

A thick dark blue vertical bar is on the left. A blue arrow points right from it, containing the date. Below the arrow, several thin, curved lines in dark blue and light grey sweep upwards from the bottom left.

18-11-2016

INSTALACIÓN Y CONFIGURACIÓN DE UN SERVIDOR VPN (openVPN) EN UNA RASPBERRY PI 3 (RASPBIAN)

José Manuel Ortega Falcón @jortfal
HACK&BEERS VALENCIA (VERSIÓN 1.0.0)

Contenido

0.- Introducción.	3
a) ¿Por qué queremos conectarnos a una red (WiFi) pública?	3
b) Riesgos de las redes públicas.	3
c) Conceptos previos.	3
¿Qué es una Red Privada Virtual (RPV) – en inglés, Virtual Private Network (VPN) –?.....	3
¿Qué es openVPN?	3
¿Qué es easy-rsa (/usr/share/easy-rsa)?.....	3
¿Qué es openSSL?.....	3
¿Qué es port forwarding?	4
¿Qué es NAT loopback (NAT Reflection, NAT Hairpinning o NAT-on-a-Stick)?.....	4
¿Qué es Diffie-Hellman?	4
d) Raspberry Pi: comparación y elección del modelo a utilizar.	5
e) ¿Qué se necesita?	6
f) Objetivos:.....	6
1.- Tipos de configuración (topología de la red).	7
2.- Configuraciones en la raspberryPi.	8
2.01.- Instalación del sistema operativo.	8
2.02.- Accediendo a la raspberryPi.	8
2.02.- Configuración del usuario o de los usuarios del sistema operativo.	9
2.03.- Actualización de los repositorios de los paquetes y del sistema operativo.	9
2.04.- Establecer una dirección IP estática (fija). --> imprescindible si no utilizamos un servidor DHCP! <--	9
2.05.- Habilitar que los paquetes IPv4 se redirijan (IP forwarding).	9
2.6.- Instalar openVPN (server).....	10
2.07.- Copiamos la utilidad "easy-rsa" a la carpeta de openVPN, y accedemos a ella.	10
2.08.- Editamos el fichero "vars".	10
2.09.- Crear una autoridad certificadora.	11
2.10.- Crear el certificado y la clave del servidor.	11
2.11.- Crear los certificados y las claves de los clientes.	11
2.12.- Generar los parámetros de Diffie Hellman.	11
2.13.- Fortificar la seguridad del servidor openVPN con TLS Auth.	11
2.14.- Configurar el servidor openVPN (server.conf - el fichero está en el repositorio de github).	11
2.15.- Configurar el cliente openVPN (client.conf - el fichero está en el repositorio de github).	11
2.16.- Configurar el firewall del sistema operativo para permitir las conexiones entrantes.	12
2.17.- Re-direccionamiento dinámico NO-IP (https://www.noip.com).	12
3.- Configuración del router.	13
3.01.- Asignar una dirección IP estática en el servidor DHCP a la raspberryPi.	13
3.02.- Publicar el servidor openVPN al exterior (internet) redireccionando los puertos mediante "virtual servers" (port forwarding).	14

0.- Introducción.

a) ¿Por qué queremos conectarnos a una red (WiFi) pública?

- IT IS FREE!!! (¡Es gratis!).
- Alto coste de las tarifas de datos.
- Tarifas asequibles con 2~5 GB de datos.
- Agotamiento de la tarifa de datos.
- Mayor velocidad en la conexión.
- ...

b) Riesgos de las redes públicas.

- Espionaje.
- Robo de datos personales, información sensible, credenciales, tarjetas de crédito...
- Malware.
- Phishing.
- ...

c) Conceptos previos.

¿Qué es una Red Privada Virtual (RPV) – en inglés, Virtual Private Network (VPN) –?

Una **Red Privada Virtual (VPN)** es una tecnología de red que permite crear una conexión segura a otra red a través de internet.

Cuando un cliente (ordenador, tablet, Smartphone, etc) se conecta al servidor VPN, a través de internet, adquiere una dirección ip privada de la red creada por el servidor. Esto se conoce como túnel.

Para que todo tenga sentido, el tráfico entre el cliente y el servidor se realiza de forma cifrada y con certificados digitales. De este modo, podemos navegar de forma segura (autenticidad, integridad y privacidad) y evitar, todos o la mayoría de los riesgos de las redes públicas.

