ACKSYS
COMMUNICATIONS & SYSTEMS

APPLICATION NOTE

APNUS38 How to Configure External radius authentication on ACKSYS Router

February 2024

Content

1. Radius Glossary and Term

Radius – Remote Authentication Dial-In User Service.

EAP – Extensible Authentication Protocol.

NAS – Network Access Server.

MSCHAPv2- Microsoft Challenge Handshake Authentication Protocol version 2

AAA - Authentication, Authorization, Accounting.

LDAP - Lightweight Directory Access Protocol.

AP –Access Point

IPv4 – Internet Protocol Version 4.

EAPOL – Extensible Authentication Protocol Over Lan

PEAP - Protected Extensible Authentication Protocol

SSID- Service Sed Id

ICMP- Internet Control Protocol

LAN- Local Area Network

2. Introduction

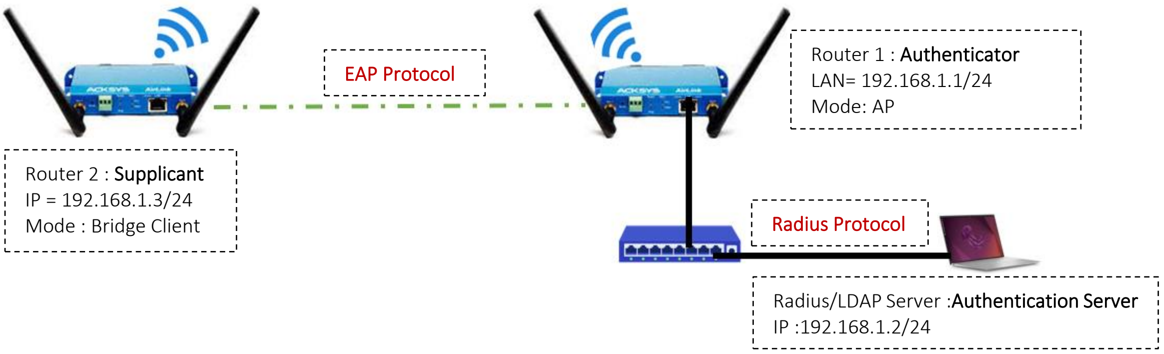
Radius stands for Remote Authentication Dial In User Service, becomes more and more important for WIFI network security. The radius is the centralized server used for the authentication, accounting, and authorization of a user in different user cases.

The Acksys Router in the AP role, can be configured as a RADIUS Client compatible with RADIUS server. Radius authentication protocol, such as EAP, can grant or deny user access, based on the responses from the server to a range of services (including Wi-Fi, VPN, and applications etc...).

In this application note, we will explain in detail the basic steps required to configure Acksys Router as Radius Authenticator (NAS) for an external radius authentication.

3. Radius Authentication Architecture

In this application note, we will use 2 Acksys Routers, one as Supplicant (Bridge Client) and other as Authenticator (AP) connected to an external radius server which embedded the Ldap Server within the same layer-2 broadcast domain to avoid routing or authentication delays.



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 :

- 2 AirLink routers or Any type of Acksys Router
  - 1 Airlink Router configured in WIFI AP Mode as authenticator
  - 1 Airlink Router configured in Bridge Client as Supplicant
- A switch to connected the Authenticator and the Radius server
- Laptop to configure the routers
- An external Radius Server embedding the user database and containing the credentials and user information needed for the RADIUS authentication

4. Radius Server Configuration and requirements

There are many radius server distributed on Linux and Windows with their RADIUS options which should work with ACKSYS access points if configured correctly.

In this Application note, we will use an external authentication server (radius and Ldap) solution and please refer to your RADIUS server documentation for specifics.

The key requirements for WPA2-Enterprise with Acksys are as follow:

- The server must host a certificate from a Certificate Authority (CA) trusted by clients on the network.
- All Access Points broadcasting the WPA2-Enterprise SSID must be configured as RADIUS clients/ authenticators on the radius server with a shared secret.
- The RADIUS server must have a user base or any Ldap server to authenticate against.
- The RADIUS server must support the same EAP authentication as the Wi-Fi bridged client (ex: PEAPv2 for our test)

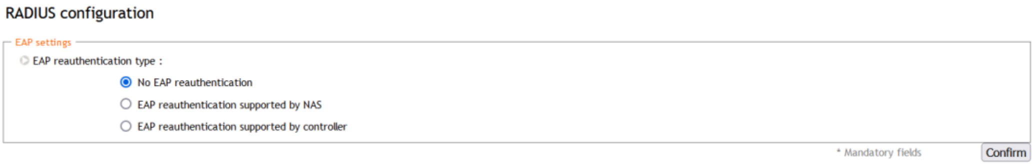
Adding AP as Radius Client(Authenticator) on Radius

In this application note, access points communicate with bridged clients and receive their credentials. Then the access point forwards these credentials to the Radius Server.

Before we configure our Acksys Router to use a RADIUS authentication server, we must have this information for our RADIUS server :

- **Shortname** — Name to identify your NAS (Use your custom name)
- **An external RADIUS server** — 192.168.1.2 (IP address and RADIUS port)
- **Shared secret** — acksys (Case-sensitive password that is the same on the Acksys and the RADIUS server)
- **Authentication methods** — Set your RADIUS server to allow the authentication method your device uses: ex: WPA2 Enterprise
- **Authorized subnet or IP address** — The authenticator IP address authorized to contact the radius server

Example of Radius Server configuration:

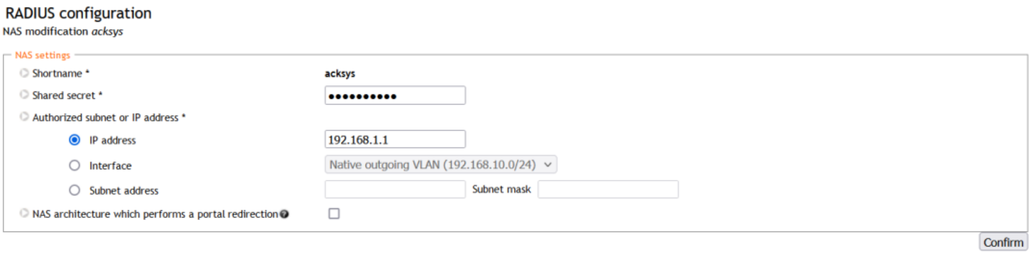


RADIUS configuration

EAP settings

EAP reauthentication type :

● No EAP reauthentication
○ EAP reauthentication supported by NAS
○ EAP reauthentication supported by controller



RADIUS configuration

NAS modification *acksys*

NAS settings

Shortname * acksys

Shared secret * ••••••••••

Authorized subnet or IP address *

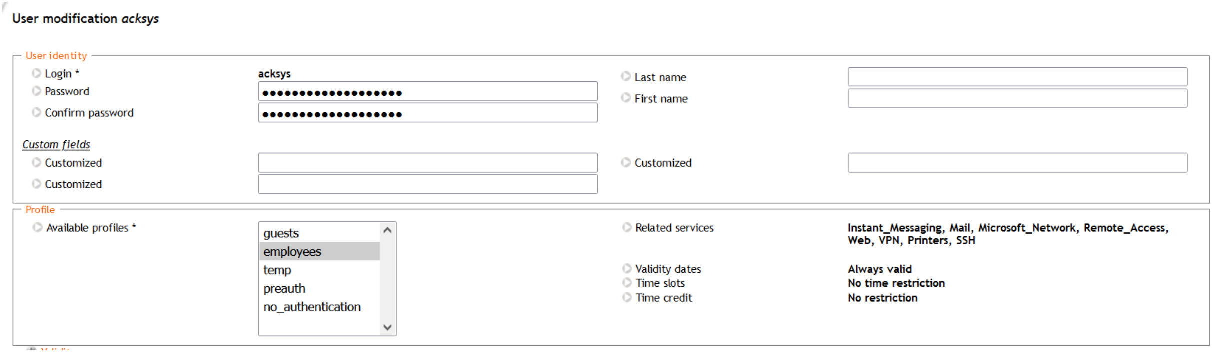
● IP address 192.168.1.1
○ Interface Native outgoing VLAN (192.168.10.0/24)
○ Subnet address Subnet mask

NAS architecture which performs a portal redirection □

Adding User on Radius Server

The Ldap Server Is embedded on the Radius Server as explained early therefore no need to create a separated external LDAP server.

