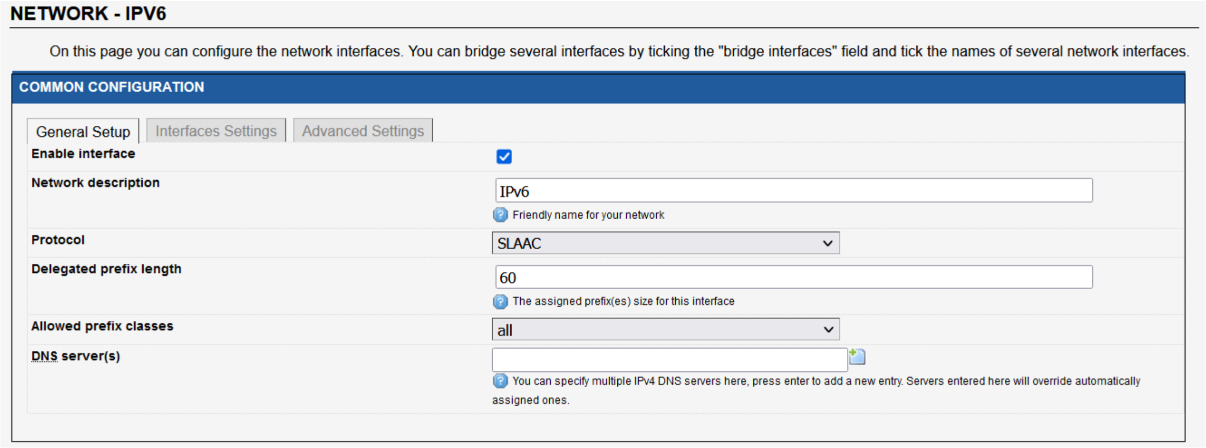
NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
lan	☑			192.168.1.253	255.255.255.0		Default	

You will be redirected to the Network settings window where you can start to add a new network (IPv6) (In this case we use SLAAC as protocol but can also be set to DHCPv6) .

Below is capture of configurations WIFI interface :

- Description interface: IPv6
- Protocol: SLAAC
- Delegated prefix length: 64
- Allowed prefix classes: all

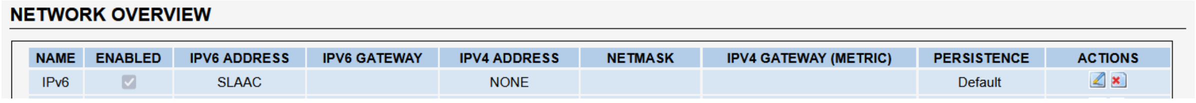


NETWORK - IPV6

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

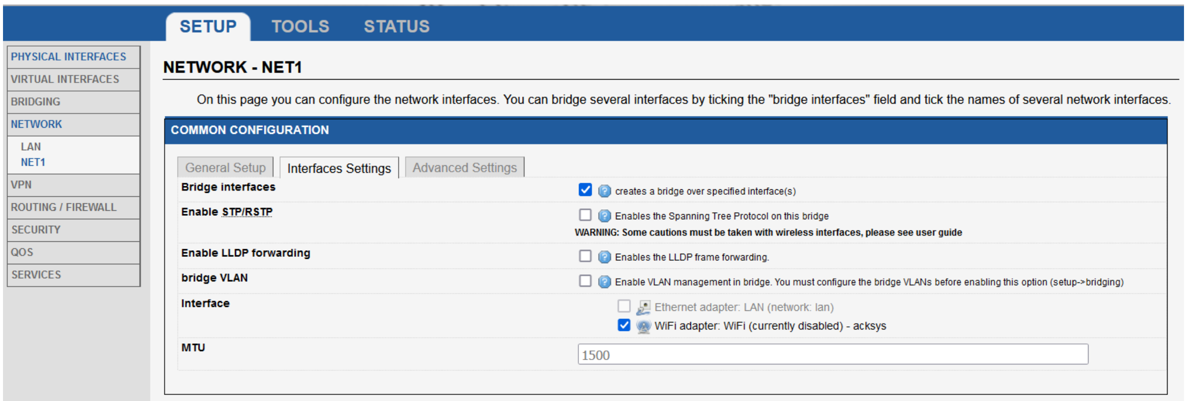
Enable interface	☑
Network description	IPv6 Friendly name for your network
Protocol	SLAAC
Delegated prefix length	60 The assigned prefix(es) size for this interface
Allowed prefix classes	all
DNS server(s)	You can specify multiple IPv4 DNS servers here, press enter to add a new entry. Servers entered here will override automatically assigned ones.



NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
IPv6	☑	SLAAC		NONE			Default	

- Edit the IPv6 network and associated to the WIFI adapter:
- Apply and save



NETWORK - NET1

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.

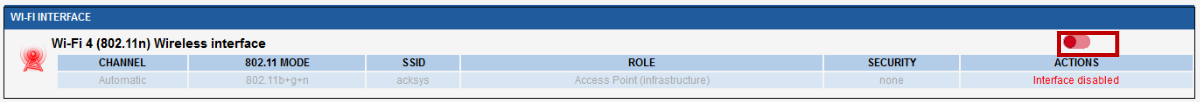
Bridge interfaces	☑ creates a bridge over specified interface(s)
Enable STP/RSTP	□ Enables the Spanning Tree Protocol on this bridge WARNING: Some cautions must be taken with wireless interfaces, please see user guide
Enable LLDP forwarding	□ Enables the LLDP frame forwarding.
bridge VLAN	□ Enable VLAN management in bridge. You must configure the bridge VLANs before enabling this option (setup->bridging)
Interface	□ Ethernet adapter: LAN (network: lan) ☑ WiFi adapter: WiFi (currently disabled) - acksys
MTU	1500

The length of a delegated prefix always be a multiple of 4. A single network at a customer site will be a /64 and user-provided IPv6 prefix for distribution to clients

Configuring Wi-Fi Node SSID:

For IPv6 Node to connect on AP, we have to configure the AP SSID

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

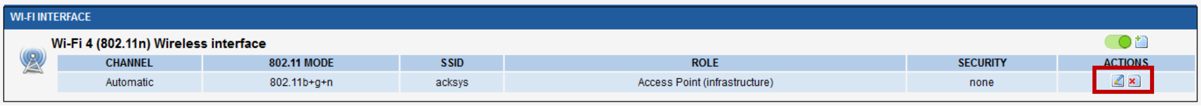


WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	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.



