UNIVERSIDAD SAN CARLOS DE GUATEMALA

CENTRO UNIVERSITARIO DE OCCIDENTE

DIVISIÓN CIENCIAS DE LA INGENIERÍA

CARRERA DE INGENIERÍA CIENCIAS Y SISTEMAS

LABORATORIO REDES DE COMPUTADORAS 1

ING: FRANCISCO ROJAS

ESTUDIANTE:

201730919 - Bryan René Gómez Gómez

TEMA: "Manual Técnico - Primer Proyecto"

FECHA: 19 de marzo de 2,021

OBJETIVOS

General

- Disminuir la contaminación radioeléctrica de una red, gestionando la transmisión de frecuencia de la misma.

Específicos

1. Aplicar conceptos recibidos en clase magistral y laboratorio acerca de la gestión de una red mediante una Access Point.
2. Monitorear la potencia de frecuencia de una red.
3. Gestionar la transmisión de frecuencia de una red.

ÍNDICE

DESCRIPCIÓN DEL PROBLEMA

Se necesita disminuir la contaminación radioeléctrica de una red, gestionando la transmisión de frecuencia de una red y monitoreando la potencia mediante otro dispositivo idealmente que sea un móvil mediante una red.

Gestionar la frecuencia de la red mediante una USB Live con características de escritura, con un Sistema Operativo GNU/Linux derivado de Debian idealmente que sea en modo estándar (sólo texto), generando una red tipo ad hoc donde el Access Point será nuestra laptop, este funcionara como un puente donde nuestro gateway será el encargado de disponer las direcciones IP´s.

Monitorear la potencia de la frecuencia de la Red mediante un dispositivo móvil con la ayuda de la aplicación WiFi Analyzer.

REQUERIMIENTOS TÉCNICOS

REQUERIMIENTOS MÍNIMOS DE HARDWARE

- **Procesador:** Core
- **Memoria RAM:** 2 Gigabytes (GB)
- **USB Almacenamiento Persistente:** 4 Gigabytes (GB)
- **USB Almacenamiento LIVE:** 4 Gigabytes (GB)
- **Tarjeta de Red:** REALTEK RTL8822BR 802.11ac
- **Dispositivo Móvil:** Redmi 7

REQUERIMIENTOS MÍNIMOS DE SOFTWARE

- **Sistema Operativo:** debian-live-10.8.0-amd64-cinnamon+nonfree
- **bridge-utils**
- **net-tools**
- **network-manager**
- **WiFi Analyzer**
- **Rufus**
- **nmcli**

HERRAMIENTAS PARA EL DESARROLLO

Debian GNU/Linux

Es un sistema operativo libre, desarrollado por miles de voluntarios de todo el mundo, que colaboran a través de Internet.

La dedicación de Debian al software libre, su base de voluntarios, su naturaleza no comercial y su modelo de desarrollo abierto la distingue de otras distribuciones del sistema operativo GNU. Todos estos aspectos y más se recogen en el llamado Contrato Social de Debian.

Debian GNU/Linux puede utilizar distintos mecanismos de instalación, como son: DVD, CD, USB, e incluso directamente desde la red (este último depende de la velocidad de la red del usuario).

Bash

GNU Bash o simplemente Bash (Bourne-again shell) es un lenguaje de órdenes y shell de Unix escrito por Brian Fox para el Proyecto GNU como un reemplazo de software libre para el shell Bourne.

Lanzado por primera vez en 1989, se ha utilizado ampliamente como el intérprete de inicio de sesión(login) predeterminado para la mayoría de las distribuciones de GNU/Linux y Mac OS X de Apple hasta la versión 10.15. Una versión también está disponible para Windows 10 y Android. También es el intérprete de órdenes de usuario predeterminado en Solaris 11.

C

Es un lenguaje de programación diseñado en 1979 por Bjarne Stroustrup. La intención de su creación fue extender al lenguaje de programación C mecanismos que permiten la manipulación de objetos. En ese sentido, desde el punto de vista de los lenguajes orientados a objetos, C es un lenguaje híbrido.

Posteriormente se añadieron facilidades de programación genérica, que se sumaron a los paradigmas de programación estructurada y programación orientada a objetos. Por esto se suele decir que el C es un lenguaje de programación multiparadigma.

bridge-utils (Paquete)

Este paquete contiene utilidades para configurar el puente Ethernet de Linux en Linux. El puente Ethernet de Linux se puede utilizar para conectar varios dispositivos Ethernet juntos.

La conexión es totalmente transparente: los hosts conectados a un dispositivo Ethernet ven los hosts conectados a los otros dispositivos Ethernet directamente.

net-tools (Paquete)

El paquete Net-tools contiene una colección de programas que forman la base del trabajo en red en Linux.

Programas instalados: arp, dnsdomainname (enlace a hostname), domainname (enlace a hostname), hostname, ifconfig, nameif, netstat, nisdomainname (enlace a hostname), plipconfig, rarp, route, slattach y ypdomainname (enlace a hostname)

network manager

NetworkManager es un servicio de red del sistema que administra sus dispositivos y conexiones de red e intenta mantener la conectividad de red activa cuando está disponible. Administra dispositivos Ethernet, WiFi, banda ancha móvil (WWAN) y PPPoE, al mismo tiempo que proporciona integración VPN con una variedad de servicios VPN diferentes.

De forma predeterminada, la administración de red en Ubuntu Core es manejada por networkd y netplan de systemd. Sin embargo, cuando se instala NetworkManager, tomará el control de todos los dispositivos de red en el sistema creando un archivo de configuración de netplan en el que se establece como el renderizador de red predeterminado.

Rufus

Es una aplicación portable, libre y de código abierto para Microsoft Windows que se puede usar para formatear y crear unidades flash USB de arranque o Live USB. Está desarrollado por Pete Batard de Akeo Consulting.

WiFi Analyzer

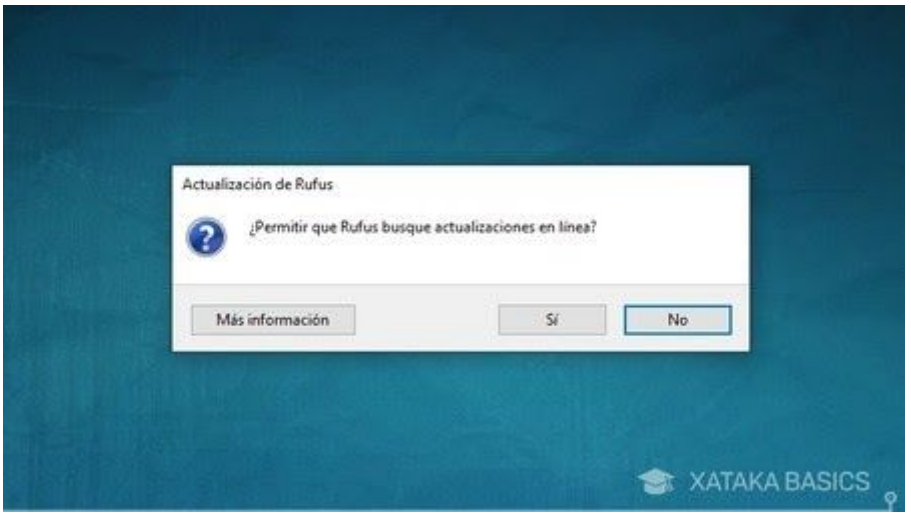
Muestra los canales Wi-Fi que le rodean. Le ayuda a encontrar un canal menos concurrido para su enrutador inalámbrico.

