

TALLER SR – PRÁCTICA 66 – ROUTER WiFi 4G LTE

VPN + Dynamic DNS + Comprobación CGNAT

NÚMERO DE GRUPO	FUNCIÓN	Apellidos, Nome
<div></div>	Coordinador/a:	
	Responsable Limpeza:	
	Responsable Documentación:	

ESCENARIO: Router WiFi 4G LTE - VPN + Dynamic DNS

Router WiFi 4G LTE

Configuración VPN

Prerrequisitos:

1. Hora sincronizada con Internet (NTP)
2. IP fixa na WAN do Router (Contratada ou Dynamic DNS)

Portátil:

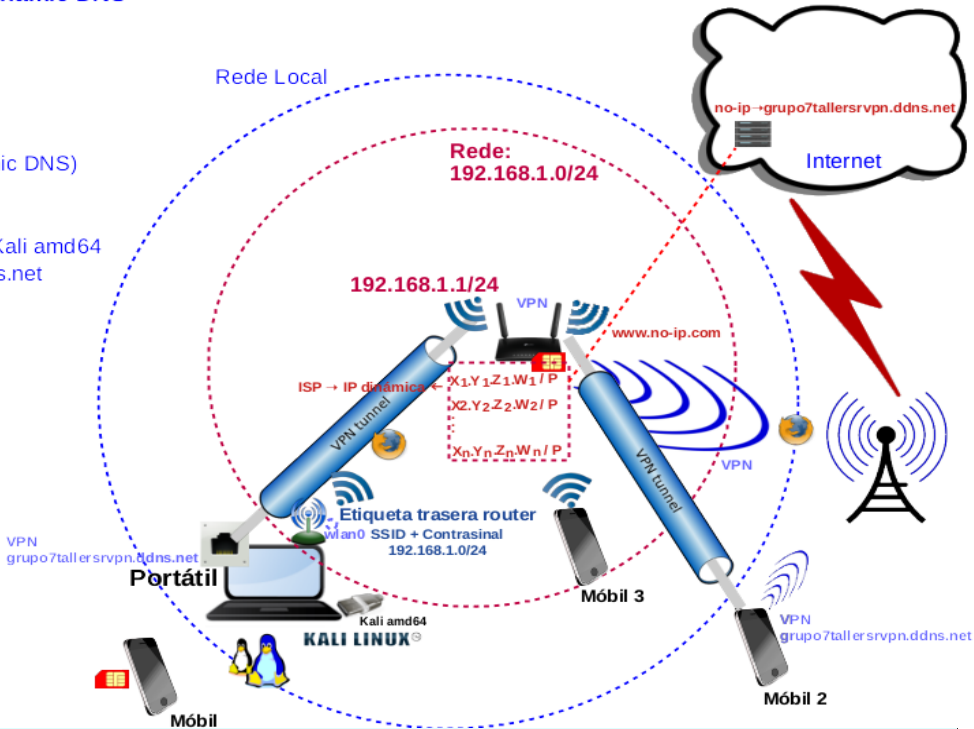
SSID + Contraseña (etiqueta trasera router) Live Kali amd64  
Ethernet Rede Aula → VPN → grupo7tallersvpn.ddns.net

SIM Móbil

Conectar ao router

www.no-ip.com (ou IP estática WAN Router)

Dynamic dns → grupo7tallersvpn.ddns.net



**LIMITACIÓN DE RESPONSABILIDADE** O autor do presente documento declina calquera responsabilidade asociada ao uso incorrecto e/ou malicioso que puidese realizarse coa información exposta no mesmo. Por tanto, non se fai responsable en ningún caso, nin pode ser considerado legalmente responsable en ningún caso, das consecuencias que poidan derivarse da información contida nel ou que esté enlazada dende ou hacia el, incluíndo os posibles erros e información incorrecta existentes, información difamatoria, así como das consecuencias que se poidan derivar sobre a súa aplicación en sistemas de información reais e/ou virtuais. Este documento foi xerado para uso didáctico e debe ser empregado en contornas privadas e virtuais controladas co permiso correspondente do administrador desas contornas.