¿Qué es openVPN?

openVPN permite crear túneles sobre cualquier subred IP o adaptador virtual de ethernet, a través de un solo puerto UDP o TCP.

¿Qué es easy-rsa (/usr/share/easy-rsa)?

easy-rsa es una utilidad, que viene incluida con openVPN, que facilita la creación de los certificados digitales y las claves tanto para el servidor como para los clientes. Está se puede utilizar de forma independiente a openVPN.

¿Qué es openssl?

openssl es una herramienta (librería) que ayuda a implementar **SSL (Secure Sockets Layer)**, así como otros protocolos relacionados con la seguridad de **TLS (Transport Layer Security)**. Además, también permite crear certificados digitales.

NOTA: hay que tener cuidado con la versión 1.0.1 y la versión 1.0.1f, pues presentan un agujero de seguridad conocido (CVE-2014-0160) como HeartBleed.

¿Qué es port forwarding?

port forwarding (virtual servers, port triggering, *DMZ*) es la acción de redirigir o reenviar un puerto, de un nodo o host, a otro puerto de otro nodo o host.

¿Qué es NAT loopback (NAT Reflection, NAT Hairpinning o NAT-on-a-Stick)?

NAT loopback es una extensión de NAT que permite acceder a la dirección pública de internet (WAN) desde la propia red de área local (LAN).

Esto es práctico cuando hay algún servidor dentro de la propia LAN, ya que permite acceder a este o estos servidores usando la dirección IP pública (y por lo tanto también un dominio asociado a dicha IP) desde dentro de la LAN.

¿Qué es Diffie-Hellman?

Es un protocolo criptográfico para el establecimiento de claves, utilizando un canal inseguro y de manera anónima, entre dos partes que no han tenido contacto previo. Su principal aplicación es acordar una clave simétrica con la que posteriormente cifrar las comunicaciones.

d) Raspberry Pi: comparación y elección del modelo a utilizar.

	NEW! Raspberry Pi 3 Model B	Raspberry Pi 2 Model B v1.2	Raspberry Pi Model B+
Processor Chipset	Broadcom BCM2837 64Bit Quad Core Processor powered Single Board Computer running at 1.2GHz	Broadcom BCM2837 64Bit Quad Core Processor powered Single Board Computer running at 900MHz	Broadcom BCM2835 32Bit SoC full HD multimedia applications processor
GPU	Videocore IV	Videocore IV	Videocore IV
Processor Speed	QUAD Core @1.2 GHz	QUAD Core @900 MHz	Single Core @700 MHz
RAM	1GB SDRAM @ 400 MHz	1GB SDRAM @ 400 MHz	512 MB SDRAM @ 400 MHz
Storage	MicroSD	MicroSD	MicroSD
USB 2.0	4x USB Ports	4x USB Ports	4x USB Ports
Max Power Draw/voltage	2.5A @ 5V	1.8A @ 5V	1.8A @ 5V
GPIO	40 pin	40 pin	40 pin
Ethernet Port	Yes	Yes	Yes
WiFi	Built in	No	No
Bluetooth LE	Built in	No	No

Figura 0.1.- Tabla comparativa de los modelos de la RaspberryPi.

e) ¿Qué se necesita?

- 1 conexión privada de internet :(
- 1 router con soporte para "port forwarding" y "NAT loopback" (opcional).
- 1 raspberryPI (recomendable raspberryPi 2 Model B v1.2 o superior).
- 1 microSD (mínimo 2GB, recomendable 4GB o más y preferiblemente de clase10).
- 1 servidor openVPN.
- 1 servicio de redireccionamiento dinámico NO-IP.
- 1 rato de tiempo libre ;)

f) Objetivos:

Utilizar las redes públicas de forma segura para:

- ahorrar datos y dinero,
- disponer de datos "infinitos" y
- fastidiar a los ISP ;)

1.- Tipos de configuración (topología de la red).

Lo primero que se debe hacer antes de comenzar a instalar y configurar el servidor de nuestra VPN es determinar la estructura de la red (Host to Host, Host to LAN o LAN to LAN). Dicha topología tiene consecuencias a la hora de realizar la configuración del servidor. A continuación, se muestra una breve explicación de cada estructura:

- Host to Host:** permite conectar dos dispositivos entre sí, por lo tanto, uno de ellos toma el rol de servidor y el otro de cliente (indistintamente).
- Host to LAN:** permite que múltiples dispositivos, de manera simultánea, se conecte a la red VPN. Estos dispositivos, dependiendo de la configuración del servidor VPN, pueden compartir recursos con la red anfitriona y entre los hosts de su misma red VPN (red huésped).
- LAN to LAN:** permite conectar distintas redes locales entre sí, ubicadas en diferentes localizaciones geográficas. De ese modo, se puede compartir información entre todos los clientes de todas las redes locales de forma fiable y segura. Esta configuración, principalmente, es utilizada en el ámbito empresarial.

