

Bastionado de redes y sistemas

Tarea 4: Administración de credenciales para el acceso a sistemas informáticos

Índice

Introducción.....	2
Instalación del servidor RADIUS.....	3
Configuración del servidor RADIUS.....	5
Configuración de router o sistema emulador.....	10
Demostración del servidor RADIUS en funcionamiento.....	13
Demostración de que el usuario se conecta correctamente.....	15
Bibliografía.....	17

Introducción

RADIUS (Remote Authentication Dial-In User Service) es un protocolo que se utiliza en servidores para la autenticación, autorización y contabilización de usuarios. Para entender su relación con un router, primero es importante saber que **WPA (Wi-Fi Protected Access)** es un protocolo de seguridad para redes inalámbricas que protege las conexiones Wi-Fi mediante encriptación y autenticación. Actualmente, existe la versión WPA3, pero la más común es la **WPA2**, que reemplazó el protocolo TKIP (Temporal Key Integrity Protocol) por el protocolo **AES (Advanced Encryption Standard)**, el cual ofrece un cifrado mucho más fuerte.

Dentro de este protocolo, los dos modos más extendidos son los siguientes:

- **WPA2-Personal o WPA2-Pre-Shared Key (WPA2-PSK):** Se usa comúnmente en routers domésticos, ya que solo requiere una contraseña compartida (Pre-Shared Key o PSK) para que los usuarios puedan conectarse a la red. Es fácil de configurar, pero si la contraseña se filtra, cualquier persona puede acceder a la red, además de que puede ser vulnerable a ataques de fuerza bruta si la clave es débil.
- **WPA2-Enterprise:** Se usa en entornos en los que muchos usuarios se conectan a una misma red privada, ya que en lugar de usar una clave compartida, cada usuario tiene credenciales únicas (usuario y contraseña, certificado digital, etc.). Esto hace que sea más seguro que WPA2-PSK porque permite administrar el acceso de cada usuario individualmente. No obstante, este modo requiere un servidor RADIUS para autenticar usuarios mediante protocolos como EAP (Extensible Authentication Protocol).

Como podemos ver, el servidor RADIUS es esencial para la autenticación de usuarios cuando un router está configurado con el protocolo WPA2-Enterprise. En este esquema, el enrutador no almacena ni valida las credenciales de los usuarios directamente, sino que actúa como un cliente RADIUS.

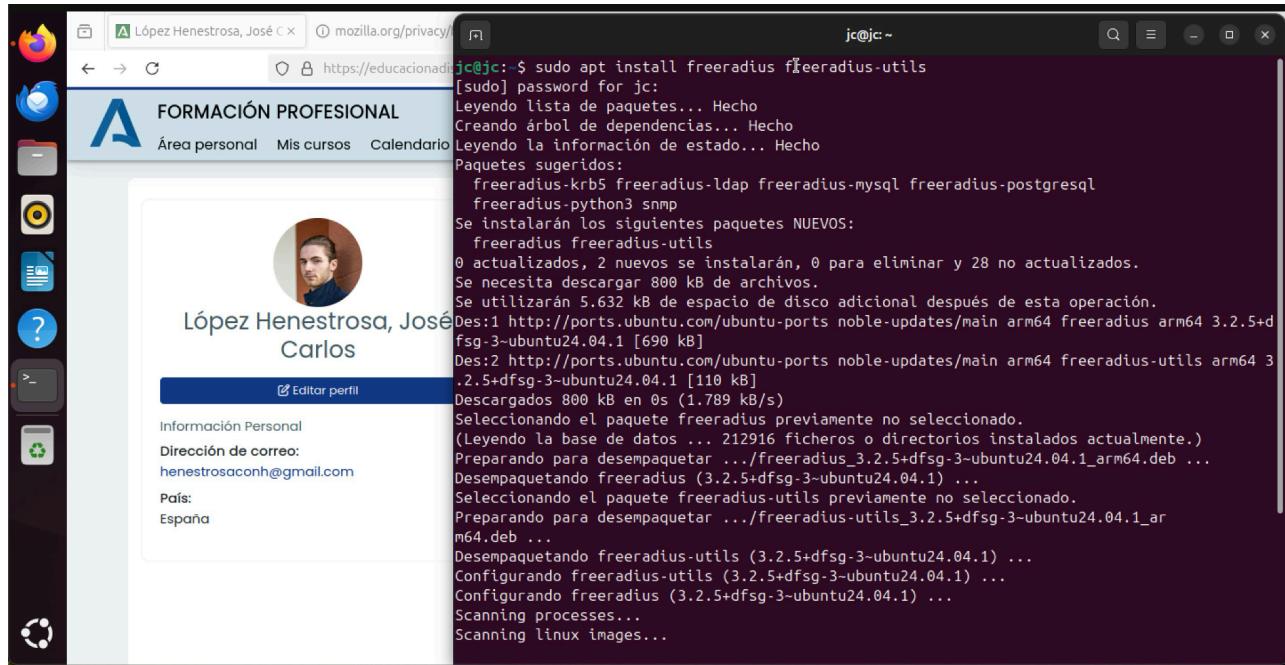
En síntesis, este es el proceso que se sigue cuando un dispositivo intenta conectarse a una red Wi-Fi protegida con WPA2-Enterprise:

1. El router recibe las credenciales de autenticación y las reenvía al servidor RADIUS.
2. El servidor RADIUS se encarga de verificar la información proporcionada y de compararla con una base de datos de usuarios autorizados, típicamente almacenados en el archivo `/etc/freeradius/3.0/users`.
3. El servidor RADIUS envía una respuesta al router en la que indica si la autenticación ha sido exitosa o no.
 - Si el acceso es aprobado, el dispositivo puede conectarse a la red
 - Si el acceso es denegado, se le rechaza la conexión.