- **User Database**
  - The user database contains the credentials and user information needed for the RADIUS server to perform authentication and authorization for the user. In this test, the Ldap is embedded in the Radius server



User modification *acksys*

User identity

Login * acksys

Password •••••••••••••••••••

Confirm password •••••••••••••••••••

Last name

First name

Custom fields

Customized

Customized

Customized

Profile

Available profiles *: guests, employees, temp, preauth, no_authentication

Related services: Instant_Messaging, Mail, Microsoft_Network, Remote_Access, Web, VPN, Printers, SSH

Validity dates: Always valid

Time slots: No time restriction

Time credit: No restriction

5. ACKSYS Router configuration

Let keeping in mind that all Acksys routers are compatible with Radius Server as Authenticator and Supplicant, but are not responsible for wireless clients authentication. The AP acts only as an intermediary between clients and the RADIUS server.

Configuring Authenticator Router1 in AP role

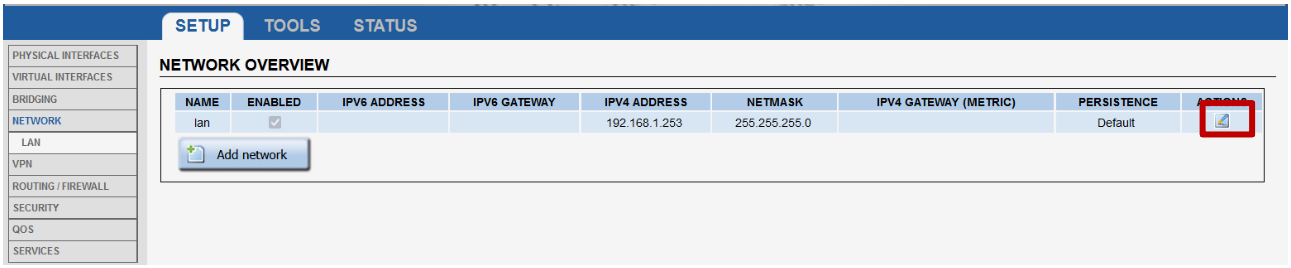
If you have familiarized yourself with the configuration scheme, we can start configuring the router using instructions provided.

Networks	AirLink Router 1: Authenticator
	IP: 192.168.1.1/24
Mode: AP	SSID:RADIUS Authentication Methods: WPA2/enterprise
Radius	IP:192.168.1.2/24 Radius Port:1812 Share Secret: Testing123

Configuring Authenticator Network Interface

In this section, we will create modify the default Network according to our network scope in Bridged Mode.

In the GUI, go to Setup → Physical Interfaces → Edit LAN Interface to create the LAN Network

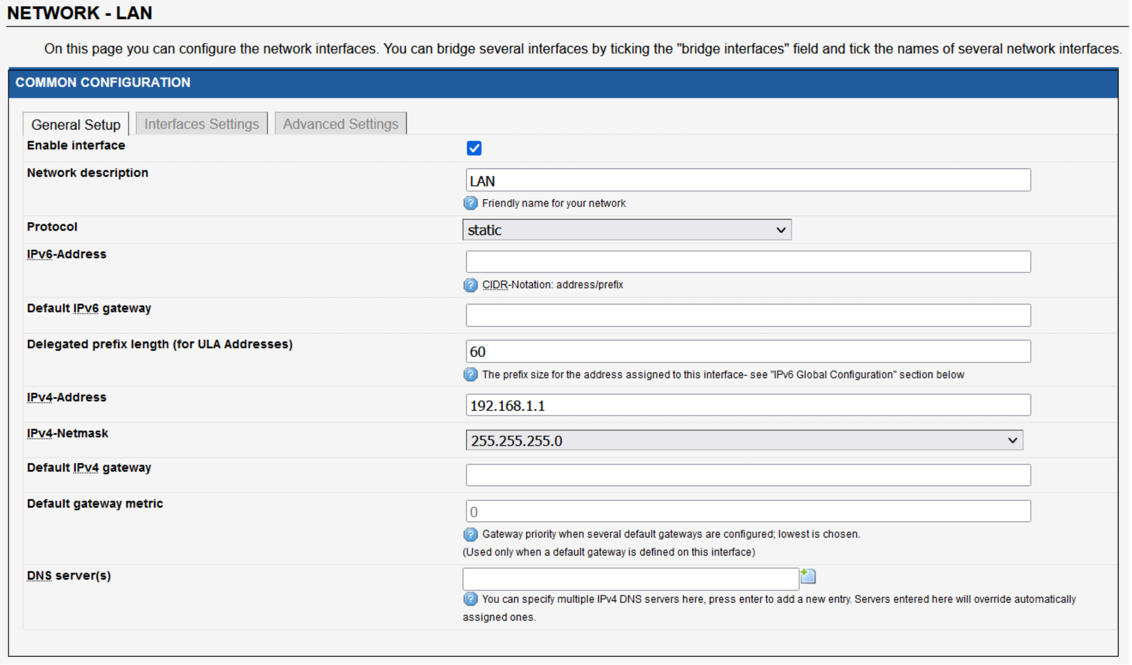


NETWORK OVERVIEW

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

Click the "Edit" button located to the right and configure the Alias IP address used to configure the LAN Interface.

- General Setup
  - Network description :WLAN (use your custom name)
  - Protocol: Static
  - IPv4-Address : 192.168.1.1
  - IPv4 Netmask:255.255.255.0
  - Save



NETWORK - LAN

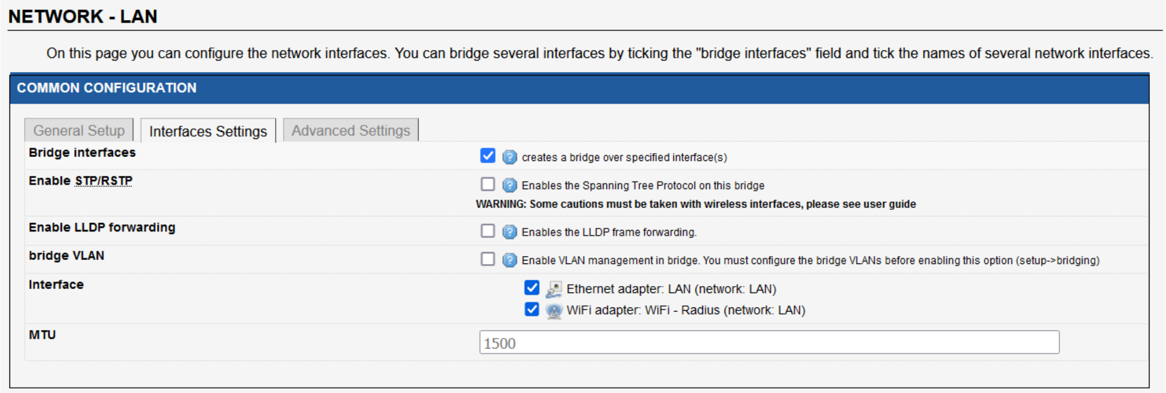
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

COMMON CONFIGURATION

General Setup | Interfaces Settings | Advanced Settings

Enable interface	☑
Network description	LAN Friendly name for your network
Protocol	static
IPv6-Address	 CIDR-Notation: address/prefix
Default IPv6 gateway	
Delegated prefix length (for ULA Addresses)	60 The prefix size for the address assigned to this interface- see "IPv6 Global Configuration" section below
IPv4-Address	192.168.1.1
IPv4-Netmask	255.255.255.0
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.