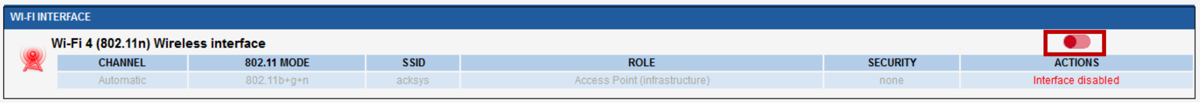
WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

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

- You will be redirected to the settings window where you can start configuring the WIFI interface. Below is capture of configurations WIFI interface:
  - ESSID: IPv6
  - Network: WIFI Interface associated to IPv6 network
  - Wireless Security: No encryption
  - Apply and save

Login the SSID on which client will be connected: in GUI and go to **Setup** → **Physical Interfaces** → **Enable the WIFI Interface**.

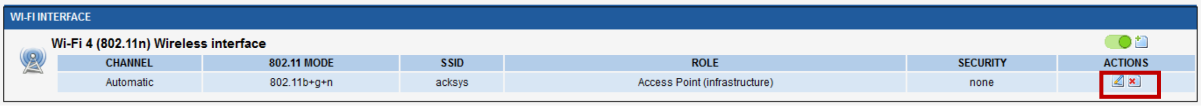


WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	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.



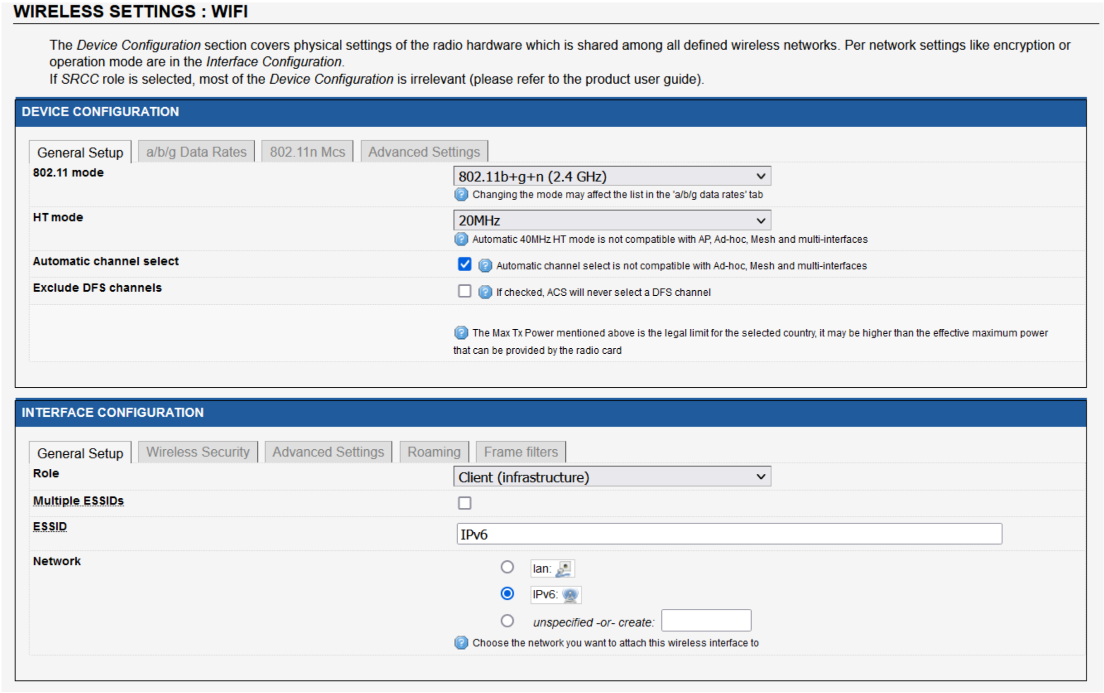
WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

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

You will be redirected to the settings window where you can start configuring the WIFI interface. Below is capture of configurations WIFI interface:

- Role: Client
- ESSID: IPv6
- Network: WIFI Interface associated to IPv6 network
- Wireless Security: No encryption
- Apply and save



WIRELESS SETTINGS : WIFI

The *Device Configuration* section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the *Interface Configuration*.
If *SRCC* role is selected, most of the *Device Configuration* is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION

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

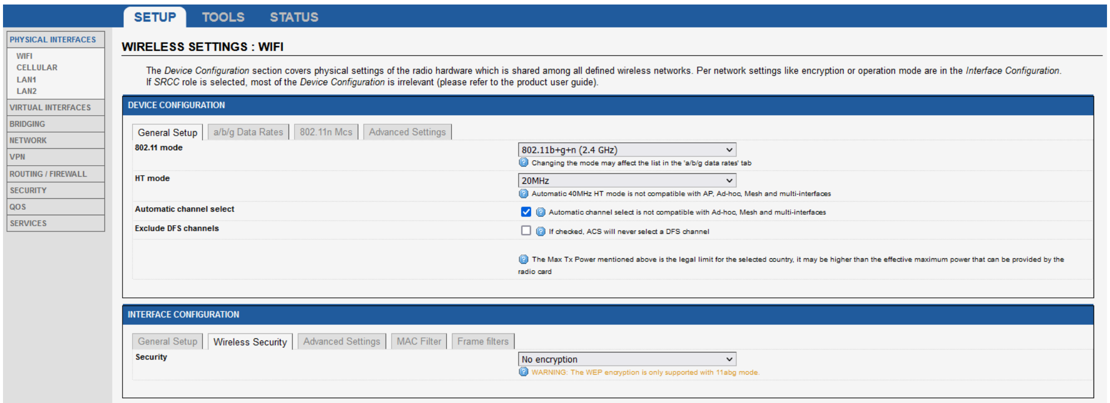
INTERFACE CONFIGURATION

Role: Client (infrastructure)

Multiple ESSIDs: □

ESSID: IPv6

Network:
○ lan:
● IPv6:
○ *unspecified -or- create:*
Choose the network you want to attach this wireless interface to



WIRELESS SETTINGS : WIFI

The *Device Configuration* section covers physical settings of the radio hardware which is shared among all defined wireless networks. Per network settings like encryption or operation mode are in the *Interface Configuration*.
If *SRCC* role is selected, most of the *Device Configuration* is irrelevant (please refer to the product user guide).