Instalación del servidor RADIUS

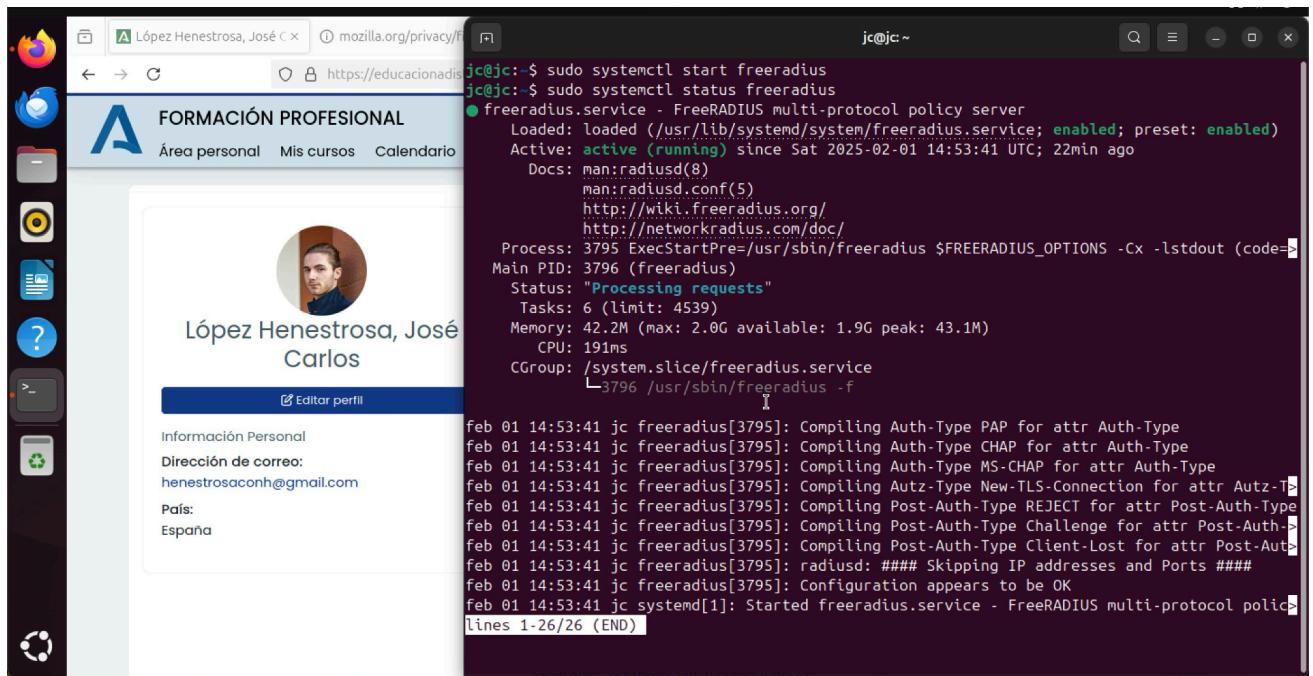
En Ubuntu, se puede instalar un servidor RADIUS a través de FreeRADIUS, una de las implementaciones más populares de este protocolo. Para instalarlo, ejecutamos el siguiente comando:

```
sudo apt install freeradius freeradius-utils
```



Instalando los paquetes `freeradius` y `freeradius-utils`

Tras instalarlo, activamos el servicio ejecutando `sudo systemctl start freeradius` y verificamos su estado con `sudo systemctl status freeradius`.



Iniciando y comprobando el correcto funcionamiento de `freeradius`

Llegados a este punto, el servidor RADIUS ha sido instalado e iniciado correctamente.

Configuración del servidor RADIUS

Para configurar FreeRADIUS en Ubuntu con el fin de que los usuarios se autentifiquen con credenciales (nombre de usuario y contraseña) en lugar de una clave WiFi genérica, tenemos que usar el protocolo EAP (Extensible Authentication Protocol) para habilitar el acceso seguro con credenciales en redes inalámbricas.

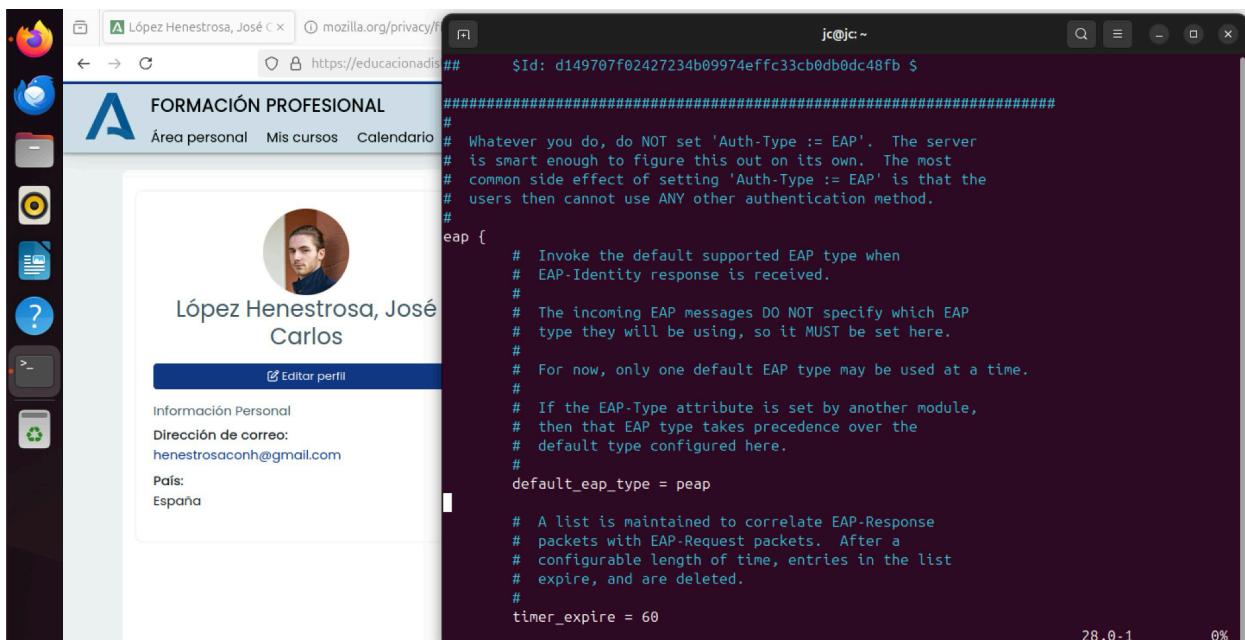
Este es el procedimiento desglosado en pasos:

1. Habilitar el módulo EAP-PEAP

Por defecto, EAP está configurado para usar MD5 (EAP-MD5), el cual es un método de autenticación dentro del protocolo EAP que utiliza el algoritmo de hash MD5 para validar credenciales. Es uno de los métodos más básicos de EAP, pero también el menos seguro.

En su lugar, vamos a configurarlo para usar PEAP (Protected EAP) + MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2), el cual es el método estándar en WPA2-Enterprise dado a su amplio soporte y seguridad.

Para ello, editamos el archivo `/etc/freeradius/3.0/mods-enabled/eap` y cambiamos la línea en la que pone `default_eap_type = md5` por `default_eap_type = peap`.