En este proyecto la topología de la red es "Host to LAN", debido a que múltiples dispositivos son conectados a una red VPN.

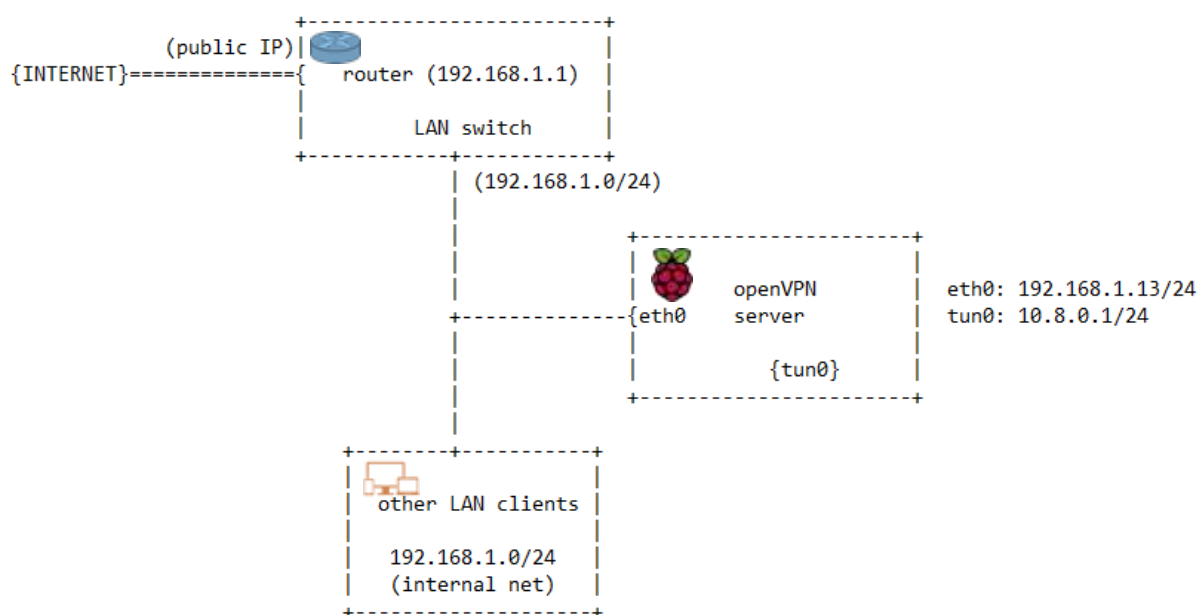


Figura 1.1.- Esquema de la topología de la red.

2.- Configuraciones en la raspberryPi.

2.01.- Instalación del sistema operativo.

Lo primero que se debe hacer es proporcionar de un sistema operativo a la raspberryPi. Por ello, se ha optado por utilizar "Raspbian Jessie Lite", se trata del sistema operativo Debian Jessie adaptado para este dispositivo, y sin interfaz gráfica (siendo así más ligero).

Una vez elegido el sistema operativo a utilizar, hay que instalarlo (quemar la imagen ".img") en la microSD que se introducirá en la RaspberryPi. Dependiendo del sistema operativo que se disponga se utiliza una herramienta u otra:

- a) En los sistemas operativos basados en Linux, se dispone de la herramienta "dd" la cual se utiliza a través del siguiente comando:

```
dd bs=4M if=2016-09-23-raspbian-jessie-lite.img of=/dev/sdb
```

Los principales parámetros son:

if=origen (lee desde el archivo indicado como origen. Por defecto lee de la entrada estándar).

of=destino (escribe al archivo indicado como destino. Por defecto escribe en la salida estándar).

ibs=N (lee N bytes del archivo origen).

obs=N (escribe N bytes en el archivo destino).

bs=N (lee y escribe N bytes. Alternativa a usar ibs y obs con un mismo valor).