DEVICE CONFIGURATION

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

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

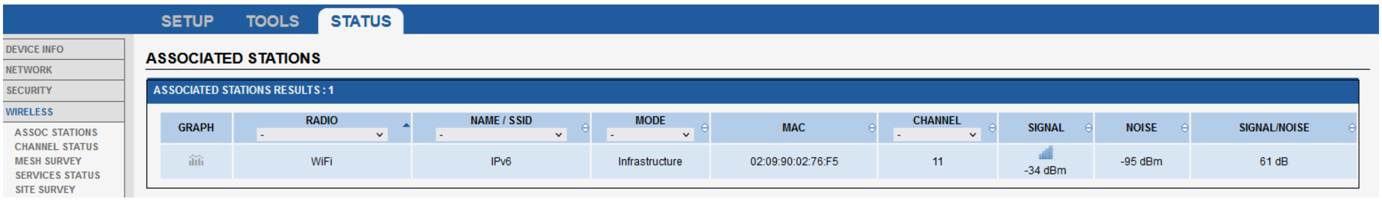
6. STATUS

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

WAN Router: Wi-Fi Status

For IPv6 Node to connect in WIFI, we can see the AirLink IPv6 node connected on the AP SSID as below :

In GUI and go to **Status** → **Wireless**



ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

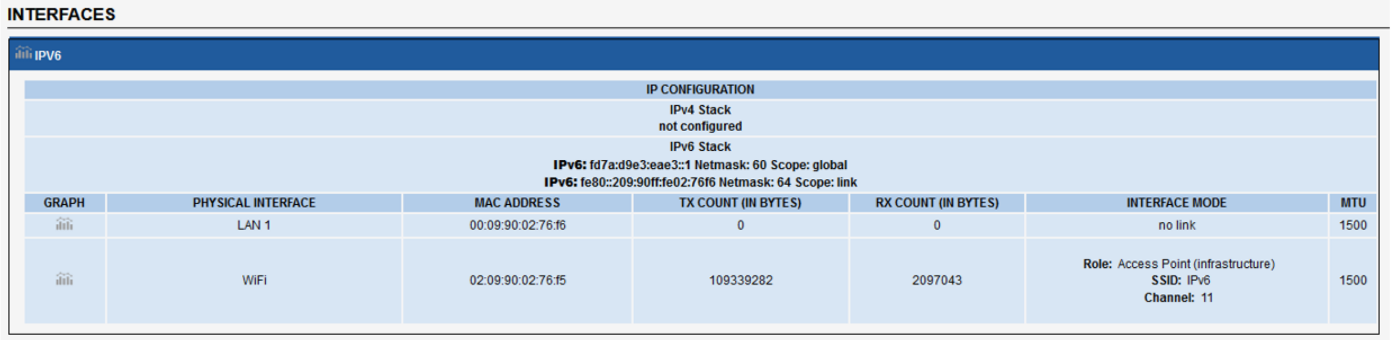
GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	-	-	-		-			
	WiFi	IPv6	Infrastructure	02:09:90:02:76:F5	11	-34 dBm	-95 dBm	61 dB

WAN Router: Network Status

To verify the connection, click in Status>Network as shown in the screenshot below and in CLI if the IPv6 address is well allocated (The IPv4 Network must not be considered in this note) and only IPv6 interface, WIFI Interface and WAN (Cellular) are concerned:

In GUI and go to **Status** → **Network: IPv6**

The network named IPv6 is autoconfigure in SLAAC with a Global Scope as shown on the below screenshot:



INTERFACES

IPV6

IP CONFIGURATION

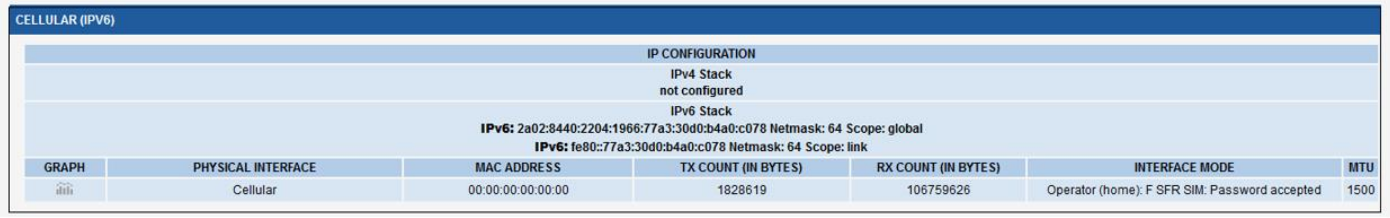
IPv4 Stack
not configured

IPv6 Stack
IPv6: fd7a:d9e3:eae3::1 Netmask: 60 Scope: global
IPv6: fe80::209:90ff:fe02:76f6 Netmask: 64 Scope: link

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	LAN 1	00:09:90:02:76:f6	0	0	no link	1500
	WiFi	02:09:90:02:76:f5	109339282	2097043	**Role:** Access Point (infrastructure) **SSID:** IPv6 **Channel:** 11	1500

In GUI and go to **Status** → **Network: WAN**

The network named WAN in DHCPv6 note is received it IPv6 address from the ISP DHCPv6 Server in SLAAC with a Global Scope as shown on the below screenshot:



CELLULAR (IPV6)

IP CONFIGURATION

IPv4 Stack
not configured

IPv6 Stack
IPv6: 2a02:8440:2204:1966:77a3:30d0:b4a0:c078 Netmask: 64 Scope: global
IPv6: fe80::77a3:30d0:b4a0:c078 Netmask: 64 Scope: link

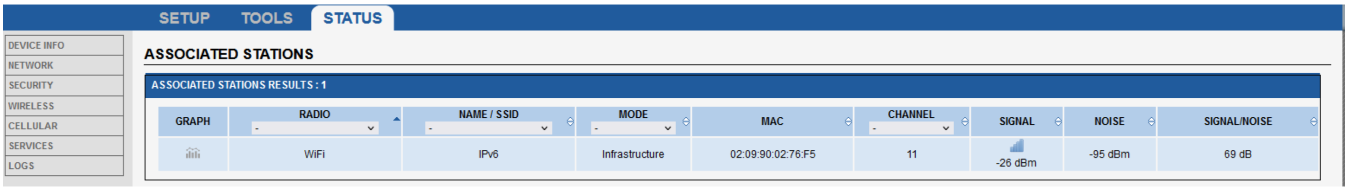
GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	Cellular	00:00:00:00:00:00	1828619	106759626	Operator (home): F SFR SIM: Password accepted	1500

IPv6 GUA assigned by the ISP: 2a02:8440:2204:1966:77a3:30d0:b4a0:c078 Netmask: 64 Scope: global

IPv6 Link local: fe80::77a3:30d0:b4a0:c078 Netmask: 64 Scope: link

SLAAC Wi-Fi node: Wi-Fi Status

If you've followed all the steps presented above, your configuration should be finished and see associated client on the AP as below:



ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	WiFi	IPv6	Infrastructure	02:09:90:02:76:F5	11	-26 dBm	-95 dBm	69 dB

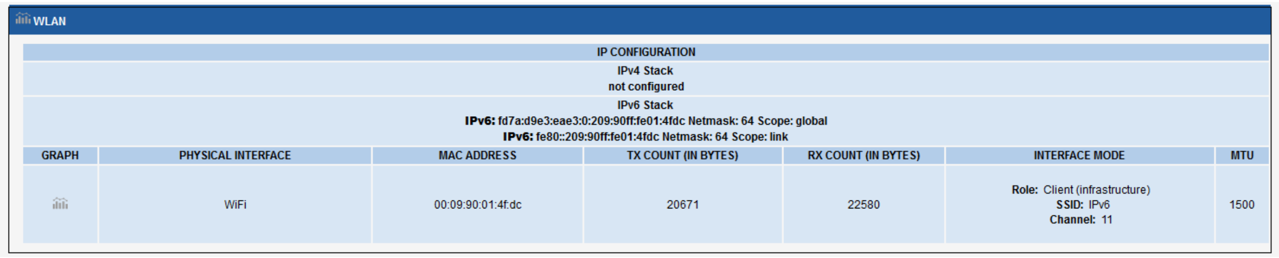
SLAAC Wi-Fi node: Network Status

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.

The Client is well associated to the access point and had received SLAAC IP address from the DHCPv6 in SLAAC only configured on the AP.

Then Go to Status → Network in order to check if the client receive IP address from AP via RA Server

To verify the network, click in Status→Network as shown in the screenshot below and in CLI if the IPv6 address is well allocated to WIFI client.

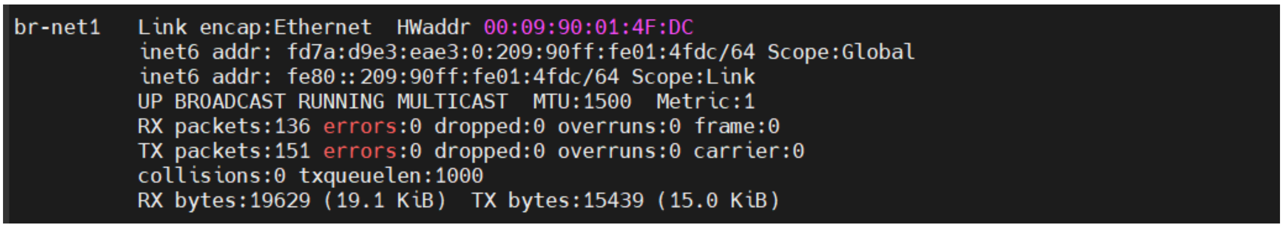


IP CONFIGURATION

IPv4 Stack
not configured

IPv6 Stack
IPv6: fd7a:d9e3:eae3:0:209:90ff:fe01:4fdc Netmask: 64 Scope: global
IPv6: fe80::209:90ff:fe01:4fdc Netmask: 64 Scope: link

GRAPH	PHYSICAL INTERFACE	MAC ADDRESS	TX COUNT (IN BYTES)	RX COUNT (IN BYTES)	INTERFACE MODE	MTU
	WiFi	00:09:90:01:4f:dc	20671	22580	**Role:** Client (infrastructure) **SSID:** IPv6 **Channel:** 11	1500



```
br-net1   Link encap:Ethernet  HWaddr 00:09:90:01:4F:DC
          inet6 addr: fd7a:d9e3:eae3:0:209:90ff:fe01:4fdc/64 Scope:Global
          inet6 addr: fe80::209:90ff:fe01:4fdc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:136 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:19629 (19.1 KiB)  TX bytes:15439 (15.0 KiB)
```

Now Airlink Router as Client IPv6 node after association with the AP (Airbox) has a global unicast address and a default gateway from the Router Advertisement Router (DHCP SLAAC only).

When the Airlink Router is connected to an IPv6 enabled network (AirBox router in AP role), the first thing it typically do is to auto-configure themselves with a link-local address use to communicate at Layer 3 with other IPv6 devices in the local segment. The most widely adopted way of auto-configuring a link-local address is by combining the link-local prefix FE80::/64 and the MAC address (**00:09:90:01:4F:DC**) of the interface as shown on the screenshot of the Airlink Network Status.