Configuración del archivo `/etc/freeradius/3.0/mods-enabled/eap` para habilitar el protocolo PEAP

Tras cambiar el tipo de EAP, buscamos la línea `default_eap_type` dentro del bloque `peap {` para asegurarnos de que su valor es `mschapv2`.

```

# recommend using EAP-MS-CHAPv2.
#
peap {
    # Which tls-config section the TLS negotiation parameters
    # are in - see EAP-TLS above for an explanation.
    #
    # In the case that an old configuration from FreeRADIUS
    # v2.x is being used, all the options of the tls-config
    # section may also appear instead in the 'tls' section
    # above. If that is done, the tls= option here (and in
    # tls above) MUST be commented out.
    #
    tls = tls-common

    # The tunneled EAP session needs a default
    # EAP type which is separate from the one for
    # the non-tunneled EAP module. Inside of the
    # PEAP tunnel, we recommend using MS-CHAPv2,
    # as that is the default type supported by
    # Windows clients.
    #
    default_eap_type = mschapv2

    # The PEAP module also has these configuration
    # items, which are the same as for TTLS.
    #
    copy_request_to_tunnel = no

    # This configuration item is deprecated. Instead,
    # you should use:

```

Configuración del archivo /etc/freeradius/3.0/mods-enabled/eap para habilitar MSCHAPv2

2. Configurar usuarios y credenciales

Editamos el archivo /etc/freeradius/3.0/users para añadir usuarios con credenciales personalizadas. En este caso, vamos a añadir estas dos líneas:

```

usuario1 Cleartext-Password := "contraseña1"
usuario2 Cleartext-Password := "contraseña2"

```

```

#
# The canonical testing user which is in most of the
# examples.
#
#bob  Cleartext-Password := "hello"
#      Reply-Message := "Hello, %{User-Name}"
#
# This is an entry for a user with a space in their name.
# Note the double quotes surrounding the name. If you have
# users with spaces in their names, you must also change
# the "filter_username" policy to allow spaces.
#
# See raddb/policy.d/filter, filter_username {} section.
#
#"John Doe"    Cleartext-Password := "hello"
#                  Reply-Message = "Hello, %{User-Name}"
#
# Dial user back and telnet to the default host for that port

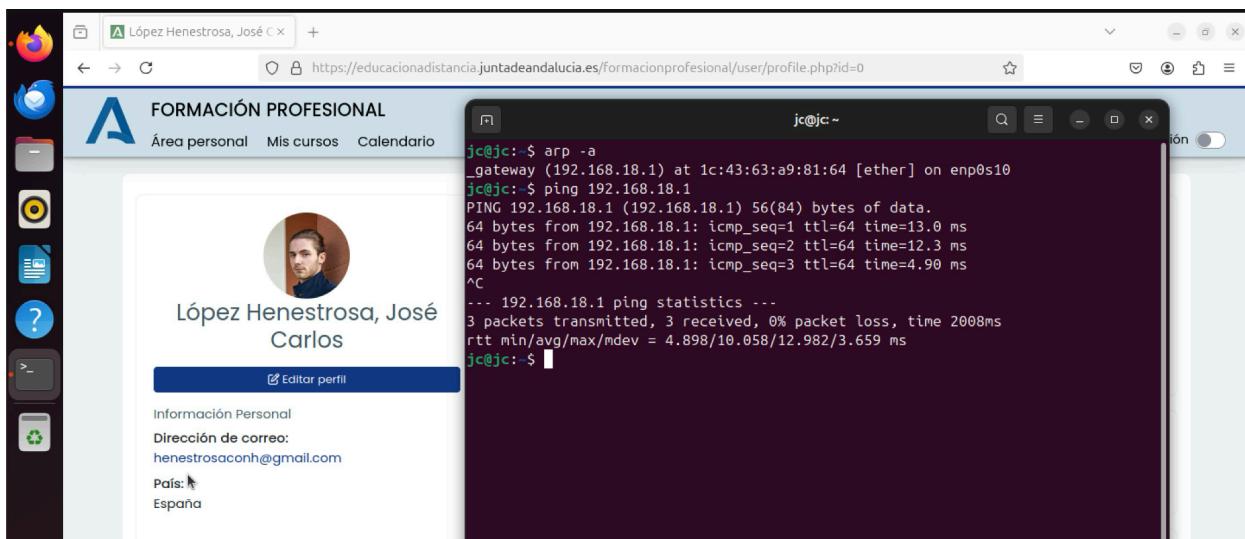
```

Configuración del archivo /etc/freeradius/3.0/users

3. Obtener IP del Punto de Acceso (AP)

Ejecutamos el comando sudo apt install net-tools para poder usar el comando arp -a. Este último paquete nos permitirá obtener la lista de dispositivos en la red junto con sus direcciones IP y MAC. Es importante mencionar que estoy ejecutando Ubuntu desde una máquina virtual, por lo que he tenido que cambiar el modo de red de la máquina a Bridge.

Una vez que tenemos localizada la dirección IP, podemos ejecutar ping para comprobar que la conexión funciona correctamente.