Material necesario	Práctica: ROUTER WiFi 4G LTE VPN + Dynamic DNS + Comprobación CGNAT
<div>■ Portátil</div> <div>■ Regleta</div> <div>■ [1] <a href="#">Práctica 63</a></div> <div>■ USB Live amd64 Kali</div> <div>■ Móviles alumnado</div> <div>■ [2] <a href="#">tp-link 4G LTE Router TR-ML6400</a></div> <div>■ [3] <a href="#">Cómo encontrar la versión de hardware en un dispositivo de TP-Link</a></div> <div>■ [4] <a href="#">TR-MR6400 Soporte</a></div> <div>■ [5] <a href="#">TL-MR6400(EU)_V5.3_Quick Installation Guide</a></div> <div>■ [6] tp-link: <a href="#">Vídeo de configuración</a></div> <div>■ [7] <a href="#">Vídeo techdroy - Análisis TP-Link TL-MR6400   TODO lo que DEBES saber de este ROUTER 4G LTE</a></div> <div>■ [8] <a href="#">www.no-ip.com</a> (Dynamic DNS)</div>	<div>(1) Prerrequisito: Realizar a <a href="#">Práctica 63</a> [1]</div> <div>(2) Entrega/Revisión material necesario para a práctica: Figuras 1,2,3,4,5 e 6</div> <div>(3) NON conectar o portátil á roseta da aula.</div> <div>(4) Portátil:<div>a) Arrancar co USB Live amd64 Kali</div><div>b) Configurar a rede WiFi según escenario (router).</div><div>c) Configurar VPN (OpenVPN) no Router WiFi 4G LTE</div><div>d) Comprobar CGNAT</div></div> <div>(5) Comprobar conexión clientes VPN:<div>a) Portátil : deshabilitar WiFi e conectar á roseta da aula.</div><div>b) Móviles alumnado.</div></div>



- Procedemento:**
1. Prerrequisito: Realizar esta práctica unha vez rematada e validada a [Práctica 63](#) [1]
  2. Entrega/Revisión material necesario para a práctica:



Figura 1:  
Lateral  
esquerda



Figura 3: Frontal



Figura 2:  
Lateral  
dereita

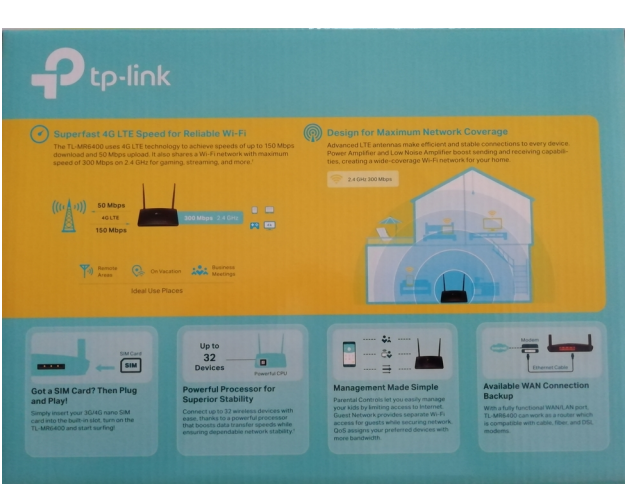


Figura 4: Trasera



Figura 5: Unboxing 1

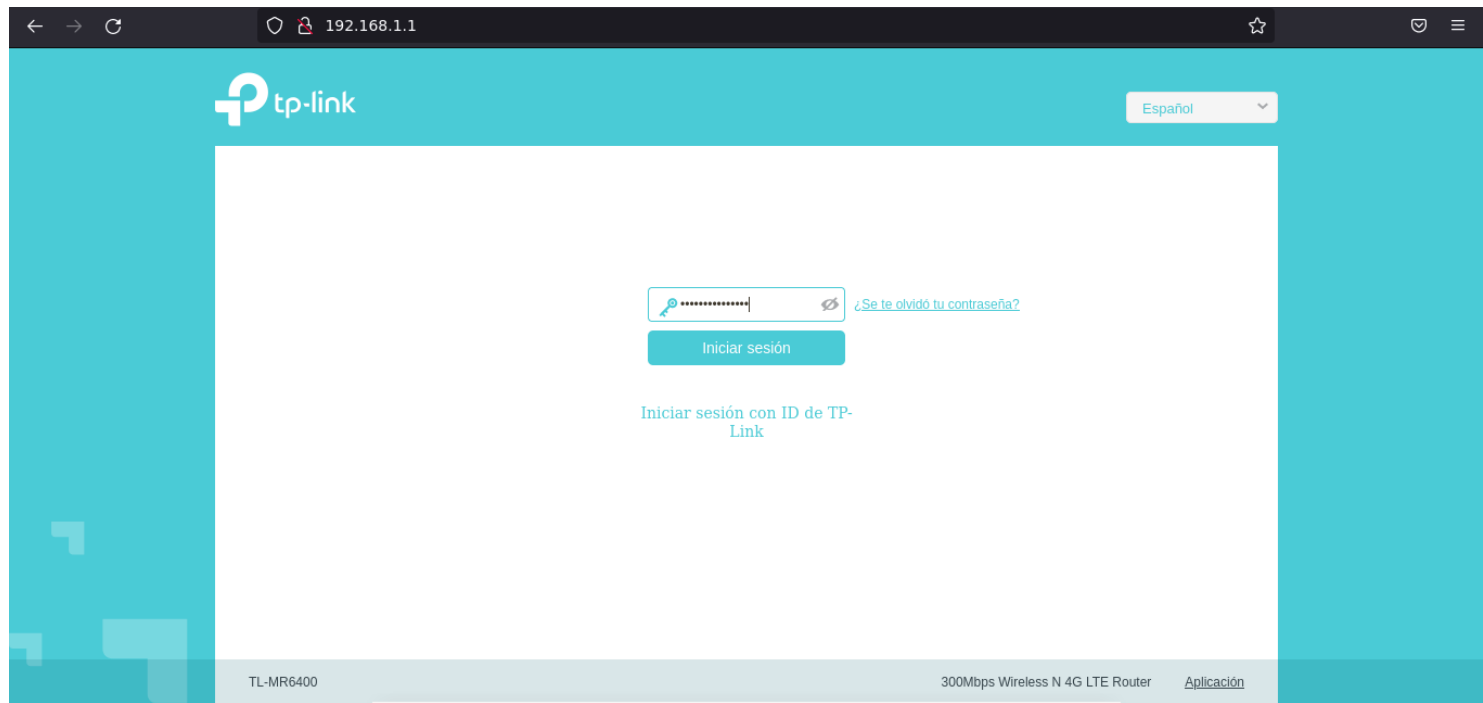


Figura 6: Unboxing 2

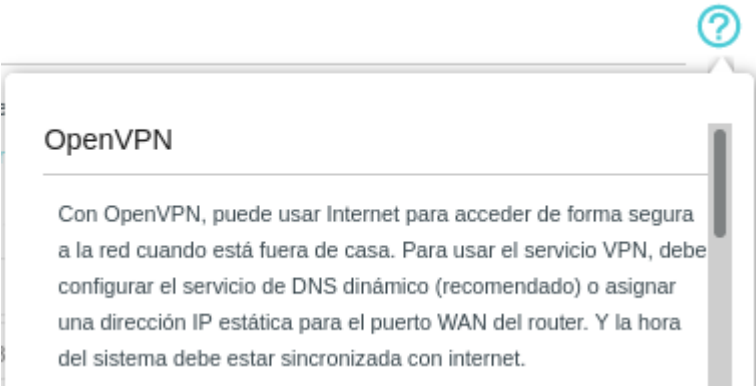
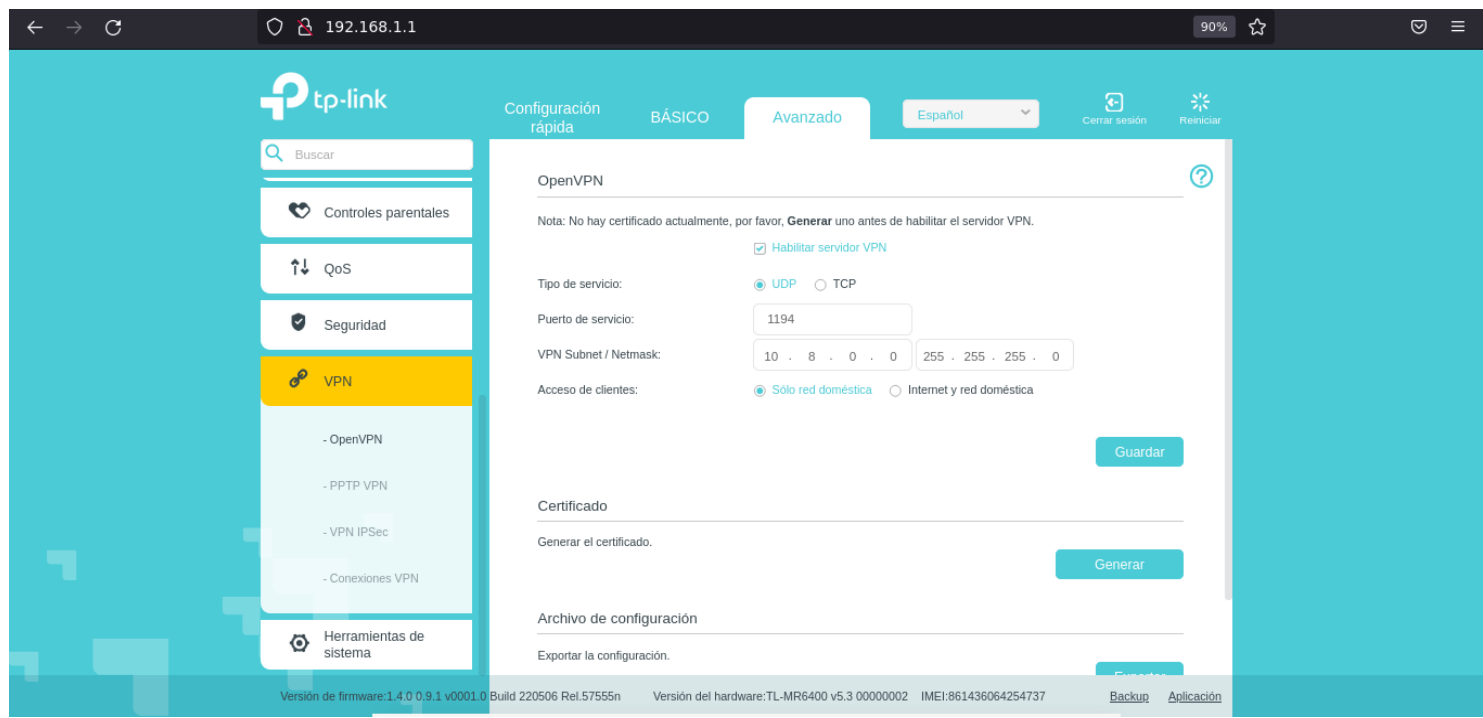
- a) Avisar ao docente para a revisión. ☐ 1
3. Conectar os dispositivos móbiles do alumnado ao router e cubrir a Táboa1. Móviles alumnado

4. Portátil:

a) Acceder mediante o navegador firefox á URL <http://192.168.1.1> e *Iniciar sesión*:



b) Dirixirse a *Avanzado* → *VPN* → *OpenVPN*



c) Este router mediante la configuración de OpenVPN permite 2 tipos de conexiones VPN a los clientes:  
*Sólo red doméstica e Internet y red doméstica*