INSTALACIONES Y CONFIGURACIONES DEL SOFTWARE DE DESARROLLO

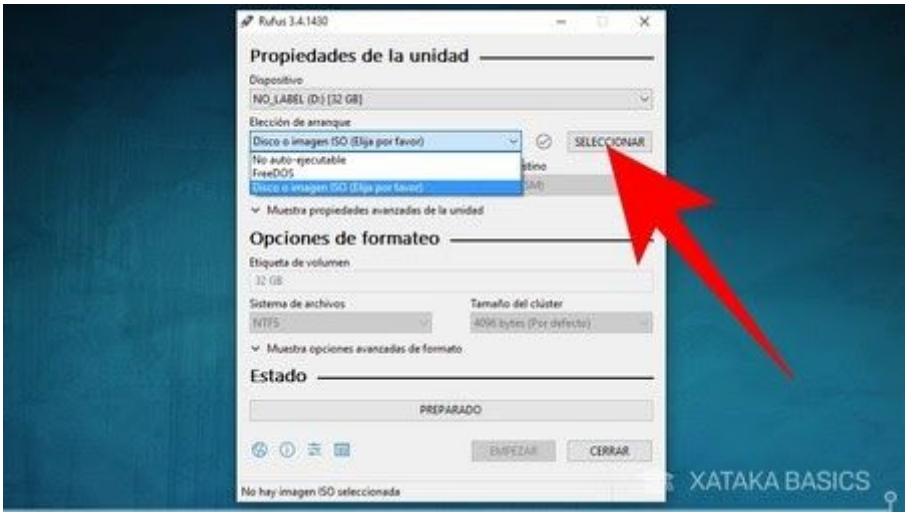
Creación de USB Live

Para realizar la creación de una USB Live necesitamos utilizar Rufus, primero tienes que haber descargado la imagen ISO que quieras utilizar para crear un USB Live.

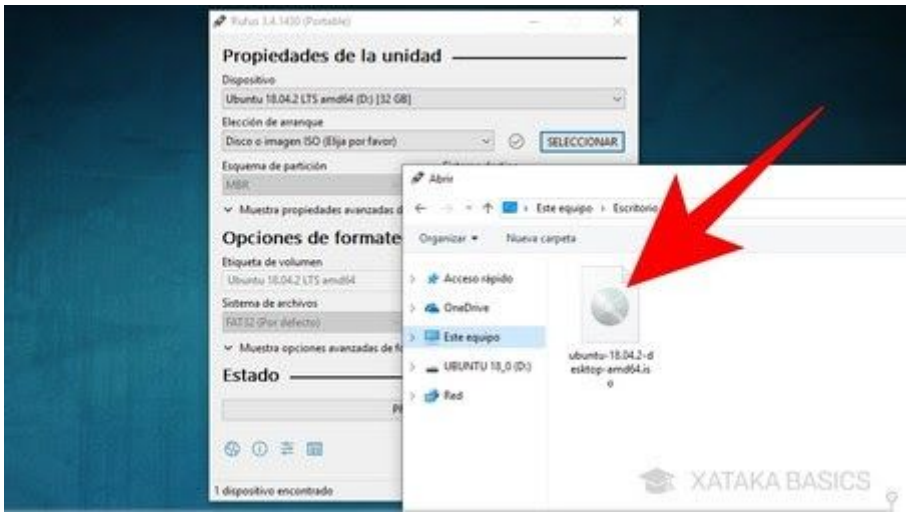
A continuación, tienes que ir a la web oficial de Rufus. En ella baja hasta el apartado Descargar, y pulsa sobre la versión que quieres bajarte, la completa y normal o la portátil para llevar en un USB y está preparada para funcionar desde una unidad externa que luego metas en un ordenador con Windows. Realmente no hay mucha diferencia entre ambas, sólo que la portátil está optimizada para usarse a través de unidades externas.



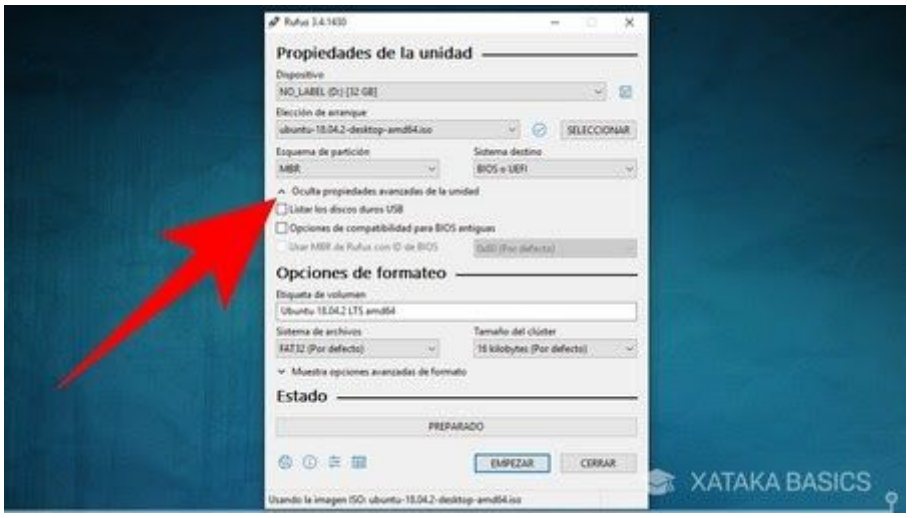
Cuando descargues la aplicación no la tienes que instalar. Simplemente pulsa sobre el archivo .exe y arrancará. Lo primero que verás es una ventana de actualización donde puedes hacer que Rufus use la conexión a Internet de tu ordenador para ver si hay versiones nuevas. Si te lo acabas de descargar de la web, no hace falta que hagas la comprobación.



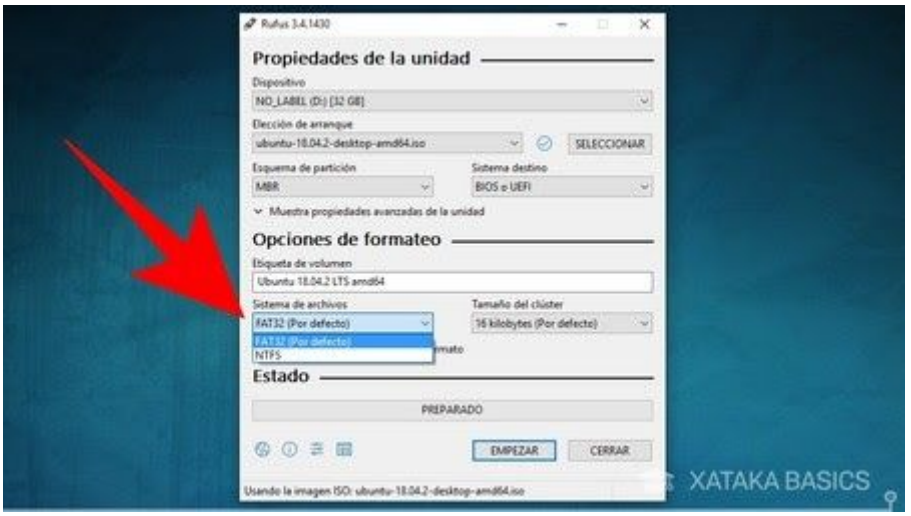
Ahora mete el USB en el ordenador para que se activen todas las opciones, verás que este aparece donde pone Dispositivo arriba del todo. A continuación, selecciona una opción en Elección de arranque, que puede ser utilizar una imagen como no autoejecutable, instalar FreeDOS (la versión libre y gratis del viejo MSDOS), o Disco o imagen ISO, que es la que debes elegir para crear un USB de arranque. Ahora, pulsa en el botón Seleccionar una vez elijas una de las opciones.



Cuando pulses en seleccionar, se abrirá una ventana del explorador para que busques y selecciones la imagen .ISO que quieres utilizar para crear el USB de arranque. Para seleccionarla simplemente haz doble click sobre ella.