- b) En los sistemas operativos Windows, se dispone de la herramienta "[Win32DiskImager](https://sourceforge.net/projects/win32diskimager/)" (<https://sourceforge.net/projects/win32diskimager/>).

Una vez finalizado el proceso de instalación se puede introducir la microSD en la RaspberryPi y arrancar está conectándola a la corriente.

2.02.- Accediendo a la raspberryPi.

Una vez instalado el sistema operativo que va a utilizar nuestro servidor vpn (raspberryPi) debemos acceder a ella para poder configurarlo, y para ello tenemos dos maneras:

- a) Conectar un teclado, un ratón y un monitor directamente a la raspberryPi,
- b) o simplemente conectar nuestra raspberryPi a nuestro punto de acceso (router o switch) por cable y acceder a ella a través de ssh (*password para el usuario pi: raspberry*)

```
ssh pi@<direccion_ip_raspberryPi>
```

Si nos conectamos por ssh, deberemos averiguar primero que dirección ip tiene asignada entrando a nuestro punto de acceso. Obtenida la dirección ip accedemos a ella desde otro ordenador con un terminal (si nuestro sistema operativo es Linux o Unix) o con un cliente ssh (putty, kitty, mobaXterm, etc).

NOTA: recomendable asignar una dirección ip privada fija a la raspberryPi - ver apartado 3a - (en el servidor DHCP), ya que si reiniciamos el punto de acceso o la raspberry esta puede cambiar.

2.02.- Configuración del usuario o de los usuarios del sistema operativo.

En este punto ya debemos de tener acceso al sistema operativo, ya sea directamente o a través de ssh. Lo primero que debemos hacer es gestionar el/los usuario/s, para ello se seguirán estos pasos:

- Cambiamos la contraseña del usuario root

```
sudo passwd root
```

- Nos logamos como usuario root

```
su
```

- Configuramos nano como editor por defecto de visudo

```
update-alternatives --config editor
```

- Creamos un usuario nuevo (vpn)

```
adduser vpn
```

- Apagar la máquina y conectarnos con el nuevo usuario

```
ssh vpn@<direccion_ip_raspberryPi>
```

- Añadimos el usuario que hemos creado a suoders (cambiar pi por vpn)

```
visudo
```

- Borramos el usuario que viene por defecto (pi)

```
sudo userdel -r pi
```

NOTA: una vez acabado de realizar toda la configuración asegurarse de desactivar el usuario root ejecutando "**sudo passwd -l root**".

2.03.- Actualización de los repositorios de los paquetes y del sistema operativo.

```
sudo apt-get update
```

```
sudo apt-get upgrade
```

2.04.- Establecer una dirección IP estática (fija). --> ¡imprescindible si no utilizamos un servidor DHCP! <--

(ver apartado 3.02)

2.05.- Habilitar que los paquetes IPv4 se redirijan (IP forwarding).

```
vi /etc/sysctl.conf
```

des-comentamos la siguiente línea: "#net.ipv4.ip_forward=1"

2.6.- Instalar openVPN (server).

```
sudo apt-get install openvpn
```

2.07.- Copiamos la utilidad "easy-rsa" a la carpeta de openVPN, y accedemos a ella.

```
cp -r /usr/share/easy-rsa /etc/openvpn/
```

```
cd /etc/openvpn/easy-rsa
```

2.08.- Editamos el fichero "vars".

Este fichero contiene los valores (por defecto) de los parámetros que requiere cualquier certificado que creamos con "easy-rsa". Además del tamaño de las claves rsa y otros campos, y por ello vamos a introducir los que deseemos.

- Abrimos el fichero "vars" con el un editor de text:

```
vi vars
```

- Datos de la entidad emisora de los certificados:

Localizar las siguientes líneas y cambiar por los valores deseados:

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL=mail(arroba)host.domain
export KEY_CN= Changeme
export KEY_OU= Changeme
```

En este proyecto se han utilizado los siguientes valores:

```
export KEY_COUNTRY="ES"
export KEY_PROVINCE="VLC"
export KEY_CITY="Valencia"
export KEY_ORG="security"
export KEY_EMAIL=mail@mail.com
export KEY_CN= Changeme
export KEY_OU= Changeme
```

- Tamaño de las claves:

Localizar la línea

```
export KEY_SIZE=1024
```

y sustituir por

```
export KEY_SIZE=2048
```

También podemos configurar el tiempo de validez que tendrá nuestra entidad certificadora y el tiempo de validez que tendrán los certificados y claves que crearemos. El valor estándar de validez son 3650 días.

- Aplicamos los cambios realizados:

```
source ./vars
```

- Borramos las claves que puedan existir:

```
./clean-all
```

2.09.- Crear una autoridad certificadora.

Necesitamos crear nuestra propia autoridad certificadora, lo que implica crear el certificado raíz (ca.ctr) y la clave de la entidad certificadora (ca.key) para así poder firmar o revocar los certificados de los usuarios (servidor openVPN y clientes openVPN).