- Interface Settings
  - Bridge Interfaces: enable
  - Interface: Tick Ethernet Adapter and WiFI Adaptor
  - Click Save



NETWORK - LAN

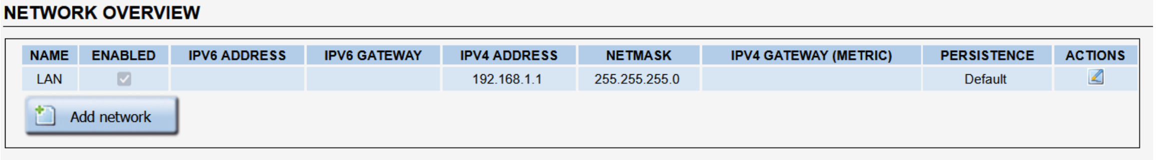
On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and tick the names of several network interfaces.

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	☑ Ethernet adapter: LAN (network: LAN) ☑ WiFi adapter: WiFi - Radius (network: LAN)
MTU	1500

After modifying the default network, we should have the result below:

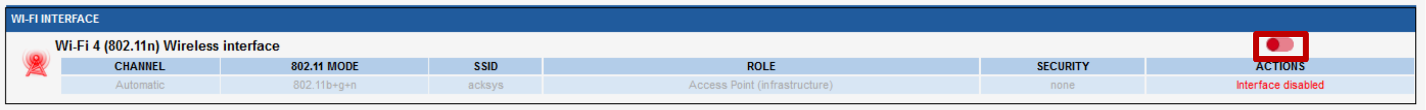


NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LAN	☑			192.168.1.1	255.255.255.0		Default	✎

Configuring Authenticator Secure SSID

By default the WiFI Adaptor is disabled therefore in this application note, we will create an SSID to associate to the WIFI adapter to allow end device in client mode to connect on its .
In the GUI, go to Setup → Physical Interfaces → Click WiFI Adaptor to On

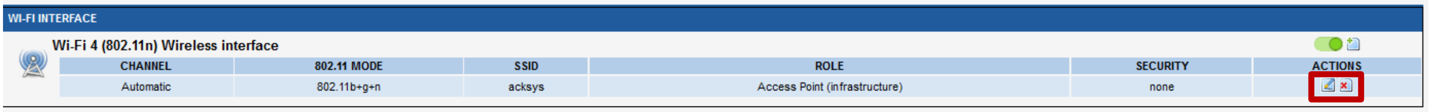


WI-FI INTERFACE

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 your SSID configuration page:

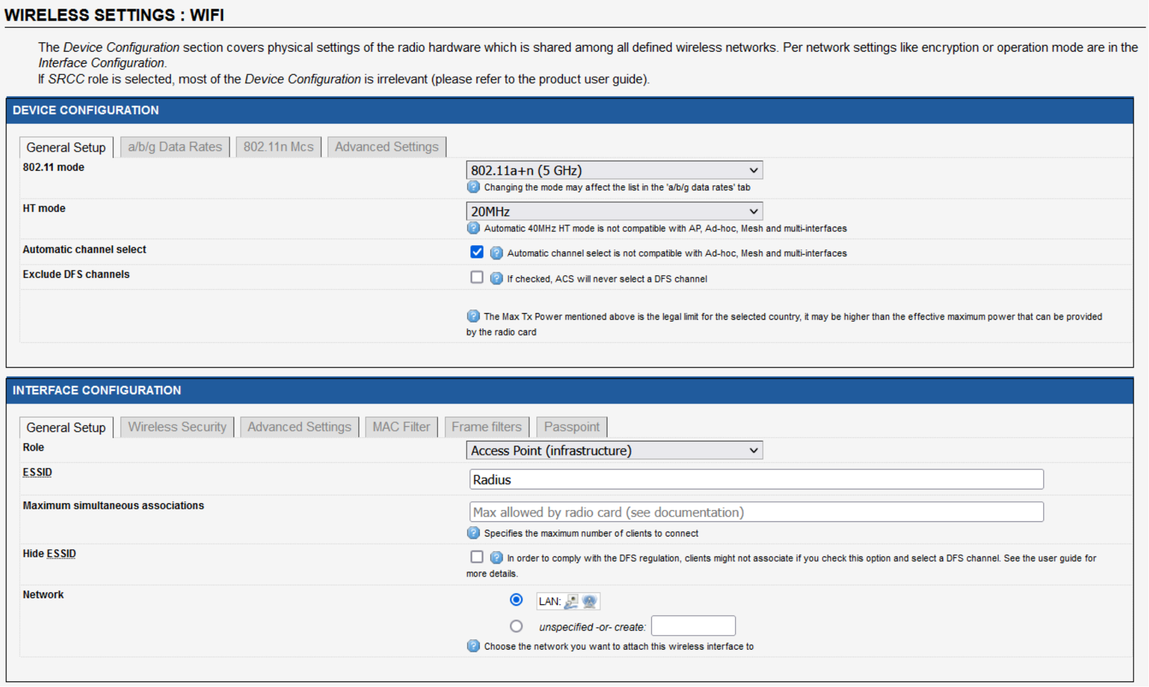


WI-FI INTERFACE

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	

  - Role: Access Point
  - ESSID: Radius
  - Network: LAN
  - 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: 802.11a+n (5 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)