Tras elegir la imagen, a continuación debes de designar el tamaño de almacenamiento persistente. También puedes desplegar un menú propiedades avanzadas para detectar discos duros o hacer que el USB sea compatible con versiones antiguas de BIOS.



El siguiente paso importante es elegir un sistema de archivos para cuando se formatee tu USB antes de instalar en él la imagen ISO que hayas seleccionado. Por defecto se utilizará el viejo FAT32, aunque también tendrás opción de utilizar el NTFS de Windows. A la derecha, también tendrás una opción para cambiar el tamaño del clúster a la hora de formatear, aunque esto no es necesario tampoco que lo toques para crear las unidades de arranque.

Instalar bridge-utils

Para instalar bridge-utils en Debian ejecutar los siguientes comandos:

```
sudo apt-get update
```

```
sudo apt-get install bridge-utils
```

Instalar net-tools

Para instalar net-tools en Debian ejecutar los siguientes comandos:

```
sudo apt-get update
```

```
sudo apt-get install net-tools
```

Instalar y configurar Network Manager

Para instalar net-tools en Debian ejecutar los siguientes comandos:

```
sudo apt-get install network-manager
```

En caso de que usamos KDE o Gnome/Xfce, utilizaremos estas variantes respectivamente:

```
sudo apt-get install network-manager-kde
```

```
sudo apt-get install network-manager-gnome
```

Es necesario luego que comentemos el archivo / etc/network/interfaces para que quede de la siguiente forma:

```
auto lo
```

```
iface lo inet loopback
```

Este paso no es obligatorio pero sí acelera el proceso de detección de la red por parte del NetworkManager. En Debian son necesarios algunos pasos más. Debemos añadir al usuario que usará el NetworkManager al grupo netdev:

```
adduser su_usuario netdev
```

Luego para que funcione correctamente es necesario reiniciar la sesión ya que la modificación de la asociación grupo-usuario no quedará vigente hasta que esto ocurra.

Es posible de que nos topemos con un problema como este:

```
nma_dbus_init(): could not acquire its service.  dbus_bus_acquire_service() says:
'Connection "1.38" is not allowed to own the service :
"org.freedesktop.NetworkManagerInfo" due to security policies in the configuration file'
```

Esto ocurre porque en el archivo de configuración que maneja la permisología sobre el cliente existen problemas con el usuario especificado. El archivo /etc/dbus-1/system.d/nm-applet.conf contiene dichos permisos, simplemente añadimos nuestro usuario como una vía “rápida” para resolver el problema. De lo contrario podemos indagar más en el uso del NetworkManager de este fichero:

```
<policy user="icomputo" allow own="org.freedesktop.NetworkManagerInfo" >
```

```
<allow send_destination="org.freedesktop.NetworkManagerInfo"/>;
```

```
<allow send_interface="org.freedesktop.NetworkManagerInfo>
```

```
</policy>

<policy user="root" >

<allow own="org.freedesktop.NetworkManagerInfo" >

<allow send_destination="org.freedesktop.NetworkManagerInfo" >

<allow send_interface="org.freedesktop.NetworkManagerInfo" >

</policy>
```

Notarán que las políticas para root y para icomputo (el usuario) son las mismas. Con esto ya debe correr. Para ejecutar el applet, vamos a una consola como usuario normal:

```
nm-applet
```

Compartir una Red Física por WiFi mediante

Debemos instalar hostapd y bridge-utils

- Debian y sistemas basados en Debian (Ubuntu, Kali, Linux Mint etc...)
  ```
  sudo apt-get install hostapd
  ```

Necesitamos tener bridge-utils

- Debian y sistemas basados en Debian (Ubuntu, Kali, Linux Mint etc...)
  ```
  sudo apt-get install bridge-utils
  ```

También hace falta iw y iw-tools pero estos paquetes vienen instalados de forma nativa en todas las distribuciones

Prevenir conflictos con Network Manager

En la wiki debian aconseja desinstalar todos los paquetes relacionados con network-manager para eludir conflictos.

Es una postura "un tanto radical". Eficaz, sin dudas, pero algo radical.

Lo que vamos a hacer es simplemente parar network manager

```
sudo systemctl stop NetworkManager.service
```

```
sudo systemctl disable NetworkManager.service
```

Si no es suficiente crearemos una excepción para la(s) interfaz(ces) que da(n) problema.

Esto se hace modificando el fichero NetworkManager.conf

```
sudo gedit /etc/NetworkManager/NetworkManager.conf
```

Si es la tarjeta wifi interna del portátil será probablemente wlan0 o enselp0 (o algo así según la nueva nomenclatura que aconsejo abandonar) añadimos al fichero

```
[keyfile]
unmanaged-devices=interface-name:wlan0   # añadido para hot spot hostapd
```

Guardamos los cambios y listo.

Recordar que si editas el fichero debemos borrar lo que hemos añadido para que network manager pueda manejarla otra vez. (para conectarse con ella)

Configurar hostapd

Debemos indicar al demonio hostapd la ruta hacía el fichero de configuración que vamos a redactar enseguida.

Para ello editamos el fichero /etc/default/hostapd

```
sudo gedit /etc/default/hostapd
```

Añadimos

```
DAEMON_CONF="/etc/hostapd/hostapd.conf"
```

Creamos el fichero de configuración hostapd (/etc/hostapd/hostapd.conf)

Abrir su editor de texto con privilegios de administrador

```
sudo nano
```

Luego añadimos algo así

```
sudo nano /etc/hostapd/hostapd.conf
```

```
interface=wlan0
bridge=br0
driver=nl80211
auth_algs=1
ignore_broadcast_ssid=0
logger_syslog=-1
logger_syslog_level=0
hw_mode=g
wmm_enabled=1
ssid=Compartir_es_vivir
channel=11
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=¡N()L0pong@sFAC1l!
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Algunas precisiones:

- **interface**: Ponemos la interfaz wifi para hacer el hotspot
- ssid: Ponemos el nombre que queremos
- **hw_mode**: Lo dejamos en g. Para habilitar el estándar "n" se añade wmm_enabled=1
- **channel**: He puesto 11. Una buena idea es hacer un escaneo para ver qué canal está menos utilizado.
- **wpa_passphrase**: poner una contraseña de al menos de 12 caracteres mezclando todo tipos de caracteres (mayúsculas, minúsculas, números y caracteres especiales

Configurar las interfaces

Debemos editar el fichero /etc/network/interfaces (con privilegios de administrador)

```
sudo nano /etc/network/interfaces
```

Debemos añadir lo siguiente:

```
# Internet mediante interfaz ethernet
 auto eth0
 allow-hotplug eth0
 iface eth0 inet dhcp
# Hot Spot con interfaz wifi
 auto br0
 iface br0 inet dhcp
 bridge-ports eth0 wlan0
```

Arrancando el Hot Spot

Para desplegar el Hot Spot ejecutamos sucesivamente los tres comandos siguientes

a. sudo /etc/init.d/networking stop
b. sudo /etc/init.d/networking start
c. sudo /etc/init.d/hostapd restart

Cómo configurar el puente de red en Debian

Para crear un puente de red usando nmcli, ejecute el siguiente comando.

```
sudo nmcli conn add type bridge con-name br0 ifname br0
```

```
aaronk@tecmint:~$ sudo nmcli conn add type bridge con-name br0 ifname br0
Connection 'br0' (e7385b2d-0e93-4a8e-b9a0-5793e5a1fda3) successfully added.
aaronk@tecmint:~$
```

Luego agregue la interfaz Ethernet como un puerto en el puente como se muestra (recuerde reemplazar enp1s0 con el nombre de su dispositivo).

```
sudo nmcli conn add type ethernet slave-type bridge con-name bridge-br0 ifname enp1s0 master br0
```

```
aaronk@tecmint:~$ sudo nmcli conn add type ethernet slave-type bridge con-name bridge-br0 ifname enp1s0 master br0
Connection 'bridge-br0' (7eca4e86-fd8d-4a74-a53b-748b306fc827) successfully added.
aaronk@tecmint:~$
```

A continuación, confirme que se ha creado el puente mostrando todas las conexiones de red.