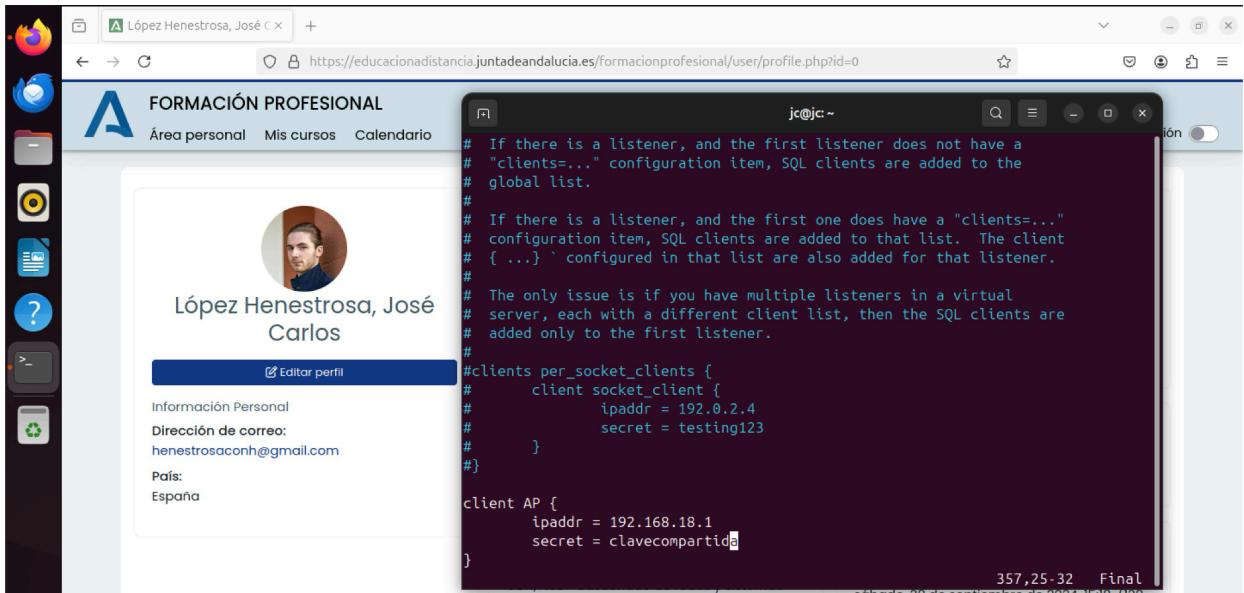


Hallando la IP del router doméstico y probando la conexión

4. Añadir cliente (AP)

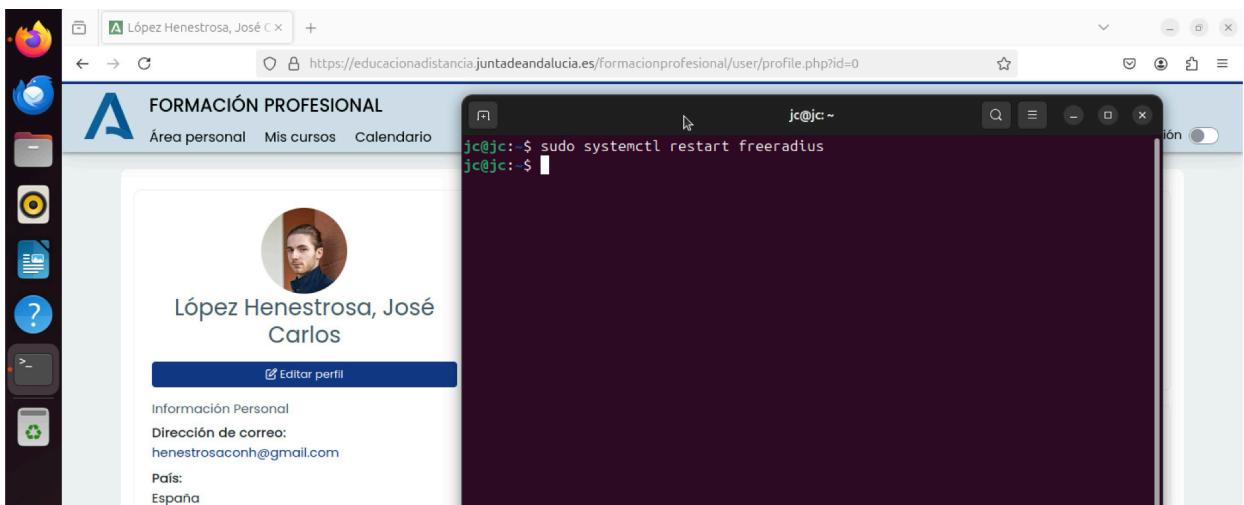
Si la IP del router termina en 1, podemos saltarnos este paso, ya que por defecto la configuración del archivo /etc/freeradius/3.0/clients.conf determina que la IP del para añadir la IP del AP (mi router doméstico) identificada anteriormente y una clave compartida (`secret`) cualquiera:

```
client AP {  
    ipaddr = 192.168.18.1  
    secret = clavecompartida  
}
```



Configuración del archivo /etc/freeradius/3.0/clients.conf con el router doméstico añadido

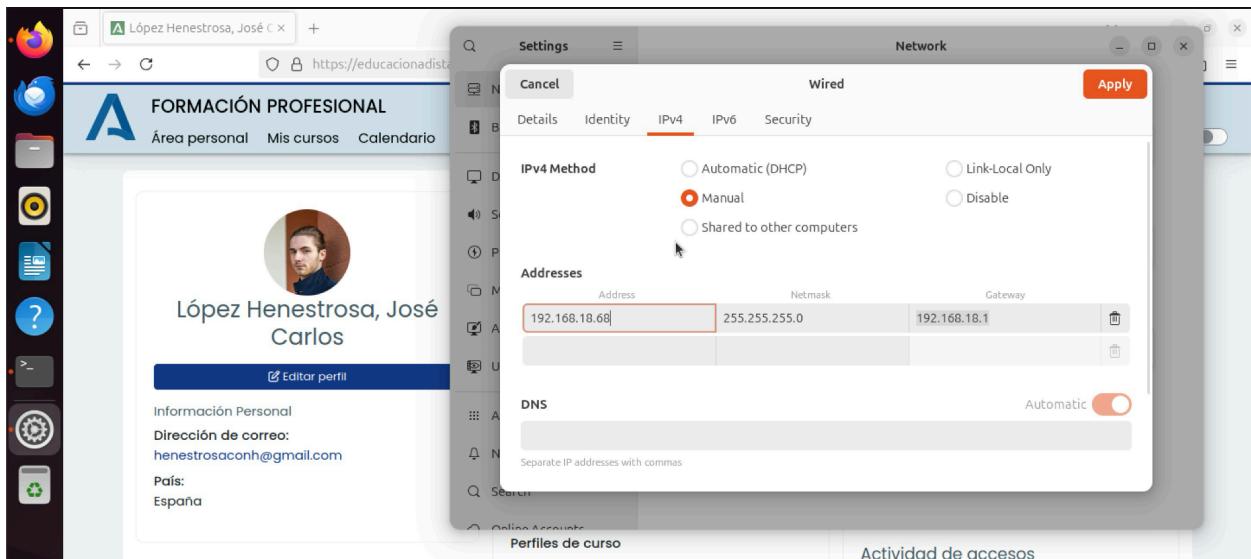
Tras guardar los cambios, reiniciamos el servicio para que la configuración surta efecto.



Reiniciando el servicio freeradius

5. Configurar IP estática

Por último, le asignamos una IP estática al servidor para garantizar que siempre tenga la misma dirección, con el fin de que los clientes, dispositivos o servicios externos puedan conectarse a él sin interrupciones. Para ello, accedemos a las opciones de configuración de red del sistema y cambiamos el **método IPV4 a manual**.



Configuración para la IP estática

Tras concluir este proceso, ya tendremos configurado el servidor RADIUS en Ubuntu.