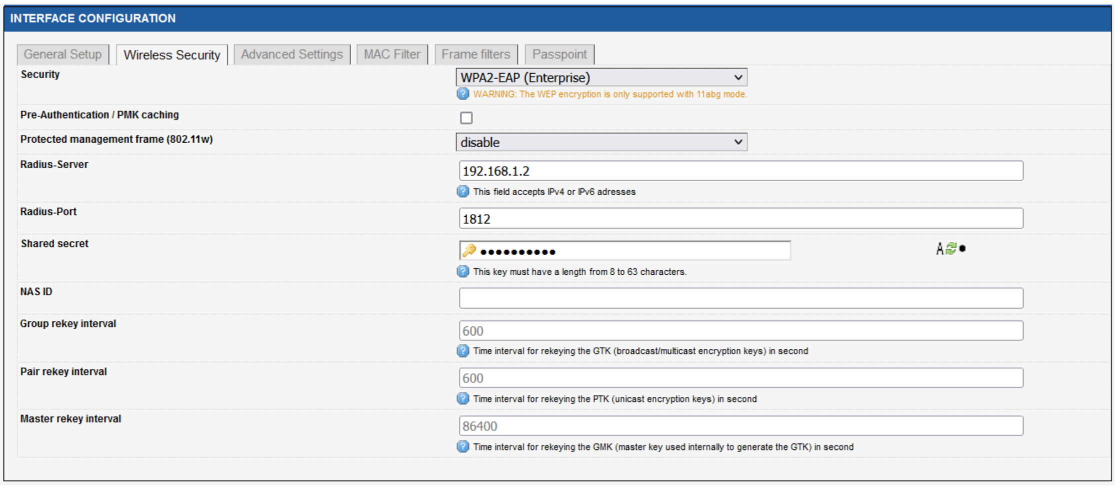
ESSID: Radius

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

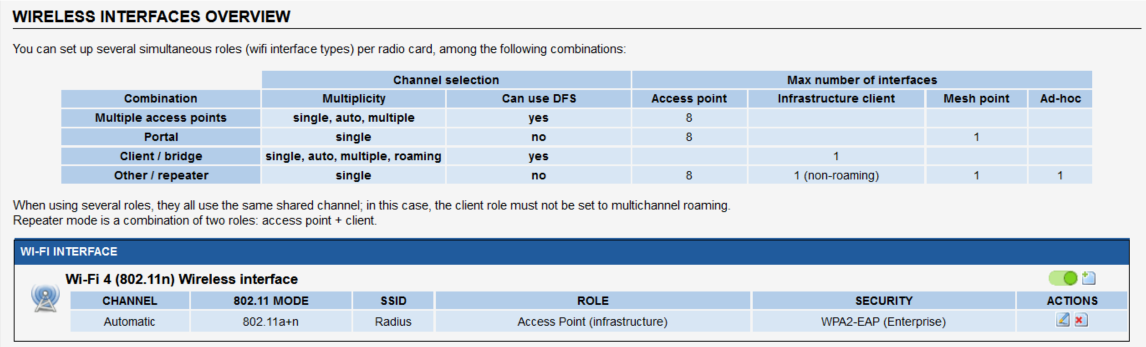
- Wireless Security
  - WPA2-EAP (Enterprise)
  - Radius Server: 192.168.1.2
  - Radius-Port: 1812
  - Shared secret: Use the same secret configured on Radius server
  - Click Save and Apply



INTERFACE CONFIGURATION

Security	WPA2-EAP (Enterprise) WARNING: The WEP encryption is only supported with 11abg mode.
Pre-Authentication / PMK caching	□
Protected management frame (802.11w)	disable
Radius-Server	192.168.1.2 This field accepts IPv4 or IPv6 adresses
Radius-Port	1812
Shared secret	•••••••••• This key must have a length from 8 to 63 characters.
NAS ID	
Group rekey interval	600 Time interval for rekeying the GTK (broadcast/multicast encryption keys) in second
Pair rekey interval	600 Time interval for rekeying the PTK (unicast encryption keys) in second
Master rekey interval	86400 Time interval for rekeying the GMK (master key used internally to generate the GTK) in second

After modifying the default WIFI parameter, we should have the result below:



WIRELESS INTERFACES OVERVIEW

You can set up several simultaneous roles (wifi interface types) per radio card, among the following combinations:

	Channel selection		Max number of interfaces			
Combination	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.

WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
Automatic	802.11a+n	Radius	Access Point (infrastructure)	WPA2-EAP (Enterprise)	

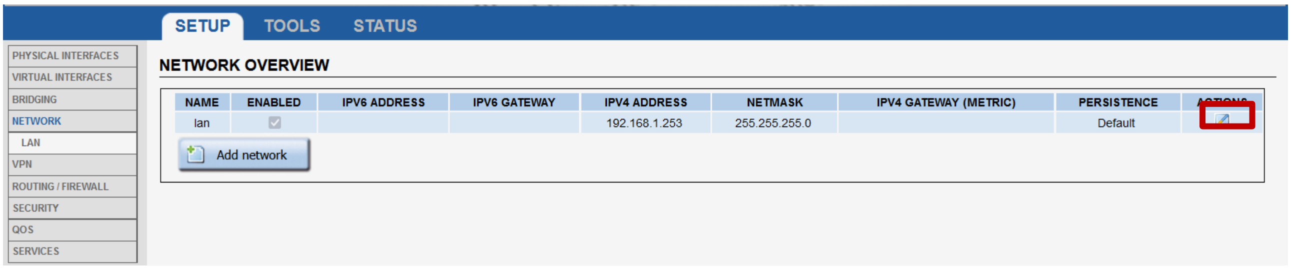
Configuring Supplicant Router1 in Bridge Client role

The Authentication configuration is similar with the supplicant with some specific with the following instructions.

Networks	AirLink Router 2: Supplicant
	IP: 192.168.1.3/24
Mode: Bridge Client	SSID:Radius Authentication Methods: PEAPv2
Radius	Share Secret:Testing123 User Identity: acksys User Password: acksys

Configuring Supplicant Network Interface

In the GUI, go to Setup → Physical Interfaces → Edit LAN Interface to create the LAN Network

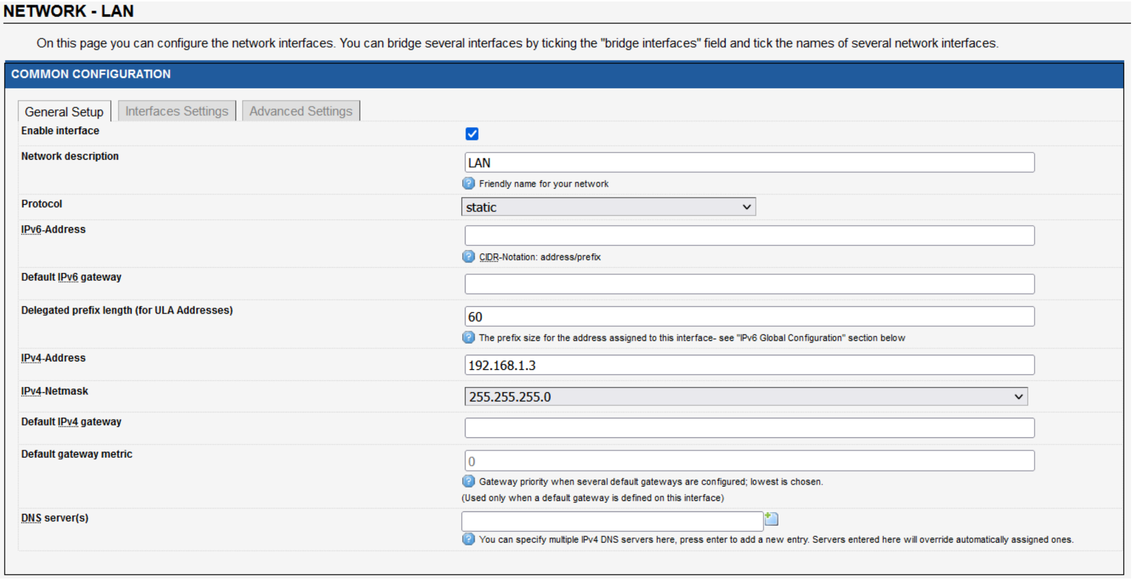


NETWORK OVERVIEW

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

Click the "Edit" button located to the right and configure the Alias IP address used to configure the LAN Interface.