```
sudo nmcli conn show --active
```

```
aaronk@tecmint:~$ sudo nmcli conn show --active
NAME                UUID                                  TYPE      DEVICE
Ethernet connection 1  525284a9-60d9-4396-a1c1-a37914d43eff  ethernet  enp1s0
br0                 e7385b2d-0e93-4a8e-b9a0-5793e5a1fda3  bridge    br0
aaronk@tecmint:~$
```

A continuación, active la conexión de puente de la siguiente manera (puede utilizar el nombre de la conexión/interfaz o el UUID).

```
sudo nmcli conn up br0
```

or

```
sudo nmcli conn up e7385b2d-0e93-4a8e-b9a0-5793e5a1fda3
```

```
aaronk@tecmint:~$ sudo nmcli conn up br0
Connection successfully activated (master waiting for slaves) (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConn
ection/5)
aaronk@tecmint:~$
```

Luego, desactive la interfaz o la conexión Ethernet.

```
sudo nmcli conn down Ethernet\ connection\ 1
```

or

```
sudo nmcli conn down 525284a9-60d9-4396-a1c1-a37914d43eff
```

```
aaronk@tecmint:~$ sudo nmcli conn down Ethernet\ connection\ 1
Connection 'Ethernet connection 1' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnec
tion/3)
aaronk@tecmint:~$
```

Ahora intente ver las conexiones activas una vez más, la interfaz Ethernet ahora debería ser esclava en la conexión de puente como se muestra en la siguiente captura de pantalla.

```
sudo nmcli conn show --active
```

Para abrir la aplicación nm-connection-editor, ejecute el siguiente comando desde la terminal.

Conexión de WLAN a Ethernet para punto de acceso (modo de infraestructura) para teléfonos Android

A continuación, elimine la dirección IP adjunta de la tarjeta Ethernet eth0. El puente no funcionará cuando se establezca una dirección IP.

ip addr flush dev eth0

A continuación, active la red IPv4 para su tarjeta inalámbrica. Esto es necesario, de lo contrario, uno de los siguientes pasos dará el error "no se puede agregar wlan1 al puente br0: operación no admitida".

iw dev wlan1 configuró 4addr en

A continuación, cree el puente br0 real con el programa auxiliar brctl:

brctl addbr br0 eth0 wlan1

A continuación, haga un puente entre Ethernet e inalámbrico. El orden de los dos últimos argumentos no es importante:

brctl addif br0 eth0 wlan1

A continuación, traiga el puente recién creado, como un dispositivo virtual:

conjunto de enlaces ip dev br0 up

En este punto, habrá perdido la conexión a su LAN / WAN. Debe configurar una dirección IP, máscara de red, enrutador, etc. para el puente. Hacemos esto a través de DHCP:

dhclient br0

Ahora debería poder acceder a Internet nuevamente. ¡Pruébalo! Si no funciona, reinicia tu computadora. No hemos realizado cambios permanentes en su sistema (¡otra ventaja de este método!)

Hasta ahora tan bueno. Ahora tenemos que crear nuestra red inalámbrica real en modo AP y usar nuestro teléfono Android para probarla. Instalar hostapd:

apt-get install hostapd

Cree un archivo de configuración en algún lugar de su unidad. Elegí la ubicación /etc/hostapd/my-wlan.conf. Asegúrese de tener el controlador correcto configurado para su tarjeta (consulte el blog mencionado anteriormente para obtener más información. N180211 debería funcionar en la mayoría de los casos):

interfaz = wlan1
controlador = nl80211
wmm_enabled = 0
ssid = nombre de red
canal = 6
puente = br0

# establece el modo de wifi, depende de los dispositivos que utilizará. Puede ser a, b, g, n. Establecer en g asegura la compatibilidad con versiones anteriores.
hw_mode = g

#macaddr_acl establece opciones para el filtrado de direcciones mac. 0 significa "aceptar a menos que esté en la lista de denegados"
macaddr_acl = 0

# establecer ignore_broadcast_ssid en 1 inhabilitará la transmisión de ssid
ignore_broadcast_ssid = 0

#Sets algoritmo de autenticación
# 1 - solo autenticación de sistema abierto
# 2: autenticación de sistema abierto y autenticación de clave compartida
auth_algs = 1

Establece la autenticación WPA y WPA2
La opción #wpa establece qué implementación de wpa usar
# 1 - solo wpa
# 2 - solo wpa2
# 3 - ambos
wpa = 3

# establece la contraseña de wpa requerida por los clientes para autenticarse en la red
wpa_passphrase = 12345678

```
#sets gestión de claves de wpa
wpa_key_mgmt = WPA-PSK

#establece el cifrado utilizado por WPA
wpa_pairwise = TKIP

# establece el cifrado utilizado por WPA2
rsn_pairwise = CCMP
```

Posteriormente debe de parar el servicio de NetworkManager:

```
sudo service NetworkManager stop
```

Ahora, simplemente inicie hostapd con este archivo de configuración como único argumento:

```
hostapd /etc/hostapd/my-wlan.conf
```

Crear una red ad hoc en Debian (Otra Opción)

Configuración del servidor

Primero hay que dar de baja a la interfaz de red. En dependencia del dispositivo que utilicemos habrá que especificar la entrada correcta.

```
ifconfig wlan0 down
```

Ahora procedemos a la configuración de la interface, pasando a modo ad-hoc el wireless tengan en cuenta que no todas las tarjetas inalámbricas pueden hacer esto, debido a que no todas tienen drivers nativos o completos para linux, para pasarla a modo ad-hoc ejecutamos lo siguiente:

```
iwconfig wlan0 mode ad-hoc
```

Continuamos dándole un nombre a la red que vamos a crear, este nombre es el que se podrá ver al detectar la red ya sea por medio de un #iwlist o algún software para wifi (ejemplo wicd). Para ello ejecutamos el siguiente comando:

```
iwconfig wlan0 essid "miRed"
```

Luego de ello procedemos a configurar el canal y es por medio del cual fluirán los datos. Si existen más redes en el área les recomendaría utilizar un canal que este libre.

```
iwconfig wlan0 channel 6
```

Seguridad en la red por medio de contraseña, este paso es opcional esto dependerá de en donde vivan o los datos que manejan en la red, para ello ejecutamos el siguiente comando:

```
iwconfig wlan0 key "0123456789"
```

Ahora le damos una dirección ip al servidor, esto servirá para que el cliente pueda encontrar al servidor dentro de la red y viceversa, no asignaremos mascar de subred, dejaremos que el sistema se encargue de ello, así que solo ejecutamos el siguiente comando:

```
ifconfig wlan0 192.162.0.1
```

Ahora procedemos a habilitar el redireccionamiento. Ejecutamos el siguiente comando:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Por último configuramos un cortafuegos (firewall) para redireccionar los paquetes desde una interfaz a otra. En este caso usaremos **iptables** que permitirá compartir la conectividad principal al cliente. Para ello ejecutamos:

```
iptables -t nat -A POSTROUTING -s eno1 -j MASQUERADE
```

Configuración del Cliente

Para configurar el cliente es de la misma manera que el servidor sólo que con algunos parámetros invertidos. En este caso de ejemplo usaremos otra interfaz de red para que el usuario no se pierda en la explicación. En este caso usaremos una tarjeta de red Atheros (ath0).