Acceso de clientes

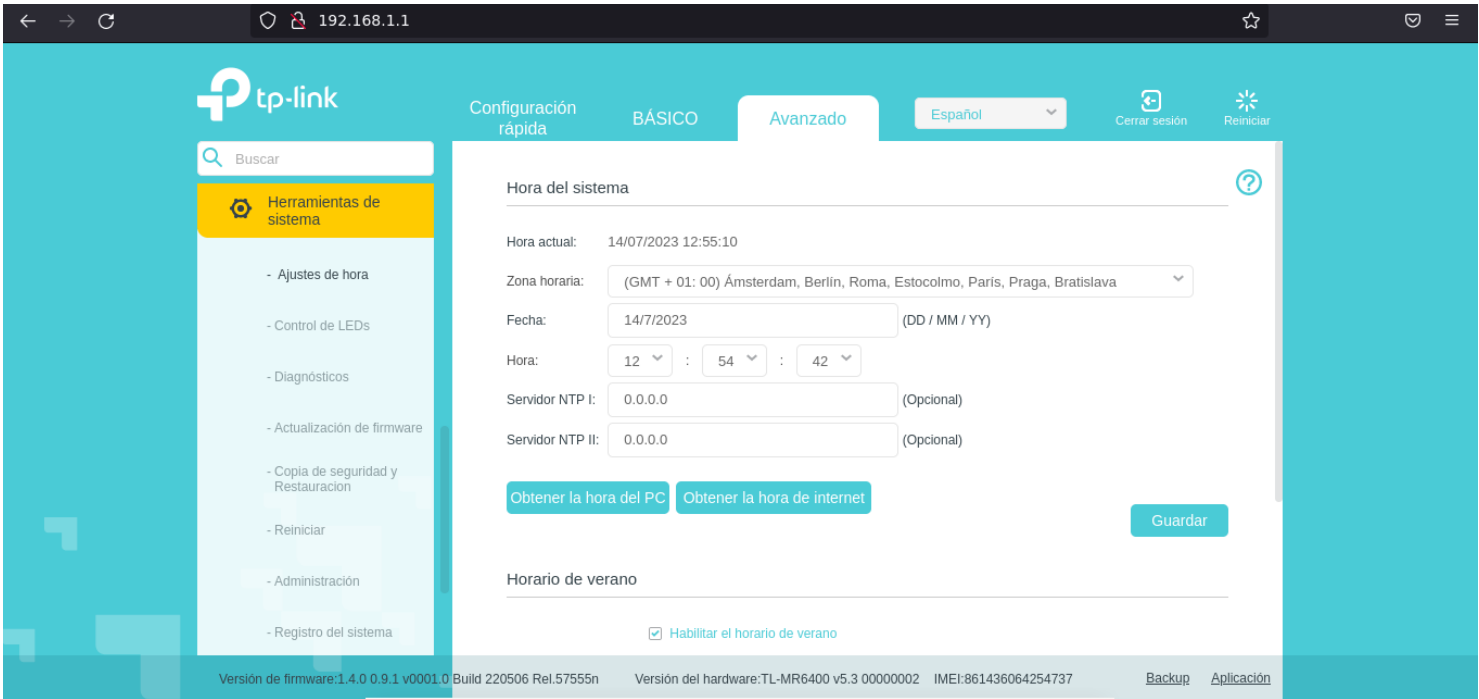
Seleccione el tipo de acceso para el cliente OpenVPN.

**Sólo red doméstica** - El cliente solo puede acceder a la red doméstica. La ruta por defecto del cliente no se cambiará.

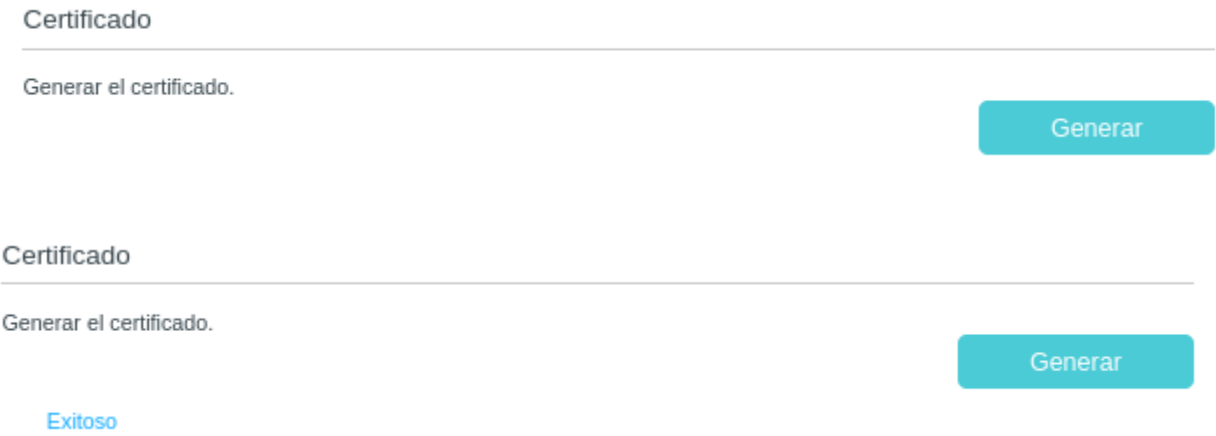
**Internet y red doméstica** - El cliente puede acceder a la red doméstica y a los sitios o servicios de Internet con una limitación geográfica cuando se encuentre fuera del país. La ruta por defecto del cliente será alterada.