- General Setup
  - Network description :LAN (use your custom name)
  - Protocol: Static
  - IPv4-Address : 192.168.1.3
  - IPv4 Netmask:255.255.255.0
  - Save



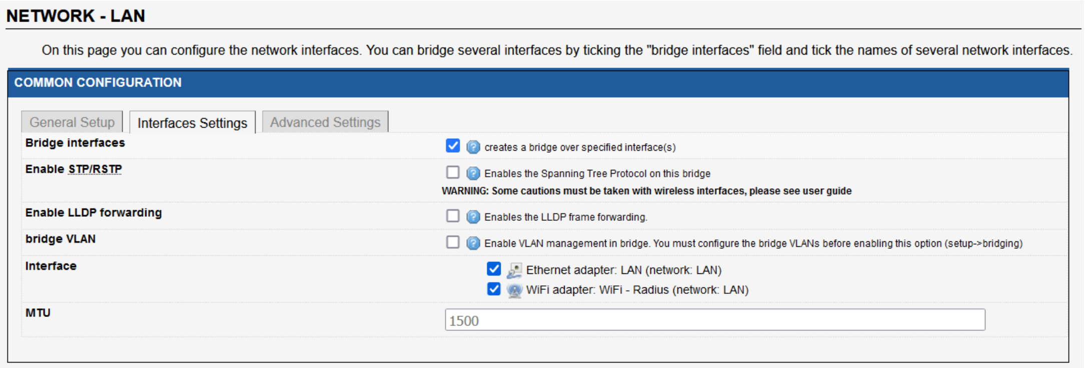
NETWORK - LAN

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

Enable interface	☑
Network description	LAN Friendly name for your network
Protocol	static
IPv6-Address	 CIDR-Notation: address/prefix
Default IPv6 gateway	
Delegated prefix length (for ULA Addresses)	60 The prefix size for the address assigned to this interface- see "IPv6 Global Configuration" section below
IPv4-Address	192.168.1.3
IPv4-Netmask	255.255.255.0
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.

- Interface Settings
  - Bridge Interfaces: enable
  - Interface: Tick Ethernet Adapter and WiFI Adaptor
  - Click Save



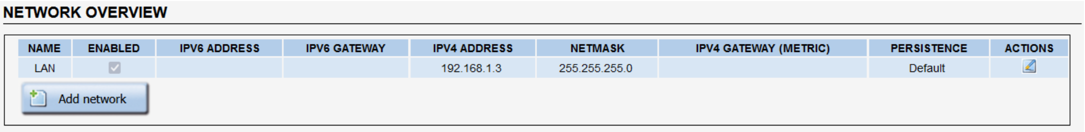
NETWORK - LAN

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	☑ Ethernet adapter: LAN (network: LAN) ☑ WiFi adapter: WiFi - Radius (network: LAN)
MTU	1500

After modifying the default network, we should have the result below:



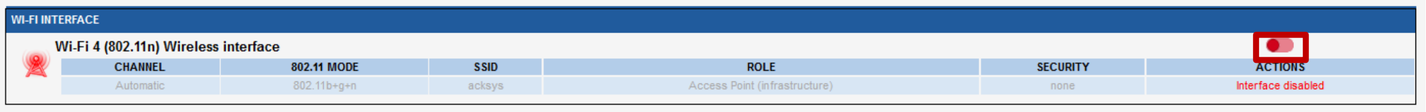
NETWORK OVERVIEW

NAME	ENABLED	IPV6 ADDRESS	IPV6 GATEWAY	IPV4 ADDRESS	NETMASK	IPV4 GATEWAY (METRIC)	PERSISTENCE	ACTIONS
LAN	☑			192.168.1.3	255.255.255.0		Default	

Add network

Configuring Supplicant SSID

In the GUI, go to Setup → Physical Interfaces → Click WiFI Adaptor to On

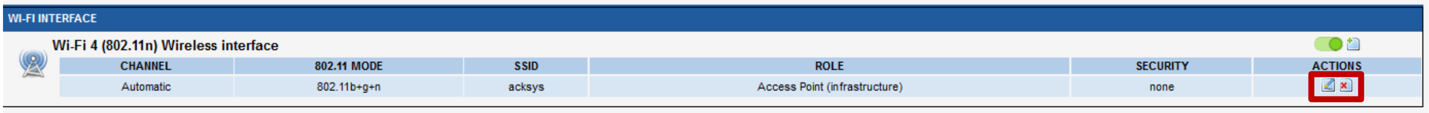


WI-FI INTERFACE

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 your SSID configuration page:

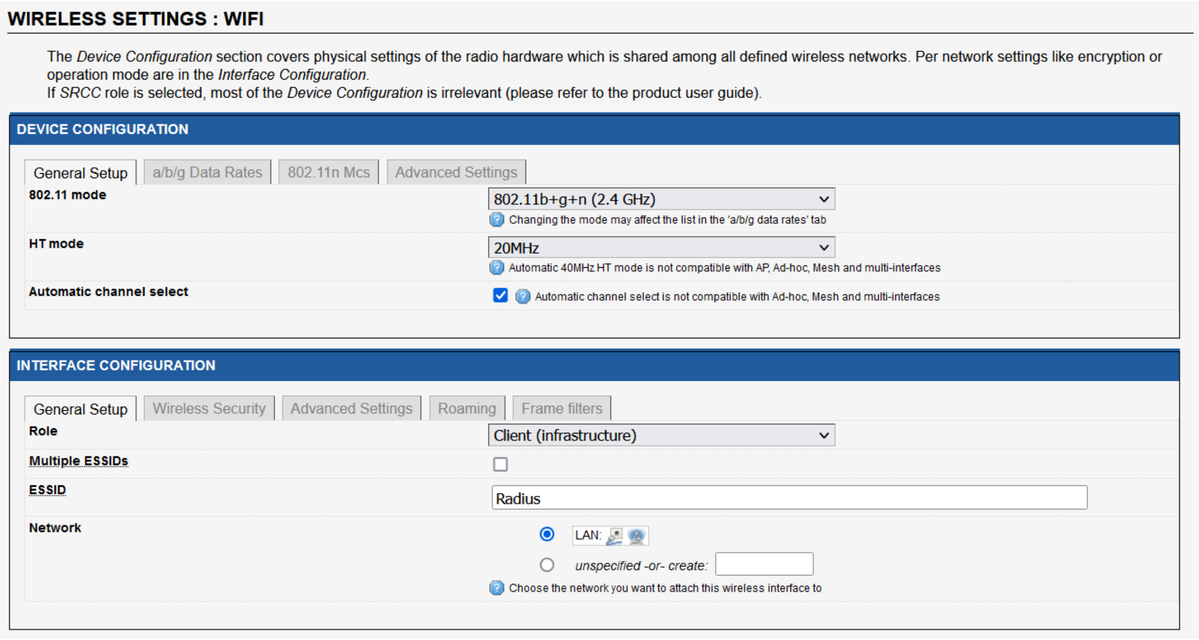


WI-FI INTERFACE

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	

- Role: Client
- ESSID: Radius
- Network: LAN
- 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

INTERFACE CONFIGURATION

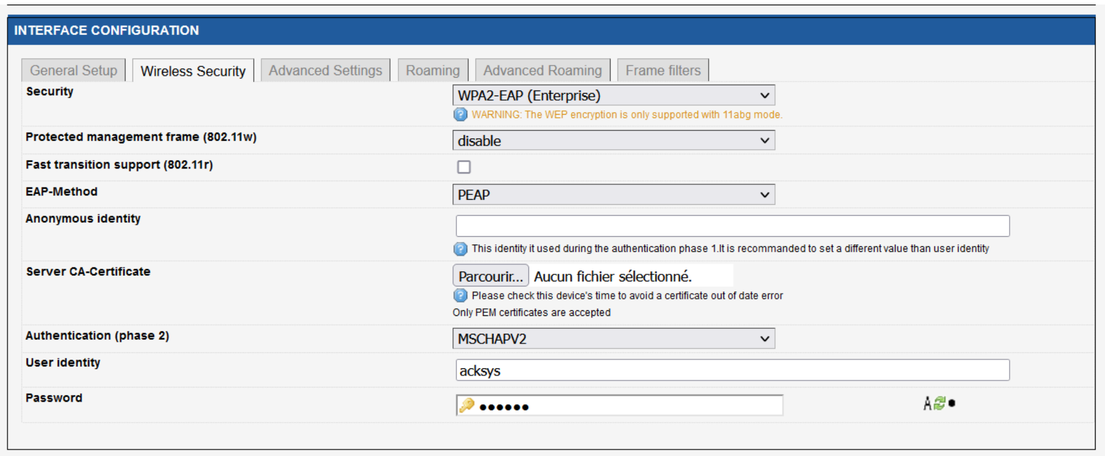
Role: Client (infrastructure)