```
./build-ca
```

2.10.- Crear el certificado y la clave del servidor.

```
./build-key-server raspberryPiVPN
```

Este comando crea el certificado y la clave privada para el servidor openVPN. Cuando lo ejecutamos nos pide unos parámetros, si hemos configurado correctamente el archivo "vars" solo tendremos que aceptar los parámetros por defecto (que son los que hemos establecido en el apartado 02.08).

2.11.- Crear los certificados y las claves de los clientes.

```
./build-key <user_name>
```

Este comando crea el certificado y la clave privada para el cliente (usuarios). Cuando lo ejecutamos nos pide unos parámetros, si hemos configurado correctamente el archivo "vars" solo tendremos que aceptar los parámetros por defecto (que son los que hemos establecido en el apartado 02.08).

NOTA: este paso se realizará tantas veces como usuarios necesitemos.

2.12.- Generar los parámetros de Diffie Hellman.

```
./build-dh
```

2.13.- Fortificar la seguridad del servidor openVPN con TLS Auth.

```
cd /etc/openvpn/easy-rsa/keys
```

```
openvpn --genkey --secret ta.key
```

2.14.- Configurar el servidor openVPN (server.conf - el fichero está en el repositorio de github).

```
vi /etc/openvpn/server.conf
```

2.15.- Configurar el cliente openVPN (client.conf - el fichero está en el repositorio de github).

```
vi /etc/openvpn/client.conf
```

2.16.- Configurar el firewall del sistema operativo para permitir las conexiones entrantes.

Añadir en el fichero "/etc/network/interfaces" dentro del correspondiente adaptador (por defecto eth0) la siguiente línea: `pre-up /etc/firewall_rules.sh` (el fichero está en el repositorio de github).

Es cargara las reglas del firewall antes de que se levante la interfaz de red durante la carga del sistema operativo.

2.17.- Re-direccionamiento dinámico NO-IP (<https://www.noip.com>).

Cuando contratamos un servicio de internet para el hogar, el ISP (Proveedor de Servicios de Internet) nos proporciona una dirección IP publica para poder conectarnos con el mundo exterior. Pero resulta que esta dirección IP es dinámica y con el tiempo puedo cambiar. Al igual que si reiniciamos o apagamos y encendemos el router.

Para poder llegar a los hosts (servidores) que se encuentran en la red privada (192.168.1.0) necesitamos acceder a través de nuestra dirección IP pública y hacer una redirección de puertos (port forwarding) hacia el correspondiente host (servidor). Aquí es donde viene el problema, ya que si la dirección IP pública cambia necesitamos acceder al router (hay otras maneras) para poder averiguar cuál es en ese momento. La solución a este problema pasa por utilizar un servicio de direccionamiento DNS dinámico, como el que ofrece www.noip.com.

El direccionamiento DNS dinámico consiste en asociar un nombre de dominio a nuestra dirección IP pública. A partir de ese momento podemos acceder a nuestros hosts a través de ese dominio. Solo falta decirle al router (o instalar un agente en alguna máquina) que comunique la dirección IP pública que va teniendo en cada momento al servicio DNS dinámico para que este asocie nuestra dirección IP al dominio.

A continuación, se detalla el procedimiento para instalar un agente, en el servidor openVPN, que vaya comunicando dicha dirección IP al servicio de DNS dinámico:

- Lo primero que tenemos que hacer es darnos de alta al servicio de direccionamiento DNS dinámico y crearnos un subdominio.

- Instalar el agente que comunique nuestra IP (dnsmasq)

```
sudo apt-get install dnsmasq
```

- Configuramos nano como editor por defecto de visudo

```
update-alternatives --config editor
```

- Creamos un usuario nuevo (vpn)

```
adduser vpn
```

- Apagar la máquina y conectarnos con el nuevo usuario

```
ssh vpn@<direccion_ip_raspberryPi>
```

- Añadimos el usuario que hemos creado a suoders (cambiar pi por vpn)