d) Pero antes de *Habilitar servidor VPN* debemos:

(1) Comprobar que a configuración da data é hora do router son as que corresponden á nosa zona horaria(+1):  
*Avanzado → Herramientas de sistema → Ajustes de hora*



(2) Xerar un certificado: *Certificado → Generar el certificado → Generar*

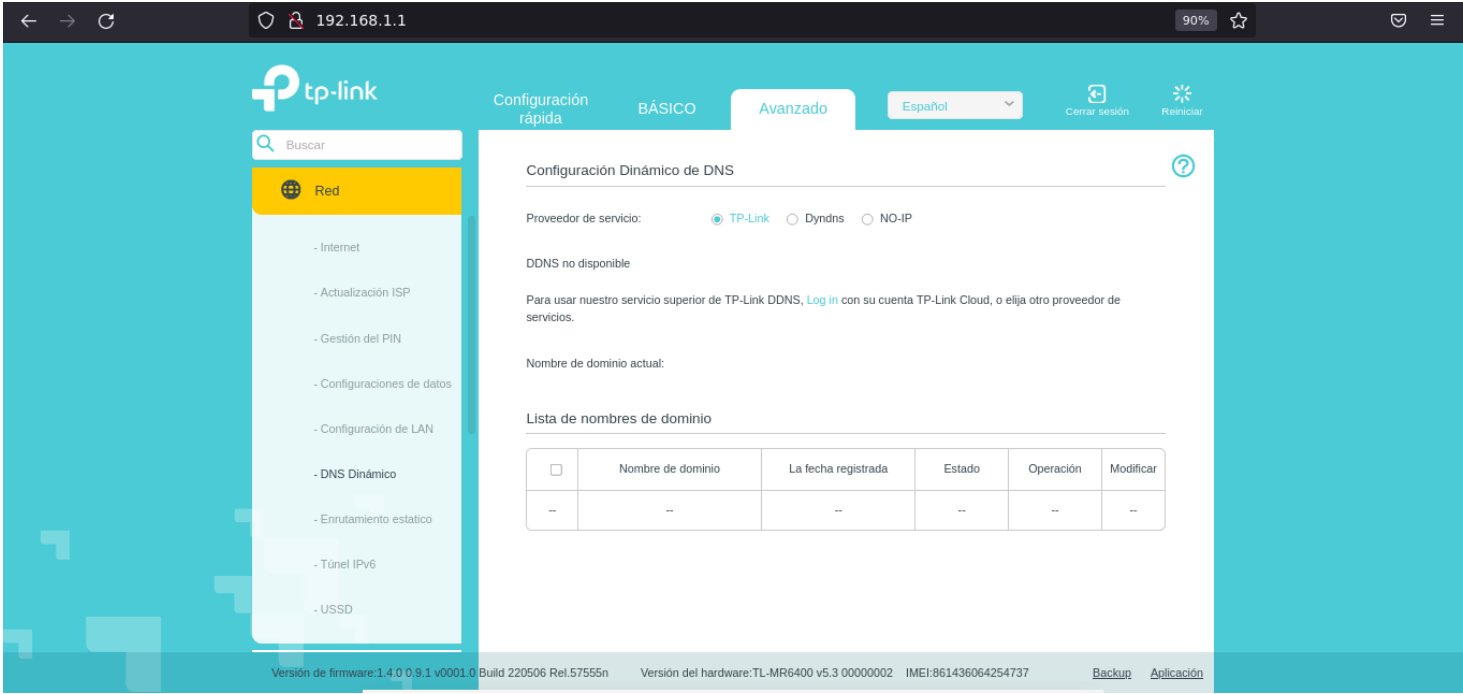


**NOTA<sub>1</sub>:** Este certificado será preciso exportarlo para que o poidan empregar os clientes no acceso VPN

(3) De non dispoñer de IP estática en Internet, é dicir, se non temos contratada co ISP unha IP estática de saída a Internet, debemos xerar/configurar unha conta DDNS (DNS Dinámico). Así, imos configurar no router unha conta DNS Dinámico para que aínda que a IP que empreguemos para saír a Internet non sexa sempre a



mesma poidamos acceder á noso router sempre co mesmo nome DNS. Se non fose así, de cada vez que un cliente se quixera conectar por VPN ao noso router debería saber a IP que o router ten concedido nese momento polo ISP.



Como podemos observar podemos configurar **DNS Dinámico** con: TP-Link, Dyndns e NO-IP. Imos xerar unha conta en NO-IP:

(a) Seguimos os pasos indicados na axuda:

Configuración Dinámica de DNS

Proveedor de servicio:

☐ TP-Link

☐ Dyndns

☒ NO-IP

[Ir al registro ...](#)

Nombre de usuario:

Código secreto:

Iniciar sesión

Cerrar sesión

Desconectado

Guardar

Configuración Dinámica de DNS