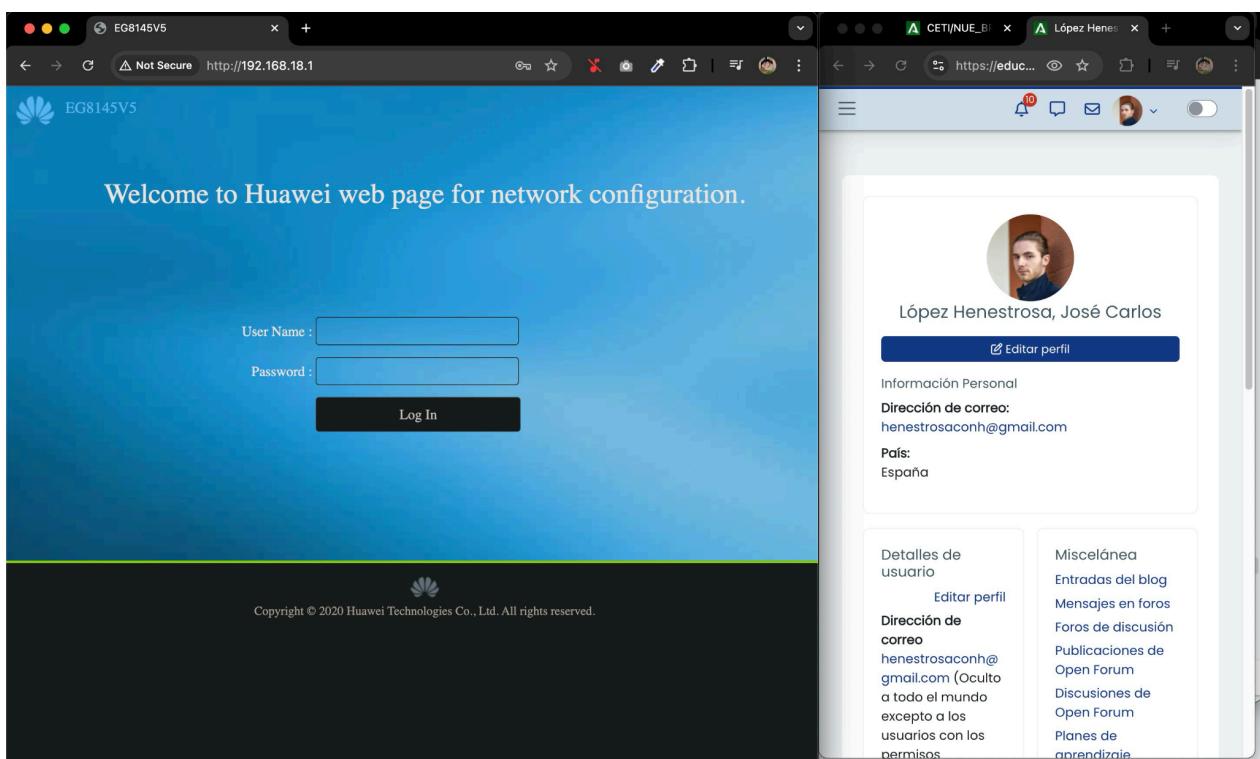
Configuración de router o sistema emulador

Este punto puede variar en función de si el router que queremos configurar dispone del protocolo **WPA2-Enterprise**. En mi caso, mi router doméstico cuenta con él, por lo que voy a configurarlo directamente. Como método alternativo, podríamos utilizar software como **OPNSense** o **RouterOS** para emular un router que nos permita implementar la autenticación con usuario y contraseña, aunque sería por LAN en lugar de Wi-Fi. Todo este proceso debe realizarse desde una segunda máquina virtual que actuará como sistema emulador de router.

Dicho esto, procedemos a configurar el AP directamente siguiendo estos pasos:

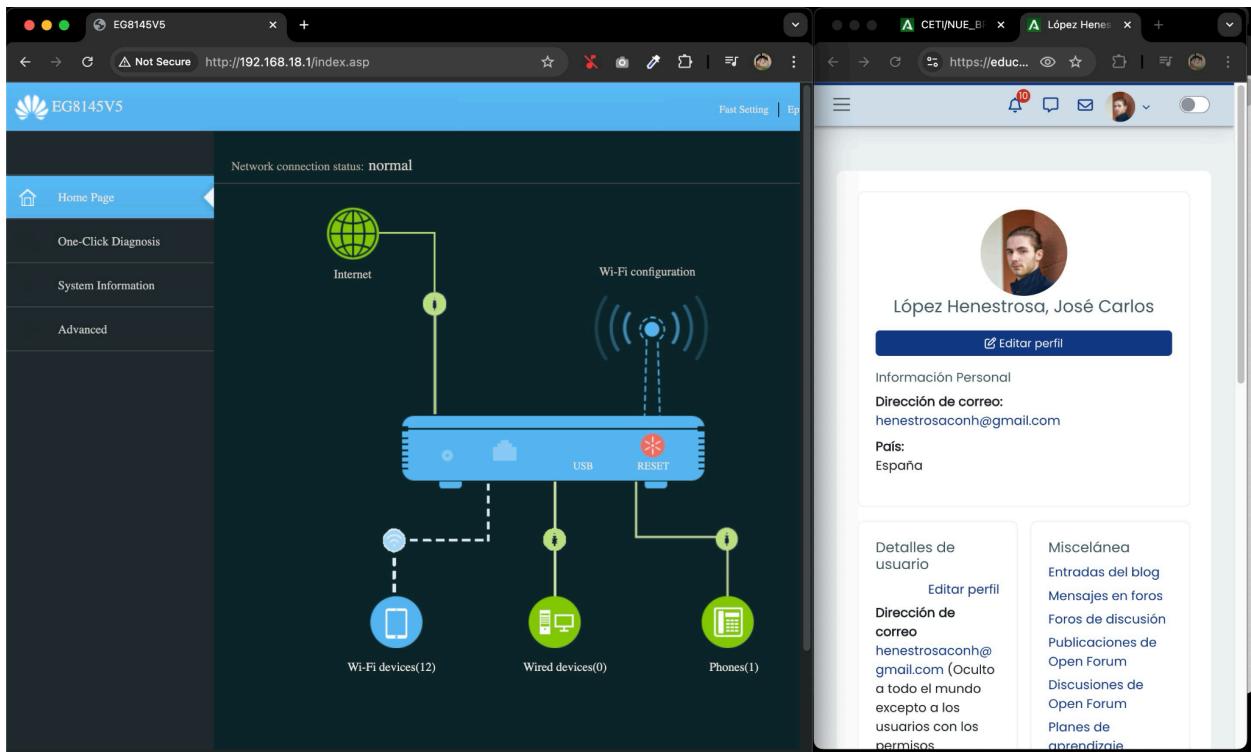
1. Acceder a la configuración del AP

Introducimos la IP del AP en un navegador web para acceder a su configuración. Como pudimos comprobar en el [apartado anterior](#), la IP del AP es 192.168.18.1, por lo que la introducimos en el navegador.