```
visudo
```

- Borramos el usuario que viene por defecto (pi)

```
sudo userdel -r pi
```

3.- Configuración del router.

3.01.- Asignar una dirección IP estática en el servidor DHCP a la raspberryPi.

Es necesario asignar una dirección IP estática al dispositivo (raspberryPi) que va a alojar el servidor VPN. Esto es debido a que el router tiene que redireccionar las peticiones de los clientes de la red VPN, que recibe por la interfaz WAN (internet), hacia la red de área local anfitriona (en este caso 192.168.1.0).

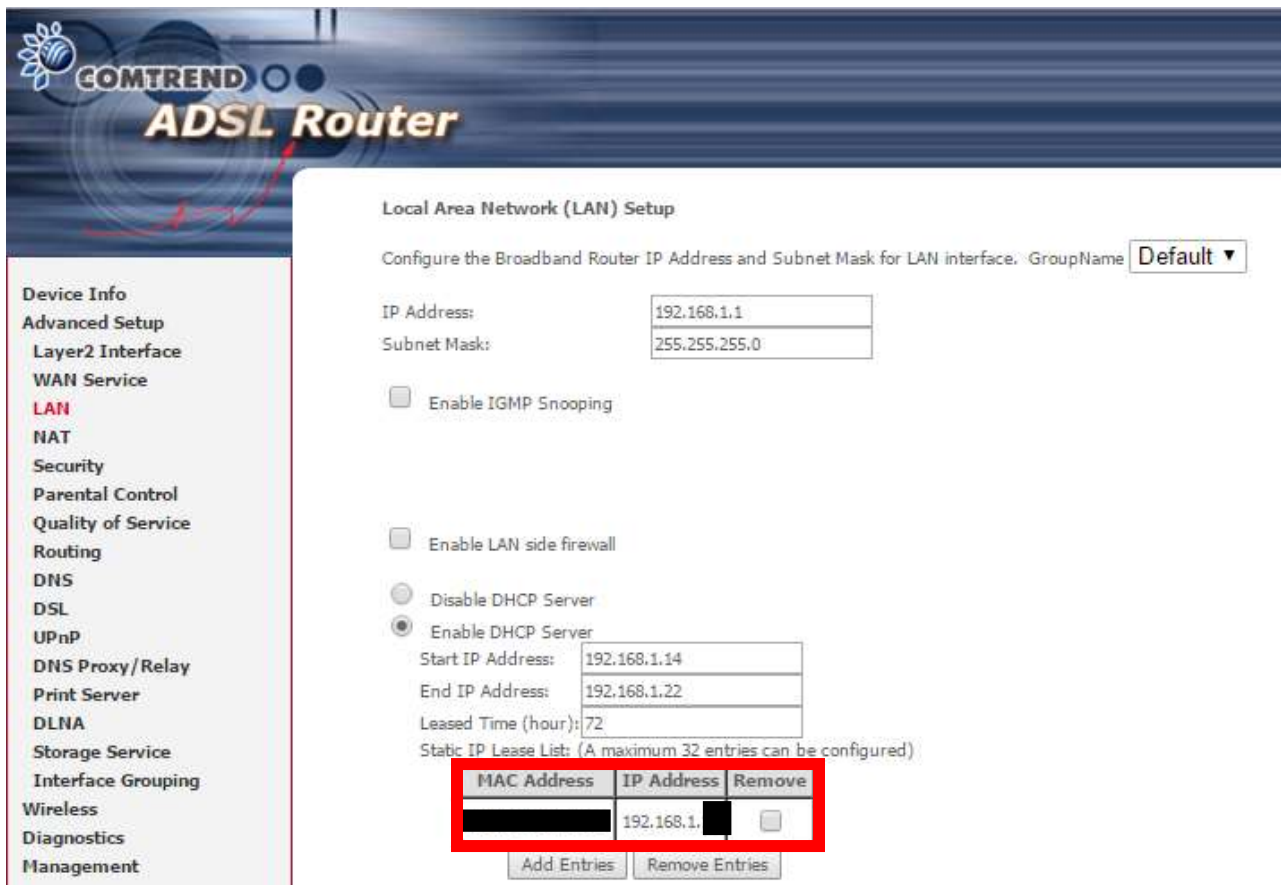


Figura 3.1.- Asignación de una dirección IP estática en el servidor DHCP.

Por defecto el sistema operativo, raspbian, está configurado para obtener una dirección ip del servidor DHCP (que se encuentra en el punto de acceso). Pero si por cualquier motivo, el servidor DHCP no está disponible o fallará, el sistema operativo comprobará si tiene configurado unos parámetros de red, y si es así, los utilizará. Estos parámetros se encuentran en el fichero "interfaces", que se encuentra en la siguiente ruta "/etc/network/".

Para establecer los parámetros correspondientes se puede seguir estos pasos:

- 1.- Para evitar todo tipo de riesgo se realiza una copia de seguridad del fichero "interfaces":