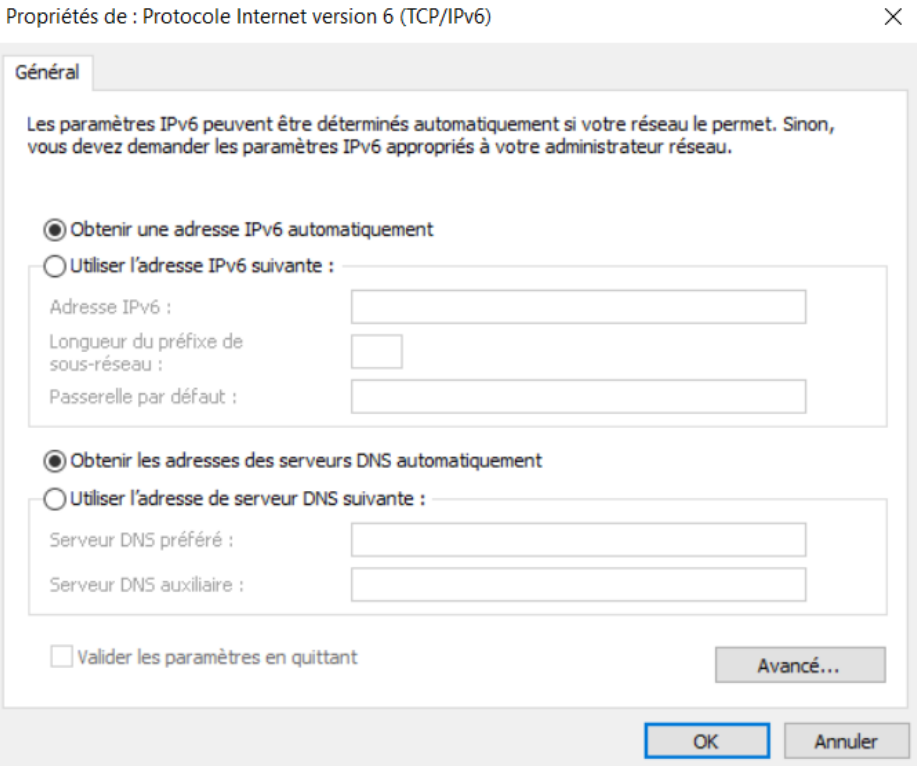
IPv6 ULA prefix autoconfigured by SLAAC: fd7a:d9e3:eae3:0:209:90ff:fe01:4fdc Netmask: 64 Scope : Global

IPv6 Link local :**fe80::209:90ff:fe01:4fdc** Netmask: 64 Scope : link

Mac Address: 00:09:90:01:4F:DC

7. Configuring IPv6 on Windows 10

In this case, Windows is configured in its IPv6 settings in an IPv6 address automatically therefore only the allocation address is done the Router Advertisements (DHCPv6 server in SLAAC only) sent by the Acksys Router AirBox in AP mode.



Propriétés de : Protocole Internet version 6 (TCP/IPv6)

Général

Les paramètres IPv6 peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IPv6 appropriés à votre administrateur réseau.

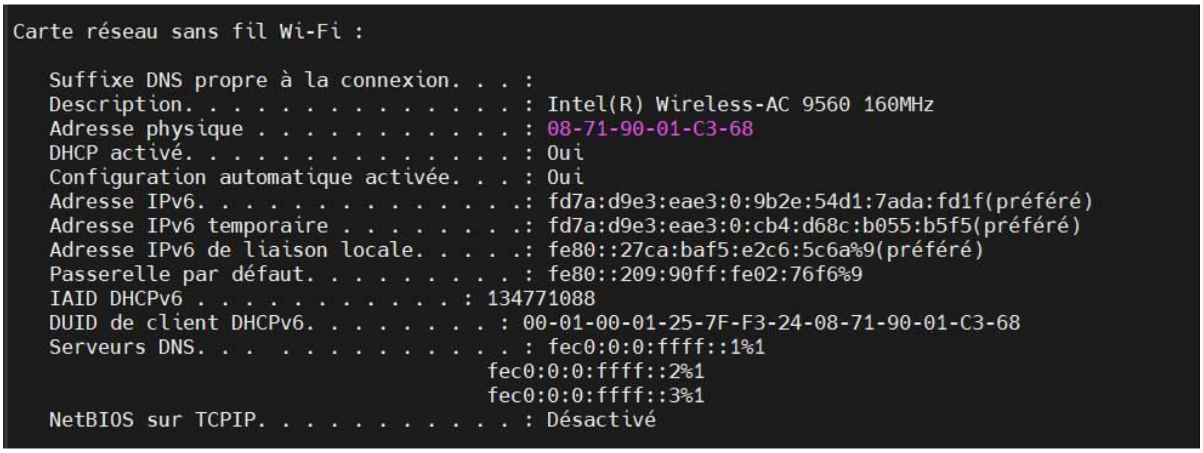
● Obtenir une adresse IPv6 automatiquement
○ Utiliser l'adresse IPv6 suivante :
Adresse IPv6 :
Longueur du préfixe de sous-réseau :
Passerelle par défaut :

● Obtenir les adresses des serveurs DNS automatiquement
○ Utiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :
Serveur DNS auxiliaire :

□ Valider les paramètres en quittant

Windows hosts used only MAC address to create Interface Identifiers (EUI-64). Globally unique address and Link-local ones were created using the segment's prefix plus the EUI-64 identifier which is generated from the physical address of the host.

Let's look at part of the output of ipconfig /all command that displays the Physical address and the Link-local address of a Windows 10 host. You can see that the MAC address is 08-71-90-01-C3-68 and therefore if Windows 10 uses EUI-64 to generate a link-local address (fe80:27ca:baf5:e2c6:5c6a%9).