```
ifconfig ath0 down
```

```
iwconfig ath0 mode ad-hoc essid "miRed" channel 6 key "0123456789"
```

Pasaremos a configurar ahora el ip de la máquina cliente. Recuerden que el servidor tenía el **192.168.0.1**. Pondremos otra dirección:

```
ifconfig ath0 192.162.0.2
```

Ahora procedemos a enrutar el servidor con el cliente, eso lo hacemos con el siguiente comando, en donde la ip que escribimos tiene que ser la del servidor:

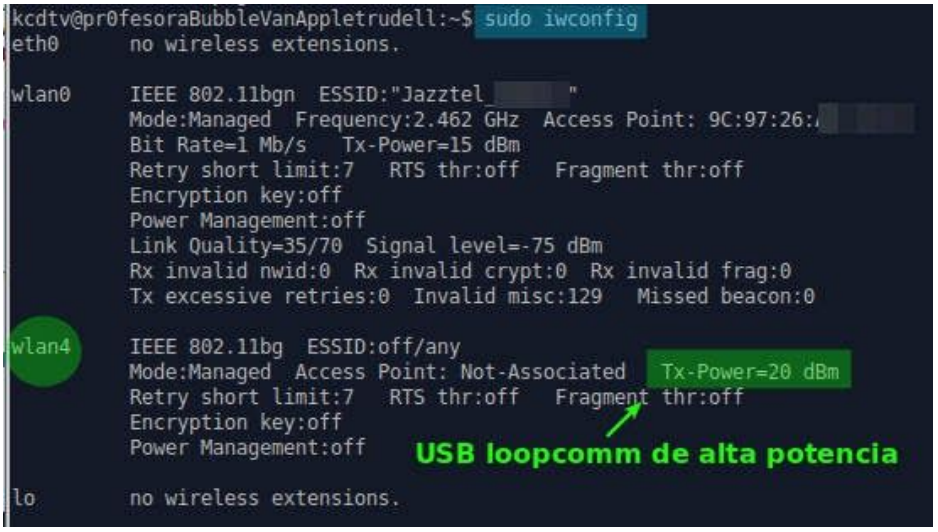
route add default gw 192.162.0.1

Gestionar la potencia en salida de nuestra red

Obtener la latencia de Signal mediante:

sudo iw dev -Nombre Tarjeta WiFi- station get -MAC Dispositivo- | grep signal

Es el caso de RTL8187l



Se ven dos interfaces

1. wlan0 :

   - La tarjeta interna con una potencia máxima de 16dBm (por debajo del máximo legal autorizado)

2. wlan4 :

   - El USB loopcomm LP-9637c con una potencia que alcanza el máximo legal : 20dBm

Para llegar a 30dBm de potencia :

1. "Bajo mi interfaz con ifconfig

sudo ifconfig wlan4 down

2. Cambio mi legislación local por la de la Guyana británica con iw

sudo iw reg set GY

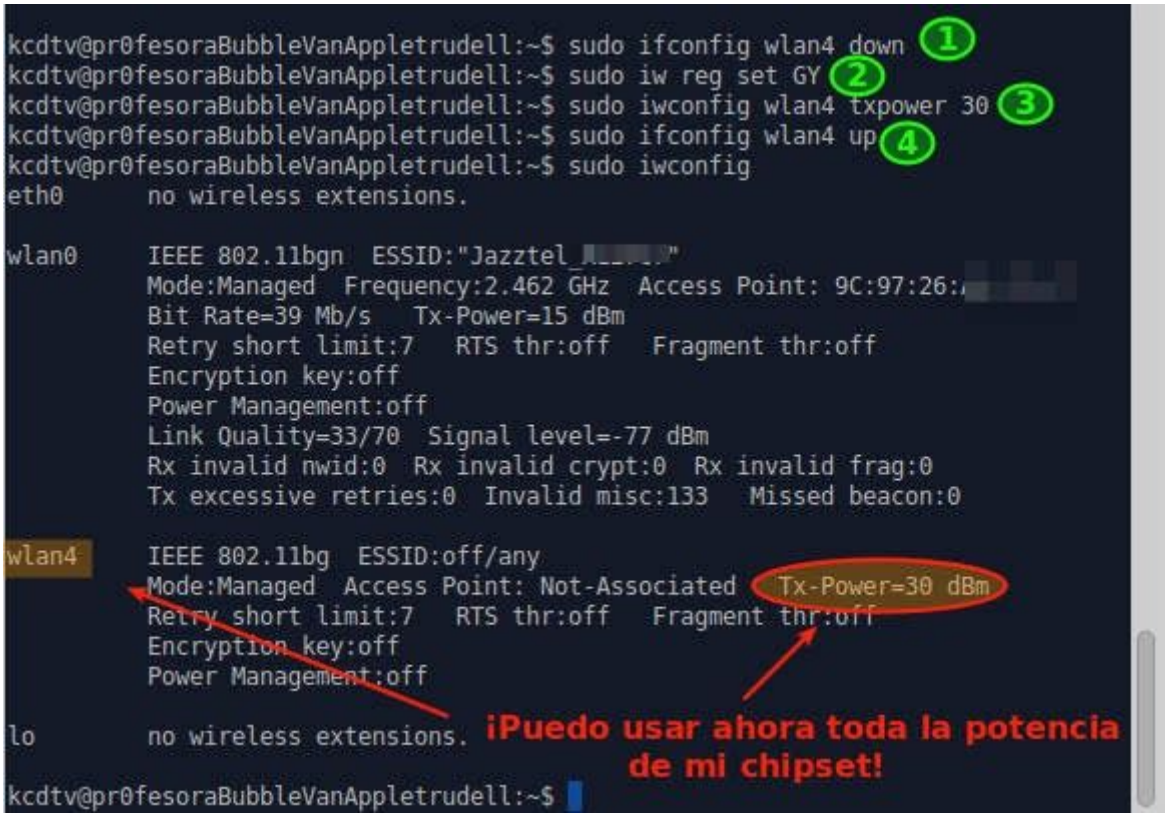
3. Aumento mi potencia con iwconfig

sudo iwconfig wlan4 txpower 30

4. Vuelvo a "subir" mi interfaz

sudo ifconfig wlan4 up

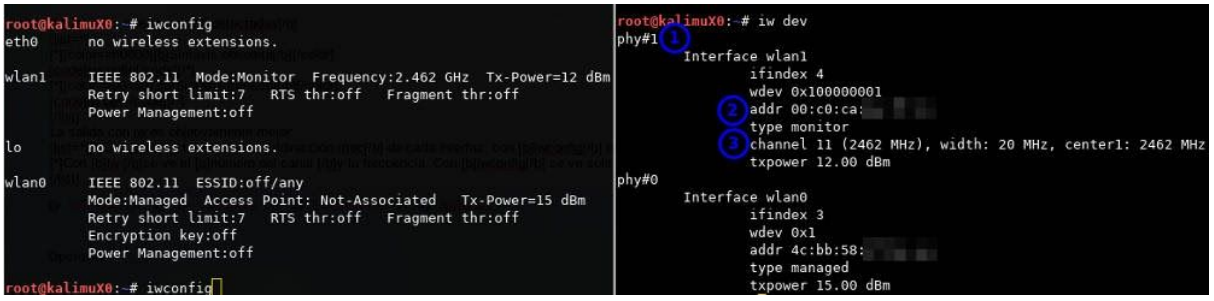
Una vez hecho verifico mi potencia con iwconfig...



Uso de iw en lugar de iwconfig

iw dev

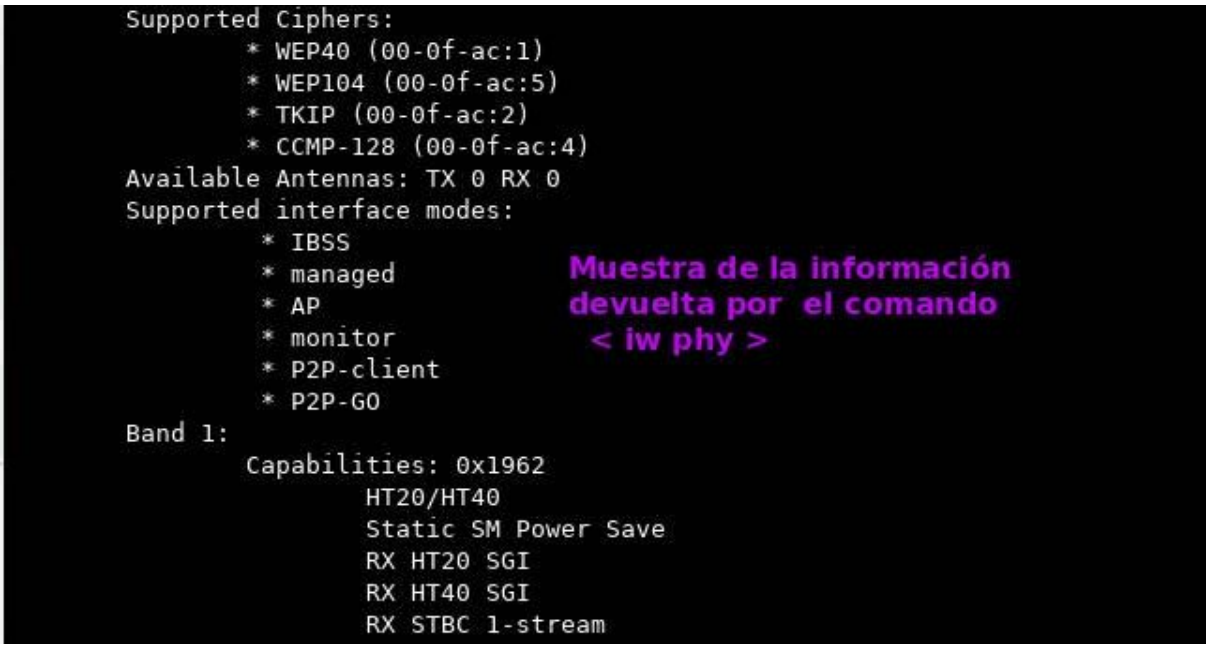
La salida con iw es objetivamente mejor:



1. Con iw sabemos la interfaz "física" (phyX) para cada interfaz, con iwconfig no la conocemos.
2. Con iw tenemos a la dirección mac de cada interfaz, con iwconfig no tenemos nada.
3. Con iw se ve el número del canal y la frecuencia. Con iwconfig se ve solo la frecuencia y es molesto, nosotr@s humanos usamos el número del canal, no la frecuencia en Mhz

Con iw dev tenemos más información y la salida está mejor ordenada, más fácil de consultar.

`iw phy`



Permite apreciar toda la potencia del comando con iw con una salida ultra detallada sobre nuestras interfaces wifi. Lo sabrás absolutamente todo

Fijar un canal

`iw dev wlan0 set channel 11`

Conectar a una red abierta

`iw wlan1 connect <nombre_de_la_red_abierta>`

Aumentar la potencia

Suponemos que nuestra interface wlan2 es una AWUS036H con chipset rtl8187l podríamos subir su potencia hasta 30 dBm (1000 mW) así:

`iw wlan2 set txpower fixed 30`

Con iw podemos además elegir entre "auto" "fixed" o "limit".

Modo monitor

El proceso es algo diferente con iw y es más cercano a lo que se hace con airmon-ng (porque airmon-ng emplea iw) iw permite la creación de interfaces virtuales, iwconfig no sabe hacer esto, y se emplea esta característica (crear interfaces virtuales) para activar el modo monitor.

iw wlan2 interface add wlan2mon type monitor

Notas que haciendo así tenéis a dos interfaces (wlan2 en modo managed y wlan2mon en modo monitor) para una misma interfaz.

Para deshabilitar el modo monitor; con iwconfig pasamos de un modo a otro (managed para conectarse), con iw se borra la interfaz en modo monitor.

iw wlan2mon del

Pero lo más interesante es todo lo que se puede hacer con iw y que no se puede hacer con iwconfig.

Un ejemplo "emblemático" para nuestro foro: Un escaneo con iw permite sacar el número de serie de una livebox y poder así generar su PIN por defecto…

Para generar el PIN es absolutamente necesario obtener el número de serie del dispositivo.

El número de serie se emite en texto claro en los parámetros avanzados WPS de las respuestas PROBE de las livebox.

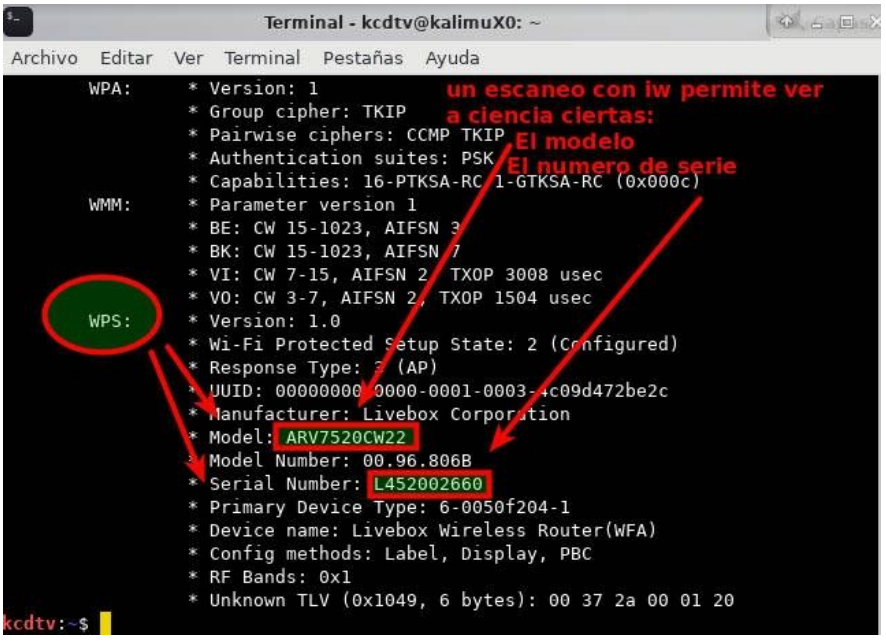
Hay varias formas de proceder, una forma universal y que no requiere modo monitor es usar el mismísimo iw.

sudo iw <inetrfaz_wifi> scan

Nos devolverá la información contenida en el probe de nuestra livebox si estamos cerca de ella.

Si estamos a distancia de nuestra box deberemos probablemente emplear un escaneo más activo, utilizando wash y su opción -j por ejemplo.

Ejemplo de serial contenido en la respuesta PROBÉ de una livebox:



Instalación Configuraciones de Recursos Mediante los Scripts

Al obtener los scripts correspondientes podemos ejecutarlos y realizar las instalaciones de dependencias junto a las configuraciones sin la necesidad de realizar lo anterior. En el repositorio están los siguientes scripts:

1. Librerias.sh
2. Crear Puente.sh
3. Crear y Configurar Red.sh

Librerías.sh:

Este script instala las dependencias necesarias para realizar la configuración correspondiente de la red y del puente. Se ejecuta mediante el siguiente comando:

`sudo sh Librerias.sh`

Crear Puente:

Este script realiza la configuración del puente entre las interfaces de wireless y ethernet de nuestra computadora para que se conecte al gateway, al ejecutar el script se necesitan los siguientes parámetros:

1. Nombre del puente.
2. Nombre de la tarjeta de Ethernet.
3. Nombre de la tarjeta WiFi.
4. Nombre de la conexión cableada.

Se ejecuta con el siguiente comando:

`sudo sh Crear Puente.sh <Nombre del Puente> <Nombre de la tarjeta Ethernet> <Nombre de la tarjeta WiFi> <Nombre de la Conexión Cableada>`

Crear y Configurar Red.sh

Este script realiza la creación de de la red, junto a la configuración de la misma y depende de los siguientes parámetros:

1. Nombre de la red.
2. Contraseña.
3. Nombre de la tarjeta WiFi.

Se ejecuta el siguiente comando:

`sudo sh Crear y Configurar Red.sh <Nombre de la Red> <Contraseña> <Nombre de la tarjeta WiFi>`

MARCO TEÓRICO

Red ad hoc inalámbrica

Es un tipo de red inalámbrica descentralizada. La red es ad hoc porque no depende de una infraestructura preexistente, como routers (en redes cableadas) o de puntos de accesos en redes inalámbricas administradas. En lugar de ello, cada nodo participa en el encaminamiento mediante el reenvío de datos hacia otros nodos, de modo que la determinación de estos nodos hacia la información se hace dinámicamente sobre la base de conectividad de la red. Además del encaminamiento clásico, las redes ad hoc pueden usar un flooding (inundación de red) para el reenvío de datos.

Una red ad hoc se refiere típicamente a cualquier conjunto de redes donde todos los nodos tienen el mismo estado dentro de la red y son libres de asociarse con cualquier otro dispositivo de red ad hoc en el rango de enlace. Las redes ad hoc se refieren generalmente a un modo de operación de las redes inalámbricas IEEE 802.11.

También se refiere a la habilidad de un dispositivo de red de mantener la información del estado de conexión para cualquier cantidad de dispositivos en un rango de un enlace (o "salto" en argot de informática), y por lo tanto, es más a menudo una actividad de capa 2. Debido a esta única actividad de capa 2, las redes ad hoc por sí solas no soportan un ambiente de red con IP encaminable sin las capacidades adicionales de otra capa 2 o capa 3.

Este tipo de red permite la adhesión de nuevos dispositivos y así, con el solo hecho de estar en el rango de alcance de un nodo ya perteneciente a la red establecida. El protocolo que rige este tipo de comunicaciones es el 802.11, que define todos los parámetros necesarios para establecer la comunicación entre dispositivos inalámbricos. El principal inconveniente de este tipo de redes radica en el número de saltos que debe recorrer la información antes de llegar a su destino.

Cada nodo que transmite la información implica un salto, cuanto más saltos mayor es el tiempo que tarda en llegar la información a su destino y aumenta la probabilidad de que la información se corrompa con cada salto.

Puente o Bridge

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

Un bridge conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primero sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

Para hacer el bridging o interconexión de más de 2 redes, se utilizan los switch.

Contaminación Radioeléctrica

Es el tipo de contaminación que tiene origen en los campos electromagnéticos (CEM) que nos rodean. Los CEM son una combinación de ondas magnéticas y eléctricas que se desplazan simultáneamente y se propagan a la velocidad de la luz. Cuanto más alta sea su frecuencia mayor será la cantidad de energía que transporte la onda.

Dentro de ellos se pueden distinguir las radiaciones ionizantes (capaces de romper los enlaces que existen entre las moléculas) y no ionizantes. La Organización Mundial de la Salud (OMS) divide a su vez estas últimas en:

- Campos electromagnéticos estaticos: es decir, no variables en el tiempo. Están presentes en los sistemas electrolíticos de aplicación industrial experimental, los trenes de levitación magnética y los sistemas de resonancia magnética de los hospitales. Los campos magnéticos estáticos de alta intensidad pueden introducir leves trastornos en los latidos del corazón y un incremento anormal del ritmo cardiaco

(arritmia), pudiendo llegar en ciertos casos a poner en peligro la vida de las personas (fibrilación ventricular).

- FEB ó ELF: también conocidos como campos electromagnéticos de frecuencia extremadamente baja (hasta 300 Hz.). Están presentes en los equipos utilizados para la generación, transporte y distribución de energía eléctrica de frecuencia industrial (50 Hz), en los electrodomésticos (lavadoras, neveras, secadoras…), etc. Hay muy pocas pruebas experimentales de la afección de estos campos, sobre la fisiología y al comportamiento humano, a las intensidades que se pueden medir en cualquier domicilio.
- FI: son los campos de frecuencia intermedia (300 Hz - 10 MHz) que emiten las cocinas de inducción, los dispositivos antirrobo y sistemas de seguridad, las bombillas de bajo consumo, las pantallas de ordenador, etc. Pueden inducir corrientes eléctricas en el organismo humano, produciendo excitaciones nerviosas y musculares, a partir de una cierta intensidad. Aún no hay datos sobre los efectos que tendría la exposición a largo plazo a este tipo de campos, debido a que el número de estudios elaborados hasta hoy es muy escaso.