Multiple ESSIDs: □

ESSID: Radius

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

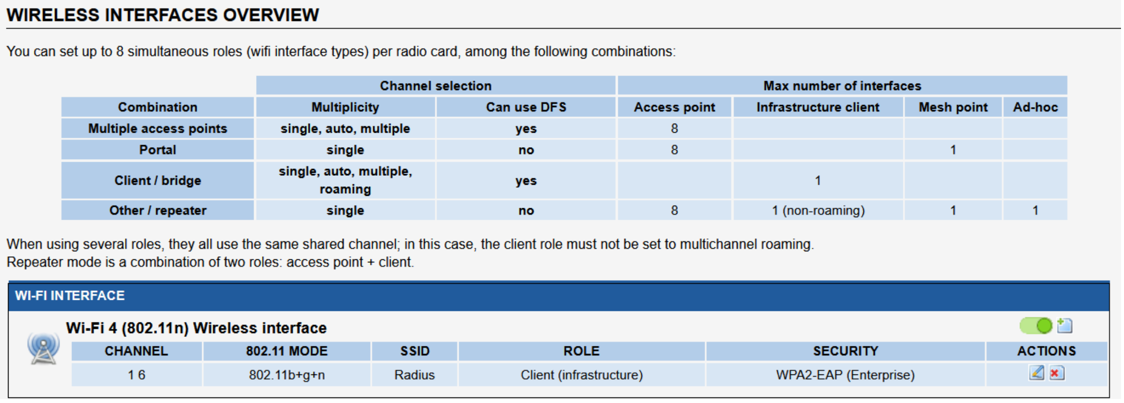
- Wireless Security
  - WPA2-EAP (Enterprise)
  - EAP-Method: PEAP
  - Server CA-Certificate: Import the .pem certificate use on the Radius Server
  - Authentication phase2: MSCHAPv2
  - User identity: acksys
  - Password: acksys
  - Click Save and Apply



INTERFACE CONFIGURATION

Security	WPA2-EAP (Enterprise) WARNING: The WEP encryption is only supported with 11abg mode.
Protected management frame (802.11w)	disable
Fast transition support (802.11r)	□
EAP-Method	PEAP
Anonymous identity	 This identity it used during the authentication phase 1.It is recommanded to set a different value than user identity
Server CA-Certificate	Parcourir... Aucun fichier sélectionné. Please check this device's time to avoid a certificate out of date error Only PEM certificates are accepted
Authentication (phase 2)	MSCHAPV2
User identity	acksys
Password	••••••

After modifying the default WIFI parameter, we should have the result below:



WIRELESS INTERFACES OVERVIEW

You can set up to 8 simultaneous roles (wifi interface types) per radio card, among the following combinations:

	Channel selection		Max number of interfaces			
Combination	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.

WI-FI INTERFACE

Wi-Fi 4 (802.11n) Wireless interface

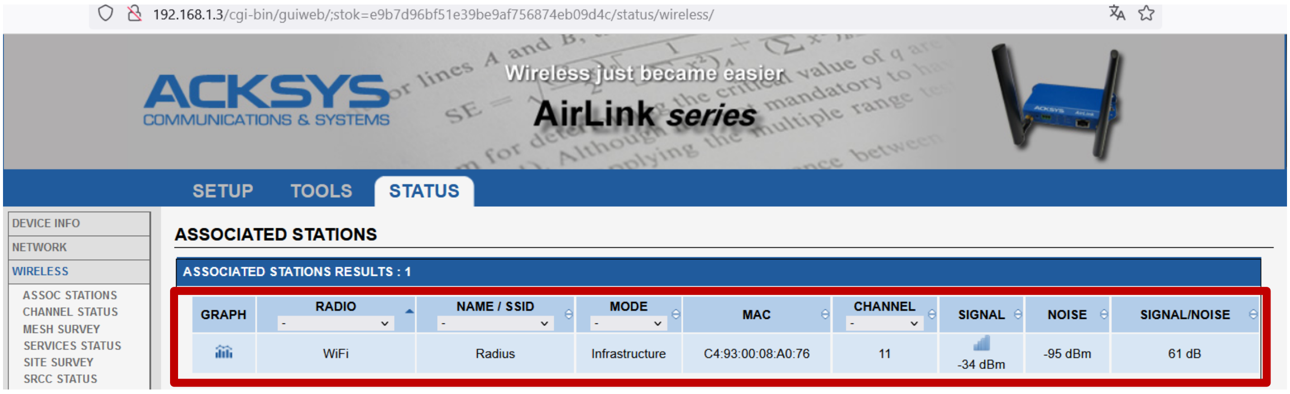
CHANNEL	802.11 MODE	SSID	ROLE	SECURITY	ACTIONS
1 6	802.11b+g+n	Radius	Client (infrastructure)	WPA2-EAP (Enterprise)	

NOTE: The AP as a RADIUS client collects user information (here user name as acksys and password as acksys) and sends this information to a RADIUS server. The RADIUS server authenticates a user according to these information and then performs authorization and accounting for the user.

6. 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.

In GUI Status →Wireless
The Router configured as Supplicant is well authenticated with its credential on the Radius Sever Via the AP configured as Authenticator.