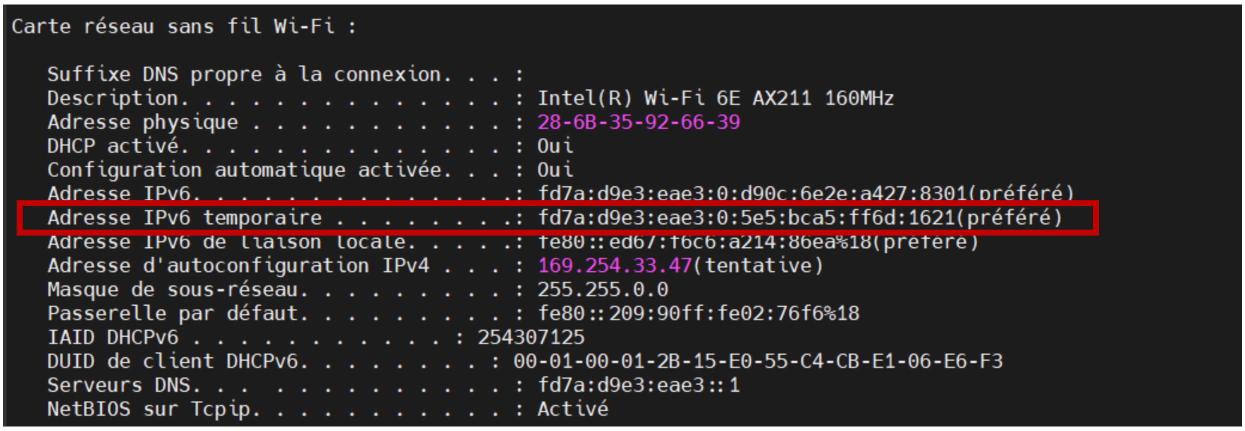


```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : Intel(R) Wireless-AC 9560 160MHz
   Adresse physique . . . . . . . . . . . : 08-71-90-01-C3-68
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6. . . . . . . . . . . . . .: fd7a:d9e3:eae3:0:9b2e:54d1:7ada:fd1f(préféré)
   Adresse IPv6 temporaire . . . . . . . .: fd7a:d9e3:eae3:0:cb4:d68c:b055:b5f5(préféré)
   Adresse IPv6 de liaison locale. . . . .: fe80::27ca:baf5:e2c6:5c6a%9(préféré)
   Passerelle par défaut. . . . . . . . . : fe80::209:90ff:fe02:76f6%9
   IAID DHCPv6 . . . . . . . . . . . : 134771088
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-25-7F-F3-24-08-71-90-01-C3-68
   Serveurs DNS. . .  . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS sur TCPIP. . . . . . . . . . . : Désactivé
```

8. Temporary IPv6 addresses

Windows devices get temporary addresses generated by SLAAC which provided a level of anonymity and of network security, this was found to be a security vulnerability.

These addresses can be randomly generated and changed over time. The IPv6 protocol for Windows creates temporary addresses for global address prefixes by default.



```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   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. . . . . . . . . . . . . .: fd7a:d9e3:eae3:0:d90c:6e2e:a427:8301(préféré)
   Adresse IPv6 temporaire . . . . . . . .: fd7a:d9e3:eae3:0:5e5:bca5:ff6d:1621(préféré)
   Adresse IPv6 de liaison locale. . . . .: fe80::ed67:f6c6:a214:86ea%18(préféré)
   Adresse d'autoconfiguration IPv4 . . . : 169.254.33.47(tentative)
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . : fe80::209:90ff:fe02:76f6%18
   IAID DHCPv6 . . . . . . . . . . . : 254307125
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2B-15-E0-55-C4-CB-E1-06-E6-F3
   Serveurs DNS. . .  . . . . . . . . . . : fd7a:d9e3:eae3::1
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

It is not generally recommend disabling temporary IPv6 addresses but it is possible to disable this temporary IPv6 addresses with the following commands and a reboot.

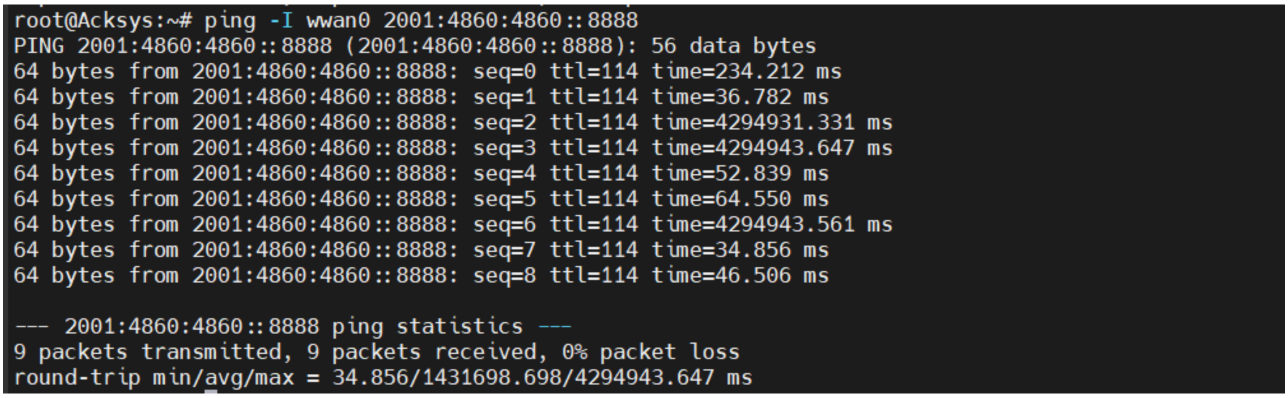
```
netsh interface ipv6 set global randomizeidentifiers=disabled