```
cp /etc/network/interfaces /etc/network/interfaces.bak
```

- 2.- Abrimos el fichero con un editor de texto (vi, vim, nano, Etc.):

```
sudo vi /etc/network/interfaces
```

3.- Añadimos/modificamos los siguientes parámetros:

Una vez ejecutado el anterior comando, en la terminal, se abrirá el editor de textos. Una vez abierto, hay que reemplazar el contenido del adaptador "eth0" por el que se muestra en la siguiente captura de pantalla:

```
GNU nano 2.2.6      Fichero: /etc/network/interfaces      Modificado
# Montaje de interfaz localhost
auto lo
iface lo inet loopback

# Montaje de la interfaz eth0
auto eth0
iface eth0 inet static
    address 192.168.1.188
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255
    gateway 192.168.1.1
    dns-nameservers 192.168.1.1
-
```

auto lo
iface lo inet loopback

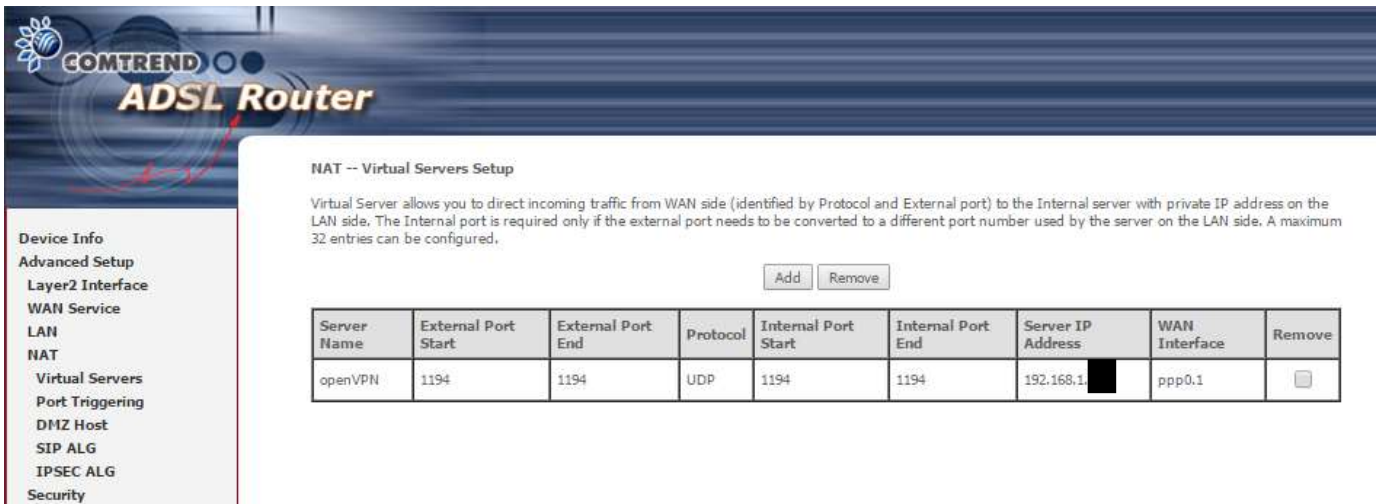
auto eth0
iface eth0 inet static
address 192.168.1.x
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
Gateway 192.168.1.1

Figura 3.2.- Contenido del archivo interfaces.

4.- Aplicamos los cambios:

Sudo systemctl restart networking

3.02.- Publicar el servidor openVPN al exterior (internet) redireccionando los puertos mediante "virtual servers" (port forwarding).



COMTREND ADSL Router

NAT -- Virtual Servers Setup

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

Add Remove

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	WAN Interface	Remove
openVPN	1194	1194	UDP	1194	1194	192.168.1.1	ppp0.1	<input type="checkbox"/>