Pantalla principal de configuración del AP

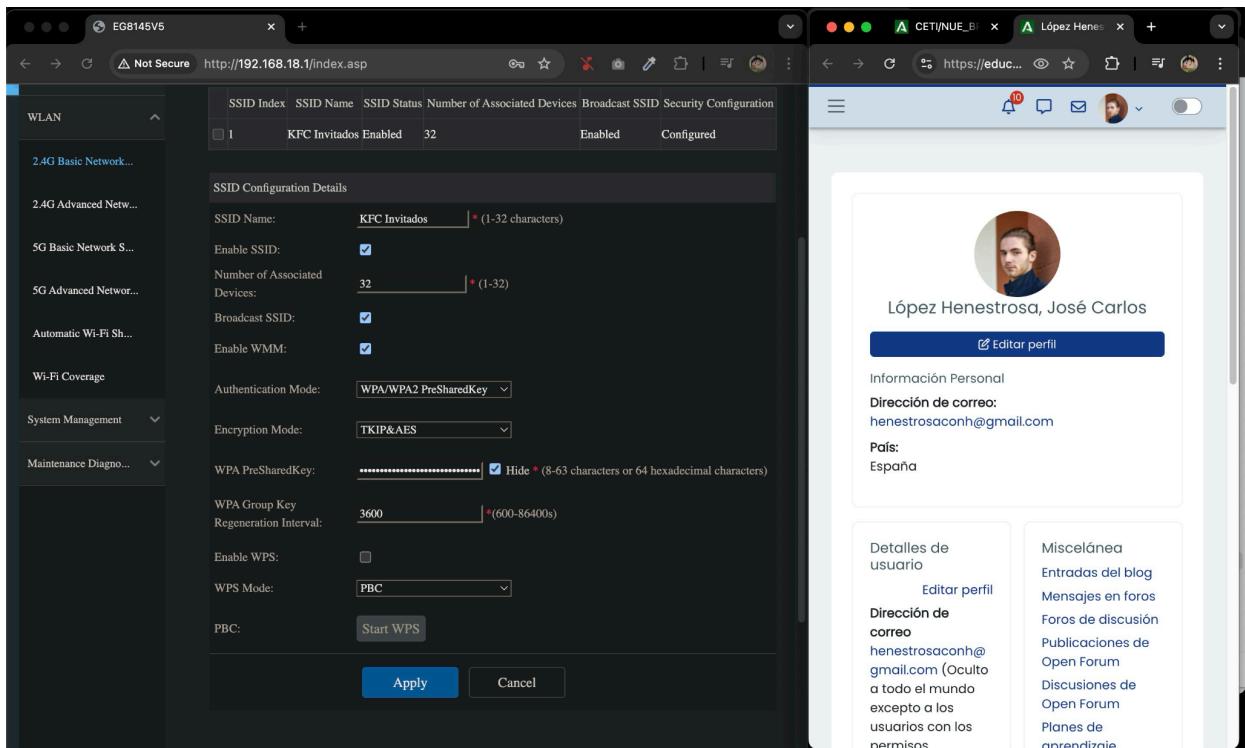
Hay que tener en cuenta que la pantalla cambiará dependiendo del fabricante del router. A su vez, cada fabricante asigna un usuario y una contraseña predeterminada. En el caso de Huawei, las credenciales son `Epuser / userEp`.



Panel de configuración del router tras iniciar sesión

2. Configurar el AP para usar WPA2-Enterprise

Una vez dentro del panel de configuración del router, lo configuramos para usar WPA2-Enterprise y establecer los parámetros del servidor RADIUS creado previamente. Para ello, seleccionamos **Advanced > WLAN > 2.4G Basic Network Settings**.



Configuración 2.4G Basic Network por defecto

Tenemos que cambiar el valor de la opción **Authentication Mode** a **WPA/WPA2 Enterprise**. Al hacer esto, se mostrarán campos de texto adicionales para añadir los parámetros del servidor RADIUS, los cuales son los siguientes:

- **Modo de autenticación:** WPA2 Enterprise.
- **Modo de encriptación:** AES (recordemos que TKIP es más débil).
- **Dirección del servidor RADIUS:** Dado que lo hemos configurado para que sea estático, introducimos la dirección IP que le asignamos previamente (192.168.18.1).
- **Puerto del servidor RADIUS:** 1812 (por defecto).
- **Clave compartida RADIUS:** La definida en el archivo `clients.conf` (`clavecompartida`).

The left screenshot shows the configuration interface for a 2.4G Basic Network, specifically for the 'KFC Invitados' SSID. It shows fields for SSID Name (KFC Invitados), Enable SSID (checked), Number of Associated Devices (32), Broadcast SSID (checked), Enable WMM (checked), Authentication Mode (WPA2 Enterprise selected), Encryption Mode (AES), RADIUS Server Address (192.168.18.68), RADIUS Server Port (1812), RADIUS Shared Key (clavecompartida), and WPA Group Key Regeneration Interval (3600). The right screenshot shows a user profile for 'López Henestrosa, José Carlos' with a picture, edit profile button, information personal, dirección de correo (henestrosaconh@gmail.com), país (España), and sidebar links for user details and miscellanea.