- RF: son campos de radiofrecuencia (10 MHz - 300 GHz.) Se incluyen las ondas de radio y de televisión, las antenas y radares, la telefonía móvil e inalámbrica, los dispositivos Wi-Fi y bluetooth, los hornos microondas, etc. No hace falta decir que actualmente el uso de estas fuentes de radiofrecuencia está muy extendido, pero sí que cabría diferenciar los que operan cerca del cuerpo humano (teléfonos móviles) de los que lo hacen lejos (antenas y radares).

Los principales efectos biológicos que producen estas radiaciones no ionizantes son el calentamiento, la alteración de reacciones químicas y la inducción de corrientes eléctricas en el interior de los tejidos. La dificultad para medir las consecuencias biológicas de esta contaminación radioeléctrica, no está en saber por encima de que umbrales se producen tales efectos (esto ya se conoce), sino en esclarecer si la exposición a bajos niveles de radiación durante largos periodos de tiempo puede o no provocar determinadas respuestas biológicas e influir sobre la salud de las personas.

A la exposición doméstica a campos electromagnéticos de baja intensidad, algunas personas le han atribuido un conjunto heterogéneo de síntomas como dolores de cabeza, ansiedad, depresión, náuseas, etc. En el sector industrial, han aparecido casos de irritación

ocular y cataratas en los trabajadores expuestos a altos niveles de radiación, de radiofrecuencia y microondas. Existen igualmente casos extremos de hipersensibilidad en los que pueden producirse migrañas, alteraciones del sueño, crisis epilépticas, etc.

Un tema muy polémico en los últimos años ha sido la existencia o no de efectos cancerígenos por exposición a esta radiación. Ciertos estudios epidemiológicos apuntan hacia un leve incremento del riesgo de leucemia infantil, asociado a la exposición a campos magnéticos de baja frecuencia en el hogar. En el año 2001 la Agencia Internacional de Investigación del Cáncer de la OMS (IARC), basándose en estudios epidemiológicos en niños, recogió sus conclusiones y clasificó los campos magnéticos de frecuencia extremadamente bajas (ELF) como posibles agentes cancerígenos, incluyéndose en el **Grupo 2B. Posiblemente cancerígeno para humanos.** En el año 2011 la IARC incluyó en ese mismo grupo los campos electromagnéticos de radiofrecuencia (RF), prestando una especial atención a la telefonía móvil e inalámbrica.

Las mejoras tecnológicas que introduce continuamente el mercado de las telecomunicaciones y los electrodomésticos, y los avances introducidos en la red eléctrica y en los aparatos que consumen esa electricidad, hace que sea cada vez menor la exposición de la población a las llamadas CEM.

Los campos de RF a la que puede exponerse una persona a la hora de hacer uso de su teléfono móvil, depende del tiempo de uso, del modelo, de lo cerca que se lo coloque de la cabeza, de la distancia a la antena más cercana (el aparato emplea más energía cuanto más lejos se encuentre la antena, para conseguir una señal adecuada), de la cantidad de tráfico de señales de telefonía que se genera habitualmente en el entorno…

Los intereses (a veces confrontados) de los diferentes agentes socioeconómicos implicados en el mundo de las telecomunicaciones, ha provocado que en los últimos años se hayan realizado bastantes estudios (experimentales, clínicos y epidemiológicos) para valorar los efectos sobre la salud de las radiofrecuencias emitidas por la telefonía móvil.

La disparidad de contenidos ha hecho que diversos organismos se hayan centrado en realizar revisiones sobre estos estudios, a objeto de valorar sus resultados, y las principales conclusiones que han sacado son:

- Los resultados clínicos y epidemiológicos detectados, no permiten establecer una clara relación causa-efecto entre las enfermedades estudiadas y la exposición a las radiofrecuencias de telefonía móvil.
- Tampoco los estudios realizados sobre personas que se declaran hipersensibles a los campos de radiofrecuencia que genera la telefonía móvil, han demostrado la existencia de una relación causa-efecto entre la sintomatología que presentan y su exposición a este tipo de ondas electromagnéticas.
- Se han detectado numerosas deficiencias en la calidad de las estimaciones de exposición a los CEM, como para realizar estudios fiables, consistentes y comparables.
- Aunque en algún estudio se ha detectado un leve incremento del riesgo de padecer tumores, entre los grupos de usuarios testeados con más horas de uso del teléfono móvil, las carencias y errores detectados en estos estudios impiden establecer relaciones causales. Interpretados en su conjunto, los resultados de los estudios epidemiológicos publicados hasta hoy sobre la aparición de tumores cerebrales ligados al uso de telefonía móvil, no demuestran ningún incremento del riesgo de padecer este tipo de enfermedades para un período de uso continuado de 10 años.
- Los cortos períodos de exposición a la telefonía móvil, con los que se cuenta actualmente, y los elevados períodos de latencia de los tumores cerebrales, aconsejan continuar con los estudios a largo plazo sobre sus posibles efectos.

REFERENCIAS