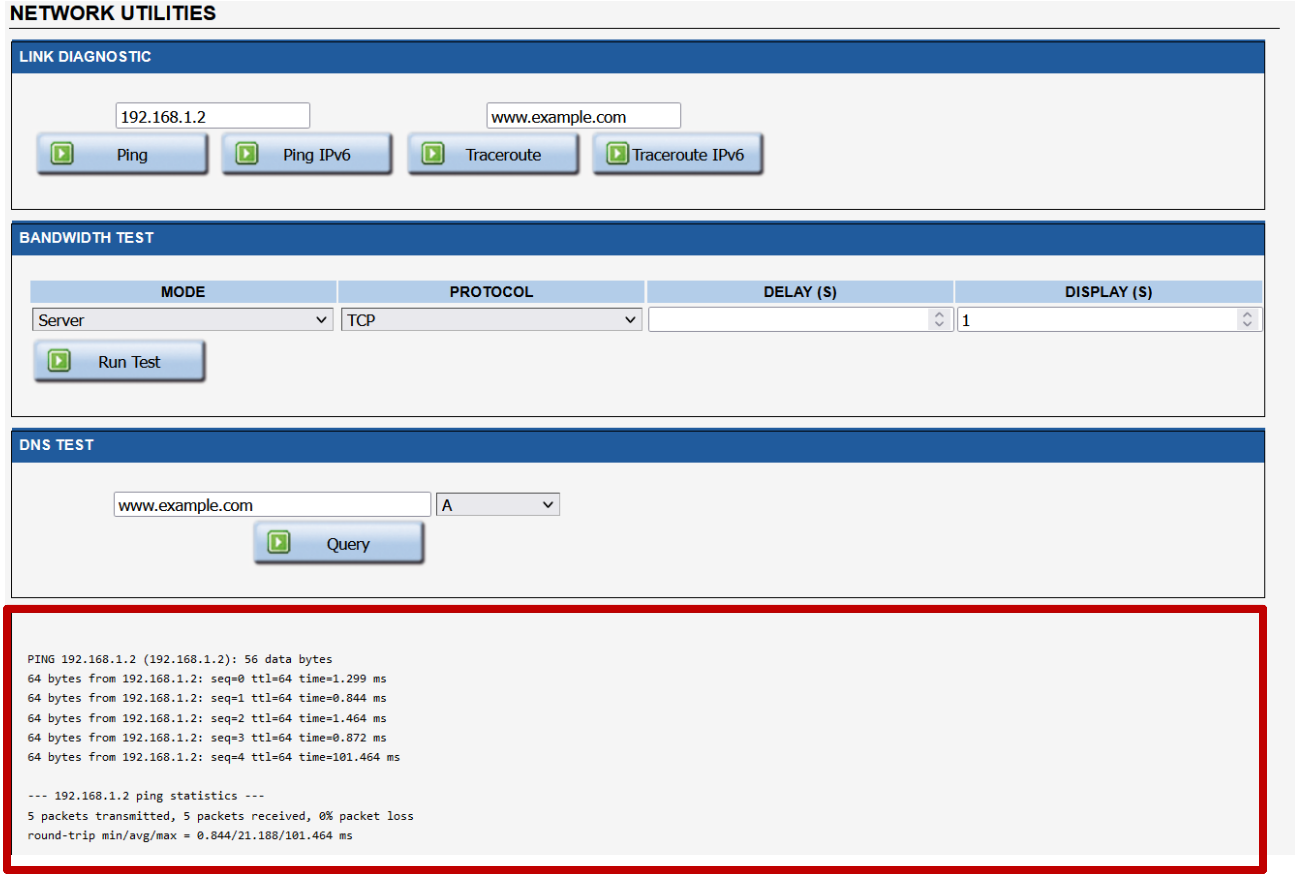

192.168.1.3/cgi-bin/guiweb/;stok=e9b7d96bf51e39be9af756874eb09d4c/status/wireless/
ACKSYS COMMUNICATIONS & SYSTEMS
Wireless just became easier
AirLink series
SETUP
TOOLS
STATUS
DEVICE INFO
NETWORK
WIRELESS
ASSOC STATIONS
CHANNEL STATUS
MESH SURVEY
SERVICES STATUS
SITE SURVEY
SRCC STATUS

ASSOCIATED STATIONS

ASSOCIATED STATIONS RESULTS : 1

GRAPH	RADIO	NAME / SSID	MODE	MAC	CHANNEL	SIGNAL	NOISE	SIGNAL/NOISE
	-	-	-		-			
	WiFi	Radius	Infrastructure	C4:93:00:08:A0:76	11	-34 dBm	-95 dBm	61 dB

IP Connectivity for the Supplicant to the Radius Server work properly showing the User Acksys is well authenticated on the radius server as shown on the below screenshot



LINK DIAGNOSTIC: 192.168.1.2 | www.example.com

BANDWIDTH TEST

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

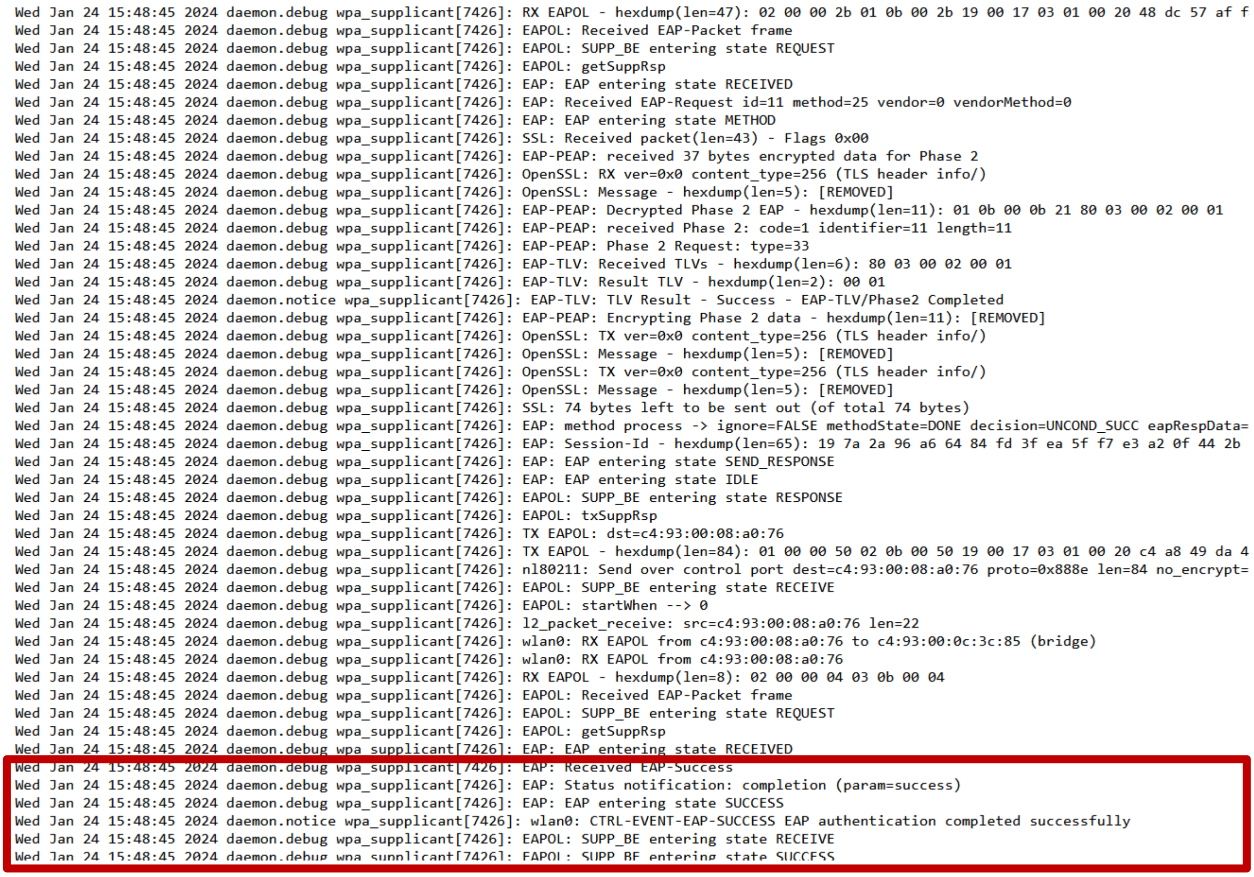
DNS TEST: www.example.com | A

```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: seq=0 ttl=64 time=1.299 ms
64 bytes from 192.168.1.2: seq=1 ttl=64 time=0.844 ms
64 bytes from 192.168.1.2: seq=2 ttl=64 time=1.464 ms
64 bytes from 192.168.1.2: seq=3 ttl=64 time=0.872 ms
64 bytes from 192.168.1.2: seq=4 ttl=64 time=101.464 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.844/21.188/101.464 ms
```

Example of Acksys Radius Logs during authentication

In the GUI, go to Status → Logs and look after radius logs to check the authentication logs