Configuración 2.4G Basic Network con el método de autenticación WPA2 Enterprise

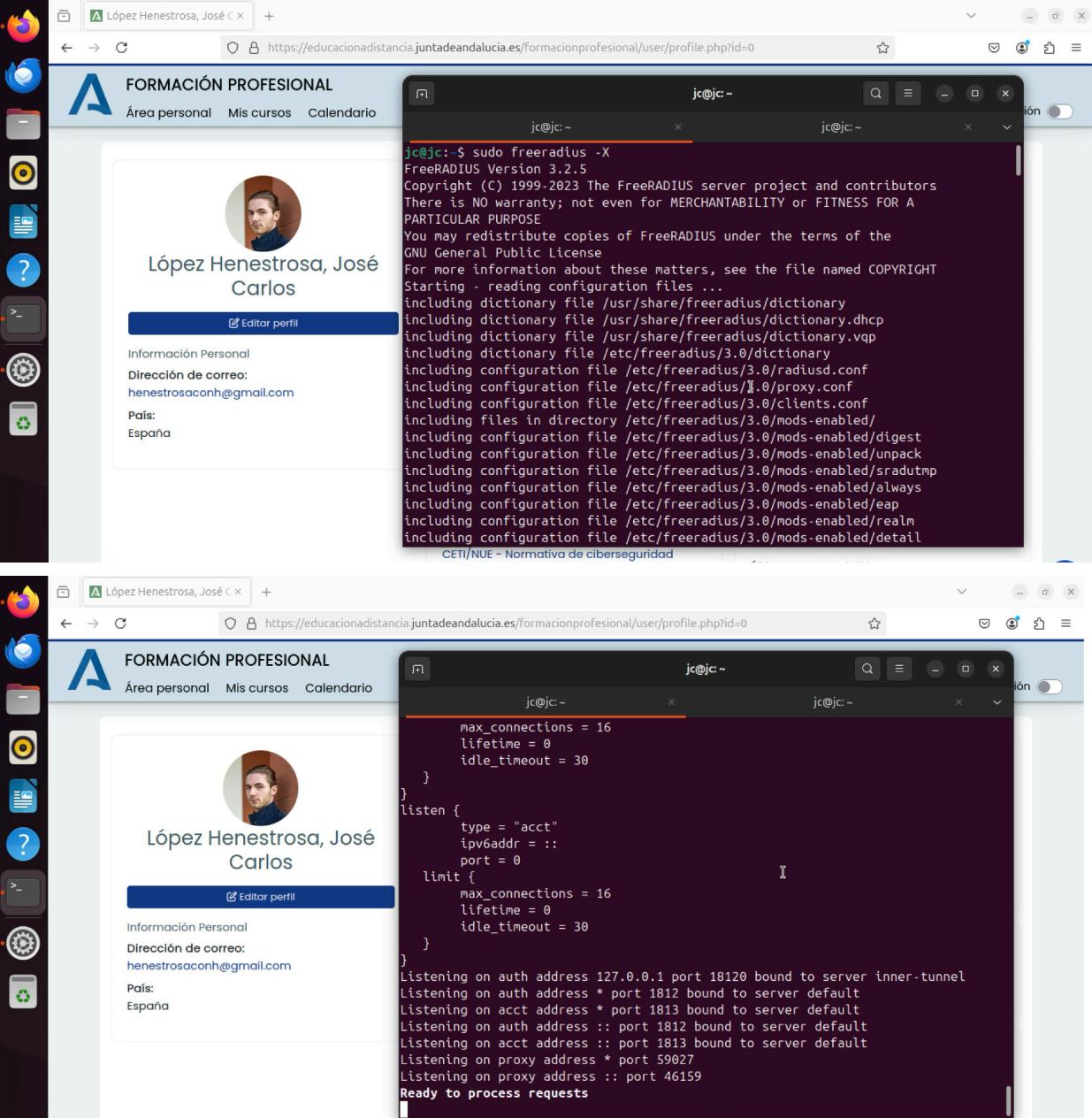
Una vez terminado el proceso, pulsamos **Apply** para que la configuración surta efecto.

Demostración del servidor RADIUS en funcionamiento

Comprobamos si el servidor RADIUS está funcionando correctamente siguiendo estos pasos:

1. Iniciar FreeRADIUS en modo depuración

Para ello, ejecutamos `sudo freeradius -X` (-X indica que el servidor se inicia en modo depuración):



```
jc@jc: ~
FreeRADIUS Version 3.2.5
Copyright (C) 1999-2023 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYRIGHT
Starting - reading configuration files ...
including dictionary file /usr/share/freeradius/dictionary
including dictionary file /usr/share/freeradius/dictionary.dhcp
including dictionary file /usr/share/freeradius/dictionary.vqp
including dictionary file /etc/freeradius/3.0/dictionary
including configuration file /etc/freeradius/3.0/radiusd.conf
including configuration file /etc/freeradius/3.0/proxy.conf
including configuration file /etc/freeradius/3.0/clients.conf
including files in directory /etc/freeradius/3.0/mods-enabled/
including configuration file /etc/freeradius/3.0/mods-enabled/digest
including configuration file /etc/freeradius/3.0/mods-enabled/unpack
including configuration file /etc/freeradius/3.0/mods-enabled/sradutmp
including configuration file /etc/freeradius/3.0/mods-enabled/always
including configuration file /etc/freeradius/3.0/mods-enabled/eap
including configuration file /etc/freeradius/3.0/mods-enabled/realm
including configuration file /etc/freeradius/3.0/mods-enabled/detail
CETI/NUE - Normativa de ciberseguridad

max_connections = 16
lifetime = 0
idle_timeout = 30
}
listen {
    type = "acct"
    ipv6addr = :::
    port = 0
    limit {
        max_connections = 16
        lifetime = 0
        idle_timeout = 30
    }
}
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on proxy address * port 59027
Listening on proxy address :: port 46159
Ready to process requests
CETI/NUE - Normativa de ciberseguridad
```

Ejecución del comando `sudo freeradius -X`

2. Realizar prueba de autenticación con radtest

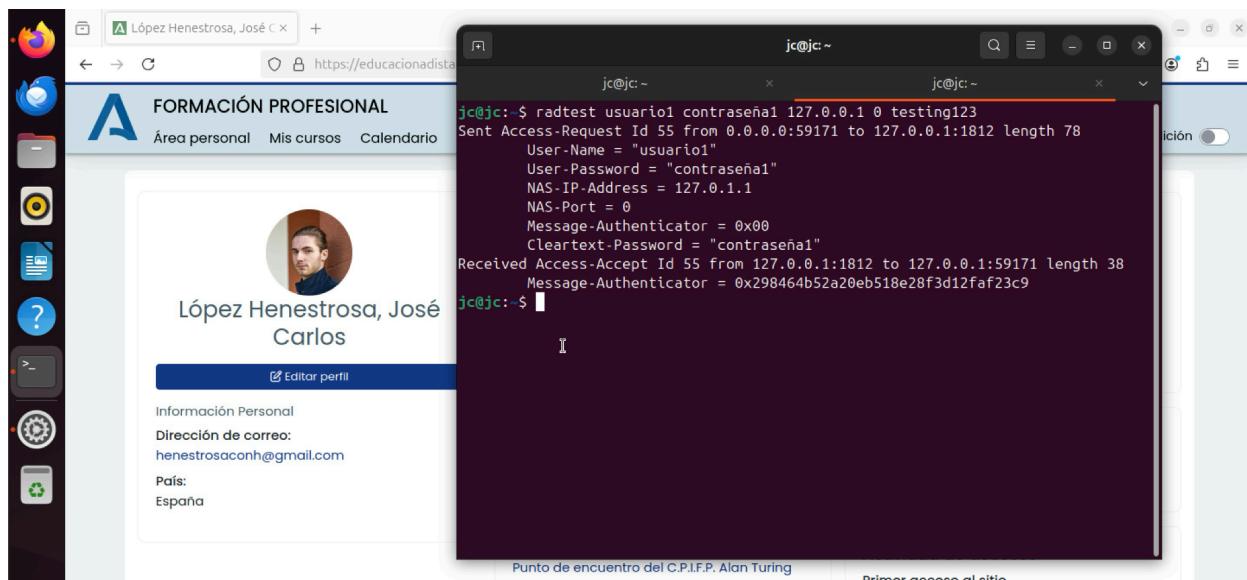
Como estamos realizando las pruebas desde la misma máquina donde está FreeRADIUS, tenemos que usar la contraseña por defecto para realizar tests, la cual es testing123.