1. (2021). Retrieved 16 March 2021, from https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=es&gl=US
2. Bash. (2021). Retrieved 16 March 2021, from https://es.wikipedia.org/wiki/Bash
3. C++. (2021). Retrieved 16 March 2021, from https://es.wikipedia.org/wiki/C%2B%2B
4. Cómo configurar el puente de red en Ubuntu. (2021). Retrieved 16 March 2021, from https://es.linux-console.net/?p=1414
5. Cómo instalar. (2021). Retrieved 16 March 2021, from https://howtoinstall.co/es/net-tools
6. Cómo instalar. (2021). Retrieved 16 March 2021, from https://howtoinstall.co/es/bridge-utils
7. Debian -- Details of package bridge-utils in stretch. (2021). Retrieved 16 March 2021, from https://packages.debian.org/stretch/bridge-utils
8. Debian -- El sistema operativo universal. (2021). Retrieved 16 March 2021, from https://www.debian.org/index.es.html
9. Fernández, Y. (2021). Qué es Rufus y cómo utilizarlo para crear un USB de arranque. Retrieved 16 March 2021, from https://www.xataka.com/basics/que-rufus-como-utilizarlo-para-crear-usb-arranque
10. Index of /cdimage/unofficial/non-free/cd-including-firmware/current-live/amd64/iso-hybrid. (2021). Retrieved 16 March 2021, from https://cdimage.debian.org/cdimage/unofficial/non-free/cd-including-firmware/current-live/amd64/iso-hybrid/
11. Linux Networking Commands - javatpoint. (2021). Retrieved 16 March 2021, from https://www.javatpoint.com/linux-networking-commands
12. Net-tools. (2021). Retrieved 16 March 2021, from http://www.escomposlinux.org/lfs-es/lfs-es-5.0/appendixa/net-tools.html
13. Network Manager | Ubuntu. (2021). Retrieved 16 March 2021, from https://ubuntu.com/core/docs/networkmanager
14. SL, U. (2021). Rufus (Windows). Retrieved 16 March 2021, from https://rufus-usb.uptodown.com/windows

15. ⊳ Cómo instalar NetworkManager en Debian ▼. (2021). Retrieved 16 March 2021, from https://www.icomputo.com/2019/02/como-instalar-networkmanager-en-debian.html
16. 3. Puentes (bridge) - Redes locales y globales. (2021). Retrieved 16 March 2021, from https://sites.google.com/site/redeslocalesyglobales/2-aspectos-fisicos/5-dispositivos-de-interconexion-de-redes/3-puentes#:~:text=Un%20puente%20de%20red%20o,equipos%20sin%20necesidad%20de%20routers).
17. (2021). Retrieved 16 March 2021, from https://ubunlog.com/como-comprobar-la-intensidad-de-una-senal-wifi-desde-la-terminal/
18. (2021). Retrieved 16 March 2021, from https://nksistemas.com/medir-la-intensidad-de-la-senal-de-tu-wifi-en-linux/
19. (2021). Retrieved 16 March 2021, from https://developer.android.com/training/connect-devices-wirelessly/wifi-direct?hl=es-419
20. Aumentar la potencia en salida de nuestro dispositivo WiFi (Pagina 1) / Wireless y redes en linux. / Foro Wifi-libre.com. (2021). Retrieved 16 March 2021, from https://www.wifi-libre.com/topic-354-aumentar-la-potencia-en-salida-de-nuestro-dispositivo-wifi.html#p14584
21. card, H., Stoyanov, G., Stoyanov, G., & Prokopec, M. (2021). Hostapd on a Raspberry Pi 3 with external WiFi card. Retrieved 16 March 2021, from https://unix.stackexchange.com/questions/480431/hostapd-on-a-raspberry-pi-3-with-external-wifi-card
22. Cómo crear una red Ad-Hoc inalámbrica …. (2021). Retrieved 16 March 2021, from https://teratuxs.wordpress.com/2010/02/19/como-crear-una-red-ad-hoc-inalambrica/
23. Cómo hacer root fácilmente a cualquier smartphone Xiaomi. (2021). Retrieved 16 March 2021, from https://www.movilzona.es/2015/10/23/como-hacer-root-facilmente-a-cualquier-smartphone-xiaomi/
24. Contaminación radioeléctrica - Contaminación atmosférica. (2021). Retrieved 16 March 2021, from https://www.aulafacil.com/cursos/medio-ambiente/contaminacion-atmosferica/contaminacion-radioelectrica-l11451#:~:text=Es%20el%20tipo%20de%20contaminación,la%20velocidad%20de%20la%20luz.

25. Control de transferencias de paquetes con el comando snoop (Guía de administración del sistema: servicios IP). (2021). Retrieved 16 March 2021, from https://docs.oracle.com/cd/E19957-01/820-2981/gexkw/index.html
26. Crear un punto de acceso con Hostapd y Dnsmasq – TheHackingFactory. (2021). Retrieved 16 March 2021, from https://thehackingfactory.com/crear-un-punto-de-acceso-con-hostapd-y-dnsmasq
27. Developers, F., & channels, O. (2021). Hostapd error and clients unable to connect. Retrieved 16 March 2021, from https://forum.openwrt.org/t/hostapd-error-and-clients-unable-to-connect/16689
28. Medir la intensidad de nuestro WiFi desde la shell en linux. (2021). Retrieved 16 March 2021, from https://lamiradadelreplicante.com/2012/06/26/medir-la-intensidad-de-nuestro-wifi-desde-la-shell-en-linux/
29. Ramírez, I. (2021). Cómo rootear Android: cuatro métodos distintos para lograrlo. Retrieved 16 March 2021, from https://www.xatakandroid.com/programacion-android/como-rootear-android-cuatro-metodos-distintos-para-lograrlo
30. Usar un ordenador como repetidor wifi en modo puente con hostapd (Pagina 1) / Wireless y redes en linux. / Foro Wifi-libre.com. (2021). Retrieved 16 March 2021, from https://www.wifi-libre.com/topic-602-usar-un-ordenador-como-repetidor-wifi-en-modo-puente-con-hostapd.html