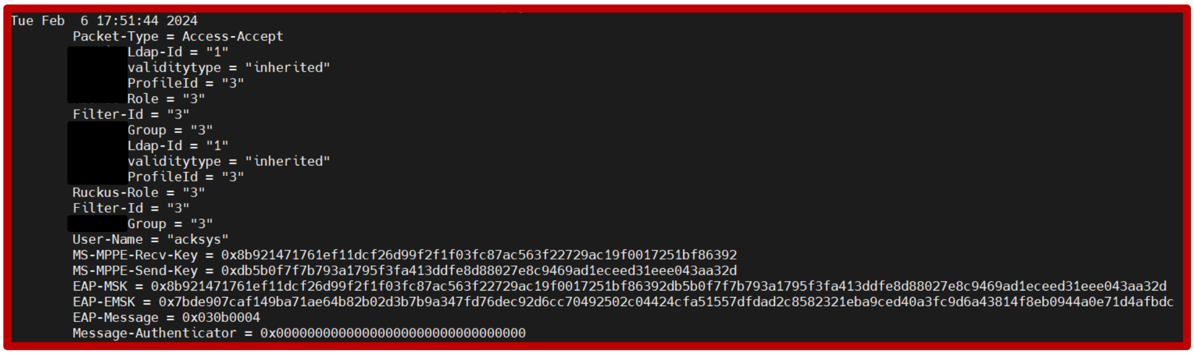


```
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: RX EAPOL - hexdump(len=47): 02 00 00 2b 01 0b 00 2b 19 00 17 03 01 00 20 48 dc 57 af f
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: Received EAP-Packet frame
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state REQUEST
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: getSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state RECEIVED
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Received EAP-Request id=11 method=25 vendor=0 vendorMethod=0
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state METHOD
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: SSL: Received packet(len=43) - Flags 0x00
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: received 37 bytes encrypted data for Phase 2
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: RX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Decrypted Phase 2 EAP - hexdump(len=11): 01 0b 00 0b 21 80 03 00 02 00 01
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: received Phase 2: code=1 identifier=11 length=11
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Phase 2 Request: type=33
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-TLV: Received TLVs - hexdump(len=6): 80 03 00 02 00 01
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-TLV: Result TLV - hexdump(len=2): 00 01
Wed Jan 24 15:48:45 2024 daemon.notice wpa_supplicant[7426]: EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP-PEAP: Encrypting Phase 2 data - hexdump(len=11): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: TX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: TX ver=0x0 content_type=256 (TLS header info/)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: OpenSSL: Message - hexdump(len=5): [REMOVED]
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: SSL: 74 bytes left to be sent out (of total 74 bytes)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: method process -> ignore=FALSE methodState=DONE decision=UNCOND_SUCC eapRespData=
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Session-Id - hexdump(len=65): 19 7a 2a 96 a6 64 84 fd 3f ea 5f f7 e3 a2 0f 44 2b
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state SEND_RESPONSE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state IDLE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RESPONSE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: txSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: TX EAPOL: dst=c4:93:00:08:a0:76
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: TX EAPOL - hexdump(len=84): 01 00 00 50 02 0b 00 50 19 00 17 03 01 00 20 c4 a8 49 da 4
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: nl80211: Send over control port dest=c4:93:00:08:a0:76 proto=0x888e len=84 no_encrypt=
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RECEIVE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: startWhen --> 0
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: l2_packet_receive: src=c4:93:00:08:a0:76 len=22
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: wlan0: RX EAPOL from c4:93:00:08:a0:76 to c4:93:00:0c:3c:85 (bridge)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: wlan0: RX EAPOL from c4:93:00:08:a0:76
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: RX EAPOL - hexdump(len=8): 02 00 00 04 03 0b 00 04
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: Received EAP-Packet frame
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state REQUEST
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: getSuppRsp
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state RECEIVED
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Received EAP-Success
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: Status notification: completion (param=success)
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAP: EAP entering state SUCCESS
Wed Jan 24 15:48:45 2024 daemon.notice wpa_supplicant[7426]: wlan0: CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state RECEIVE
Wed Jan 24 15:48:45 2024 daemon.debug wpa_supplicant[7426]: EAPOL: SUPP_BE entering state SUCCESS
```

Example of Radius server Logs during authentication

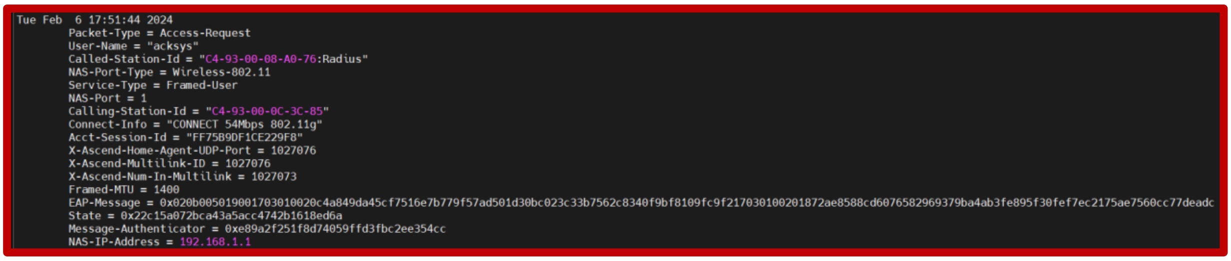
Let checking the authentication details logs and reply logs on the radius server:

Authentication details radius logs: Access-Accept for success authentication



```
Tue Feb  6 17:51:44 2024
        Packet-Type = Access-Accept
        [redacted] Ldap-Id = "1"
               validitytype = "inherited"
               ProfileId = "3"
               Role = "3"
        Filter-Id = "3"
        [redacted] Group = "3"
               Ldap-Id = "1"
               validitytype = "inherited"
               ProfileId = "3"
        Ruckus-Role = "3"
        Filter-Id = "3"
        [redacted] Group = "3"
        User-Name = "acksys"
        MS-MPPE-Recv-Key = 0x8b921471761ef11dcf26d99f2f1f03fc87ac563f22729ac19f0017251bf86392
        MS-MPPE-Send-Key = 0xdb5b0f7f7b793a1795f3fa413ddfe8d88027e8c9469ad1eceed31eee043aa32d
        EAP-MSK = 0x8b921471761ef11dcf26d99f2f1f03fc87ac563f22729ac19f0017251bf86392db5b0f7f7b793a1795f3fa413ddfe8d88027e8c9469ad1eceed31eee043aa32d
        EAP-EMSK = 0x7bde907caf149ba71ae64b82b02d3b7b9a347fd76dec92d6cc70492502c04424cfa51557dfdad2c8582321eba9ced40a3fc9d6a43814f8eb0944a0e71d4afbdc
        EAP-Message = 0x030b0004
        Message-Authenticator = 0x00000000000000000000000000000000
```

Reply detail radius logs



```
Tue Feb  6 17:51:44 2024
        Packet-Type = Access-Request
        User-Name = "acksys"
        Called-Station-Id = "C4-93-00-08-A0-76:Radius"
        NAS-Port-Type = Wireless-802.11
        Service-Type = Framed-User
        NAS-Port = 1
        Calling-Station-Id = "C4-93-00-0C-3C-85"
        Connect-Info = "CONNECT 54Mbps 802.11g"
        Acct-Session-Id = "FF75B9DF1CE229F8"
        X-Ascend-Home-Agent-UDP-Port = 1027076
        X-Ascend-Multilink-ID = 1027076
        X-Ascend-Num-In-Multilink = 1027073
        Framed-MTU = 1400
        EAP-Message = 0x020b005019001703010020c4a849da45cf7516e7b779f57ad501d30bc023c33b7562c8340f9bf8109fc9f217030100201872ae8588cd6076582969379ba4ab3fe895f30fef7ec2175ae7560cc77deadc
        State = 0x22c15a072bca43a5acc4742b1618ed6a
        Message-Authenticator = 0xe89a2f251f8d74059ffd3fbc2ee354cc
        NAS-IP-Address = 192.168.1.1
```

Support : https://support.acksys.fr