Para realizar la prueba, ejecutamos el siguiente comando:

```
radtest usuario1 contraseña1 127.0.0.1 0 testing123
```

Donde:

- **usuario1:** Nombre de usuario que configuramos en el archivo `users`.
- **contraseña1:** Nombre de usuario que configuramos en el archivo `users`.
- **127.0.0.1:** IP del servidor RADIUS (tendríamos que cambiarla por una IP real si estuviéramos en otra máquina).
- **0:** Número de puerto NAS (0 para pruebas locales).
- **testing123:** Secreto compartido configurado en `clients.conf` para hacer tests con el localhost.



Ejecución del comando `radtest usuario1 contraseña1 127.0.0.1 0 testing123`

Como podemos apreciar, el usuario fue autenticado correctamente, ya que recibimos el mensaje `Access-Accept` por parte del servidor.

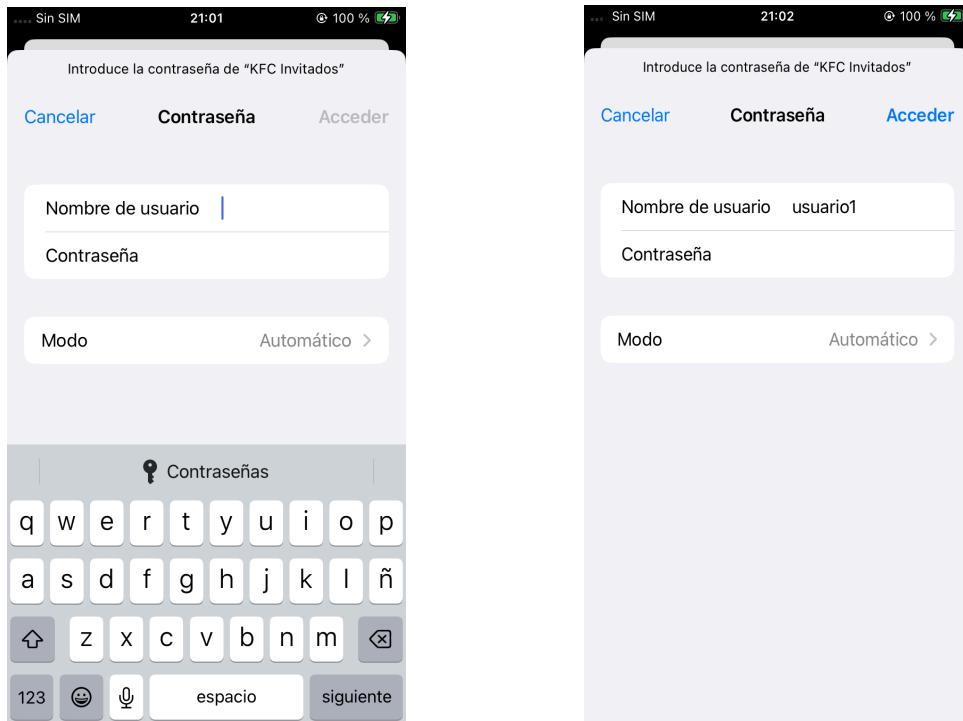
Demostración de que el usuario se conecta correctamente

Para comprobar que el router se ha configurado correctamente, vamos a usar un dispositivo móvil para conectarnos a la red. Para ello, abrimos los ajustes de Wi-Fi del dispositivo y comprobamos que la red KFC Invitados invitados está disponible, el cual es el nombre que recibe la red que hemos configurado previamente (no confundir con KFC Invitados 5G).



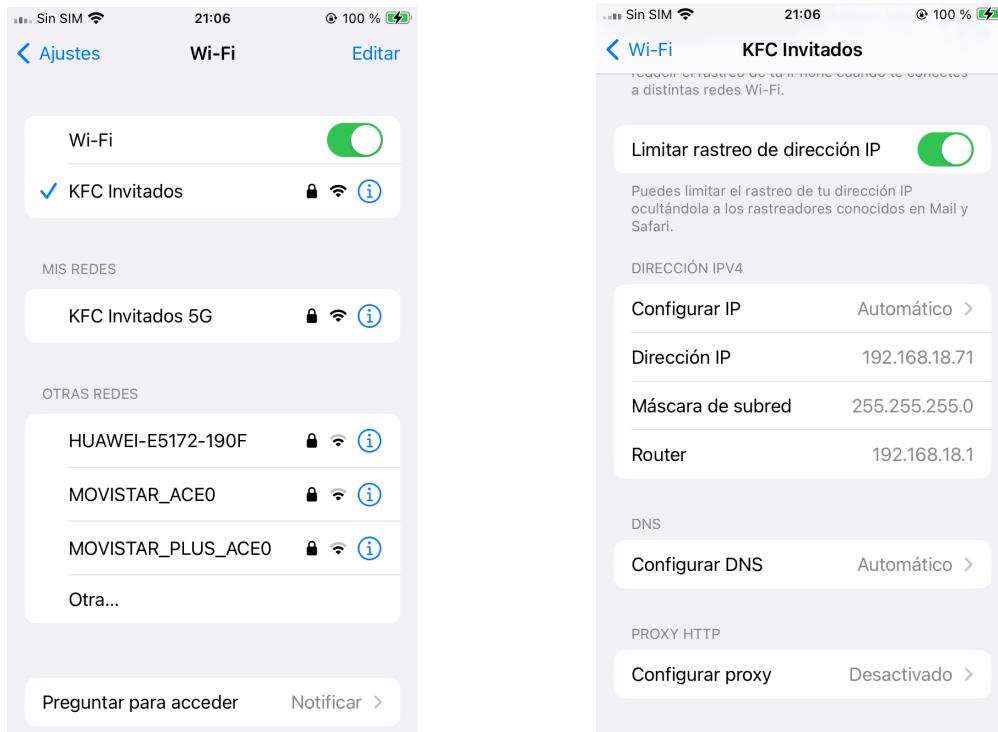
Lista de redes disponibles. KFC Invitados se encuentra entre ellas.

Pulsamos sobre la red KFC Invitados y observamos que se abre una pantalla en el dispositivo móvil solicitándonos el usuario y contraseña para conectarnos.



Por motivos de seguridad, Apple no muestra el texto introducido en los campos de texto de tipo contraseña. Sin embargo, he introducido la clave que establecimos en el apartado de configuración del servidor de RADIUS para este usuario (usuario1), que es contraseña1.

Pulsamos sobre el botón **Acceder** y veremos que el dispositivo se conecta a la red, lo cual indica que la red configurada y el servidor RADIUS funcionan correctamente.



Bibliografía

- Andres Sevillano Molina. (2021, 16 de febrero). *Instalación y configuración servidor RADIUS Ubuntu*. YouTube. <https://youtu.be/8tbAzjj6y7Q>