netsh interface ipv6 set privacy state=disabled
```

9. TESTING

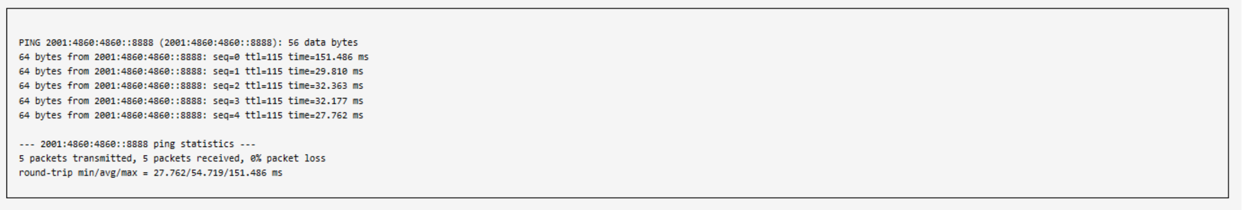
If you've followed all the steps presented above, your configuration should be finished as expected.

AirBox Router Internet Testing

Let test ICMP request to Google IPv6 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.



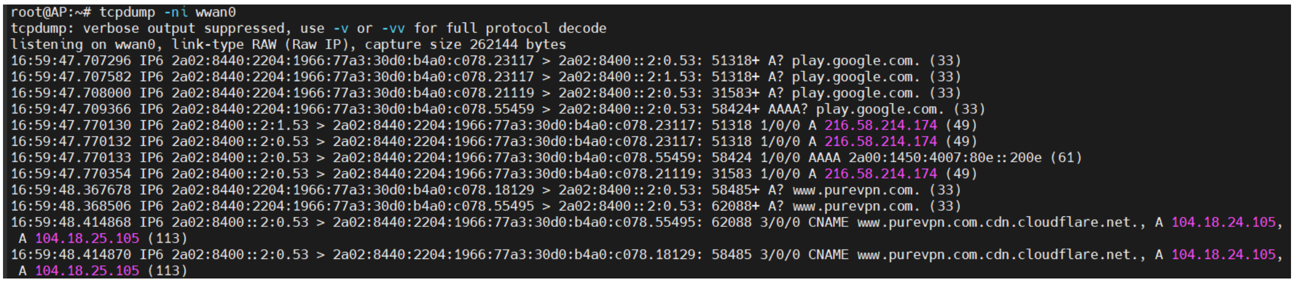
```
root@Acksys:~# ping -I wwan0 2001:4860:4860::8888
PING 2001:4860:4860::8888 (2001:4860:4860::8888): 56 data bytes
64 bytes from 2001:4860:4860::8888: seq=0 ttl=114 time=234.212 ms
64 bytes from 2001:4860:4860::8888: seq=1 ttl=114 time=36.782 ms
64 bytes from 2001:4860:4860::8888: seq=2 ttl=114 time=4294931.331 ms
64 bytes from 2001:4860:4860::8888: seq=3 ttl=114 time=4294943.647 ms
64 bytes from 2001:4860:4860::8888: seq=4 ttl=114 time=52.839 ms
64 bytes from 2001:4860:4860::8888: seq=5 ttl=114 time=64.550 ms
64 bytes from 2001:4860:4860::8888: seq=6 ttl=114 time=4294943.561 ms
64 bytes from 2001:4860:4860::8888: seq=7 ttl=114 time=34.856 ms
64 bytes from 2001:4860:4860::8888: seq=8 ttl=114 time=46.506 ms

--- 2001:4860:4860::8888 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 34.856/1431698.698/4294943.647 ms
```



```
PING 2001:4860:4860::8888 (2001:4860:4860::8888): 56 data bytes
64 bytes from 2001:4860:4860::8888: seq=0 ttl=115 time=151.486 ms
64 bytes from 2001:4860:4860::8888: seq=1 ttl=115 time=29.810 ms
64 bytes from 2001:4860:4860::8888: seq=2 ttl=115 time=32.363 ms
64 bytes from 2001:4860:4860::8888: seq=3 ttl=115 time=32.177 ms
64 bytes from 2001:4860:4860::8888: seq=4 ttl=115 time=27.762 ms

