
Crear Wireless Access Point



By kneda

Aviso

En el directorio Wireless_Access_Point encontrareis el script wap.sh. Lo podéis guardar en la carpeta que creasteis "dhcp" en Lugares/Carpeta personal, y ejecutarlo desde ahí.

Antes de empezar a ejecutar el script, tendréis que concederle permisos de ejecución y revisar el código, ya que su funcionamiento está pensado para trabajar bajo mi equipo.

Ejecución manual de códigos sin utilización del script:

Terminal 1

```
:~# route -n
```

Muestra en una tabla las direcciones IP's de la subred, la puerta de enlace, y la máscara de red. Esto nos sirve para saber cómo debemos de configurar el documento dhcpd.conf.

```
:~# nano /root/dhcp/dhcpd.conf
```

Crea en la carpeta dhcp el archivo de configuración dhcpd.conf, que es el que almacena la información de red para los clientes, el cual se configura de la siguiente manera:

```
authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.2.0 netmask 255.255.255.0 {
option routers 192.168.2.1;
option subnet-mask 255.255.255.0;
option domain-name "network";
option domain-name-servers 8.8.8.8;
range 192.168.2.100 192.168.2.110;
}
```

Una vez escrito, presionar CTRL + X para salir, pedirá guardar los cambios, presionar S, y presionar Enter.

Activar modo monitor.

```
:~# ifconfig wlan1 down
```

Desconecta la interfaz

```
:~# iwconfig wlan1 mode monitor
```

La pone en modo monitor

```
:~# ifconfig wlan1 up
```

La vuelve a conectar

El nombre por defecto dado para el modo monitor es: wlan1

```
:~# airbase-ng -c 10 -e Wi-Fi_gratis wlan1
```

Crea un AP que va a transmitir por el canal 10 con el identificador

Wi-Fi_gratis en el adaptador de red que está puesto en modo monitor.

Crea una interfaz llamada at0.

Y establece la unidad de transmisión máxima en 1500 bytes.

Terminal 2

```
:~# ifconfig at0 192.168.2.1 netmask 255.255.255.0
    Establece una dirección IP y una máscara de red para at0 creada por
    airbase.
:~# ifconfig at0 mtu 1400          mtu = unidad de transmisión máxima
    Se cambia el parámetro original de 1500 bytes a la configuración
    predeterminada de 1400 bytes.
    1400 bytes es la configuración predeterminada para los clientes PPP, los
    clientes VPN, servidores PPP o los servidores VPN que ejecutan enrutamiento
    y acceso remoto.
:~# route add -net 192.168.2.0 netmask 255.255.255.0 gw 192.168.2.1
    Que modifique la tabla de enrutamiento añadiendo a la red una dirección IP
    establecida por nosotros, una dirección para la máscara de red, y una
    dirección para la puerta de enlace.
:~# echo 1 > /proc/sys/net/ipv4/ip_forward
    Activa ip_forward, ya que su valor por defecto es 0, haciendo que el equipo
    actúe como un router.
```

Configurar iptables

iptables permite definir reglas acerca de qué hacer con los paquetes de red.

```
:~# iptables -t nat -A PREROUTING -p udp -j DNAT --to 192.168.1.1
    -t          Tabla que se va a manipular, en este caso "nat"
    -A          Añade la regla iptables al final de la cadena
    PREROUTING  Establece las comunicaciones desde la red externa a la red
                interna
    -p          Protocolo a utilizar "udp"
    -j DNAT     Se utiliza para que desde el exterior se tenga acceso a un
                servidor que se encuentra en la red interna
    --to        Para la dirección IP
    Esto es básicamente que de algún sitio tiene que coger red para poder dar acceso.
:~# iptables -P FORWARD ACCEPT
    -P          Cambia la política en la cadena de destino ...
    FORWARD ACCEPT ... aceptando el reenvío de conexiones
:~# iptables -A FORWARD -i at0 -j ACCEPT
    -A          Añade la regla iptables al final de la cadena
    FORWARD    Reenvía los paquetes a una interfaz
    -i          Interfaz de entrada "at0"
    -j ACCEPT   Permite todo el tráfico
:~# iptables -t nat -A POSTROUTING -o wlan2 -j MASQUERADE
    -t          Tabla que se va a manipular, en este caso "nat"
    -A          Añade la regla iptables al final de la cadena
    POSTROUTING Establece las comunicaciones desde la red interna al exterior
    -o          Interfaz de salida "wlan2"
    -j MASQUERADE Hace enmascaramiento del tráfico (NAT) de forma que la red
                interna salga al exterior con la dirección externa del router

:~# dhcpd -cf /root/dhcp/dhcpd.conf -pf /var/run/dhcpd.pid at0
    dhcpd      Herramienta a utilizar
    -cf        Que coja los datos almacenados en el documento dhcpd.conf
    -pf        Crea en la ruta /var/run el documento dhcpd.pid el cual
                contiene el identificador del proceso para at0

:~# /etc/init.d/isc-dhcp-server start
    Que se inicie el servidor dhcp que se encuentra en la ruta /etc/init.d
```