--- 2001:4860:4860::8888 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 27.762/54.719/151.486 ms
```

The ICMPv6 request to google IPv6 internet address are successful and that the setup works! but If not, we suggest to review all steps once more.

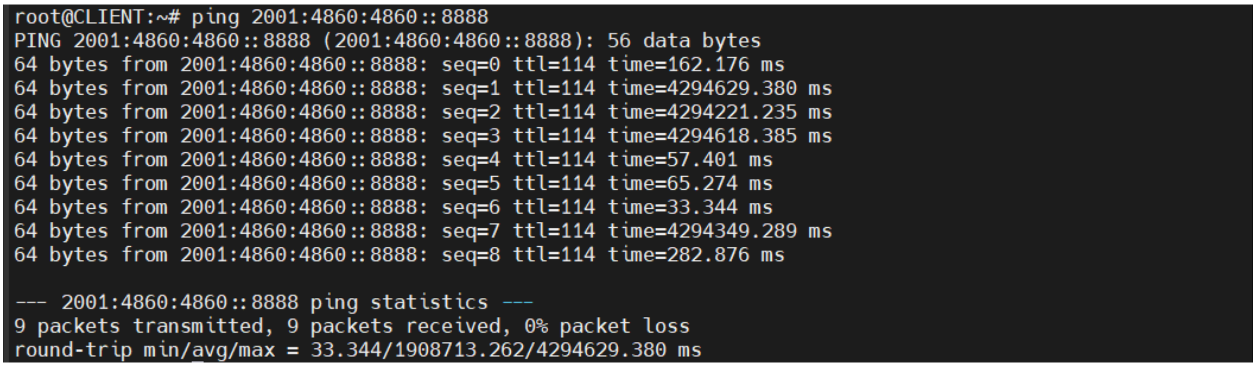
To confirm there are internet traffic via Cellular Interface WAN, a network dumps is done to analyze internet parket as shown below:



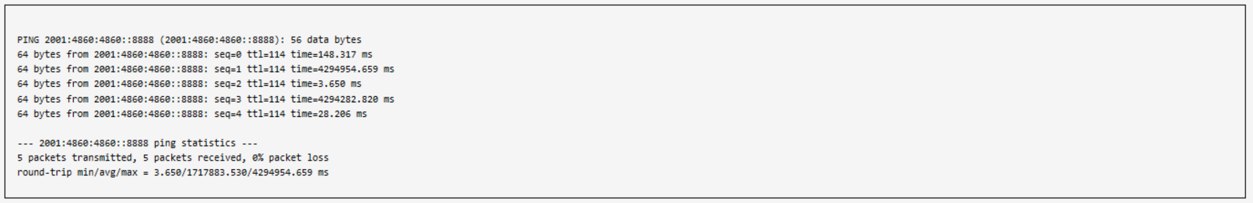
```
root@AP:~# tcpdump -ni wwan0
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wwan0, link-type RAW (Raw IP), capture size 262144 bytes
16:59:47.707296 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.23117 > 2a02:8400::2:0.53: 51318+ A? play.google.com. (33)
16:59:47.707582 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.23117 > 2a02:8400::2:1.53: 51318+ A? play.google.com. (33)
16:59:47.708000 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.21119 > 2a02:8400::2:0.53: 31583+ A? play.google.com. (33)
16:59:47.709366 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.55459 > 2a02:8400::2:0.53: 58424+ AAAA? play.google.com. (33)
16:59:47.770130 IP6 2a02:8400::2:1.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.23117: 51318 1/0/0 A 216.58.214.174 (49)
16:59:47.770132 IP6 2a02:8400::2:0.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.23117: 51318 1/0/0 A 216.58.214.174 (49)
16:59:47.770133 IP6 2a02:8400::2:0.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.55459: 58424 1/0/0 AAAA 2a00:1450:4007:80e::200e (61)
16:59:47.770354 IP6 2a02:8400::2:0.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.21119: 31583 1/0/0 A 216.58.214.174 (49)
16:59:48.367678 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.18129 > 2a02:8400::2:0.53: 58485+ A? www.purevpn.com. (33)
16:59:48.368506 IP6 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.55495 > 2a02:8400::2:0.53: 62088+ A? www.purevpn.com. (33)
16:59:48.414868 IP6 2a02:8400::2:0.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.55495: 62088 3/0/0 CNAME www.purevpn.com.cdn.cloudflare.net., A 104.18.24.105,
 A 104.18.25.105 (113)
16:59:48.414870 IP6 2a02:8400::2:0.53 > 2a02:8440:2204:1966:77a3:30d0:b4a0:c078.18129: 58485 3/0/0 CNAME www.purevpn.com.cdn.cloudflare.net., A 104.18.24.105,
 A 104.18.25.105 (113)
```

Airlink Router Internet 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 IPv6 DNS



```
root@CLIENT:~# ping 2001:4860:4860::8888
PING 2001:4860:4860::8888 (2001:4860:4860::8888): 56 data bytes
64 bytes from 2001:4860:4860::8888: seq=0 ttl=114 time=162.176 ms
64 bytes from 2001:4860:4860::8888: seq=1 ttl=114 time=4294629.380 ms
64 bytes from 2001:4860:4860::8888: seq=2 ttl=114 time=4294221.235 ms
64 bytes from 2001:4860:4860::8888: seq=3 ttl=114 time=4294618.385 ms
64 bytes from 2001:4860:4860::8888: seq=4 ttl=114 time=57.401 ms
64 bytes from 2001:4860:4860::8888: seq=5 ttl=114 time=65.274 ms
64 bytes from 2001:4860:4860::8888: seq=6 ttl=114 time=33.344 ms
64 bytes from 2001:4860:4860::8888: seq=7 ttl=114 time=4294349.289 ms
64 bytes from 2001:4860:4860::8888: seq=8 ttl=114 time=282.876 ms

--- 2001:4860:4860::8888 ping statistics ---
9 packets transmitted, 9 packets received, 0% packet loss
round-trip min/avg/max = 33.344/1908713.262/4294629.380 ms
```



```
PING 2001:4860:4860::8888 (2001:4860:4860::8888): 56 data bytes
64 bytes from 2001:4860:4860::8888: seq=0 ttl=114 time=148.317 ms
64 bytes from 2001:4860:4860::8888: seq=1 ttl=114 time=4294954.659 ms
64 bytes from 2001:4860:4860::8888: seq=2 ttl=114 time=3.650 ms
64 bytes from 2001:4860:4860::8888: seq=3 ttl=114 time=4294282.820 ms
64 bytes from 2001:4860:4860::8888: seq=4 ttl=114 time=28.206 ms

--- 2001:4860:4860::8888 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.650/1717883.530/4294954.659 ms
```

10. Common issue on Android Devices

Some android devices or even other brands, may not accept ULA address for internet connection, as ULA should not be natively routable on internet, despite NAT66 allowing internet access.

11. Annex : How SLAAC Work

NDP uses four messages types to support SLAAC procedures:

Upon connection to a network, a device uses a Router Solicitation Message (RS) to contact the network gateway router.

- The router responds with a Router Advertisement (RA) bearing the 64-bit prefix of the network. It should be noted that RAs are also periodically broadcasted by the gateway regardless of solicitations from network members.
- Upon receipt of an RA, the connecting device generates a 64-bit host identifier either randomly or from the Media Access Control (MAC) address associated with its network interface. This identifier is then appended to the network prefix obtained from the router to form a tentative 128-bit IPv6 address for the host.
- In order to verify the uniqueness of the generated address within the network, the device must perform the Duplicate Address Detection (DAD) procedure. It issues a Neighbor Solicitation (NS), a message that is used in IPv6 networks to query for the MAC address of a target host given its IPv6 address.

When used in SLAAC procedures, a device sends this message querying for its own IPv6 address.

This effectively tests for the presence of another device on the network that may accidently have the same IP address. If there is no reply to the query, then the device assumes that the generated address is unique and proceeds to use it for communication.

If it is not unique, the existing host bearing the same address returns a Neighbor Advertisement (NA) message; and the device must repeat the address generation and DAD process.