DDNS (Sistema de nombres de dominio dinámico) le permite asignar un nombre de dominio y host fijo a una dirección IP de Internet Dinámico. Es útil cuando está alojando su propio sitio web, servidor FTP u otro servidor detrás del router. Para empezar, debe registrarse con un proveedor de servicios de DNS dinámico como [www.dyndns.com](#).

Para configurar un DNS dinámico

1. Seleccione el proveedor de servicios de DNS dinámico.
2. Introduzca el nombre de usuario y la contraseña de la cuenta de DNS dinámico.
3. Introduzca el nombre de dominio que recibió del proveedor de servicios de DNS dinámico.
4. Haga clic en Iniciar sesión y haga clic en Guardar.

Nota:

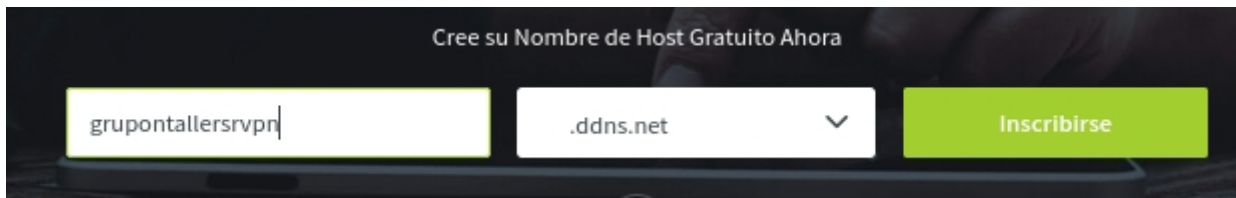
Si desea usar una nueva cuenta DDNS, primero cierre la sesión y luego inicie sesión con la nueva cuenta.



## (b) Configuración Dinámico de DNS

DDNS (Sistema de nombres de dominio dinámico) le permite asignar un nombre de dominio y host fijo a una dirección IP de Internet Dinámico. Es útil cuando está alojando su propio sitio web, servidor FTP u otro servidor detrás del router. Para empezar, debe registrarse con un proveedor de servicios de DNS dinámico como [www.dyndns.com](http://www.dyndns.com).

I. Acceder a [www.no-ip.com](http://www.no-ip.com) e xerar o dominio `grupontallersrvpn.ddns.net`, onde o primeiro *n* toma o valor do número do grupo de prácticas.

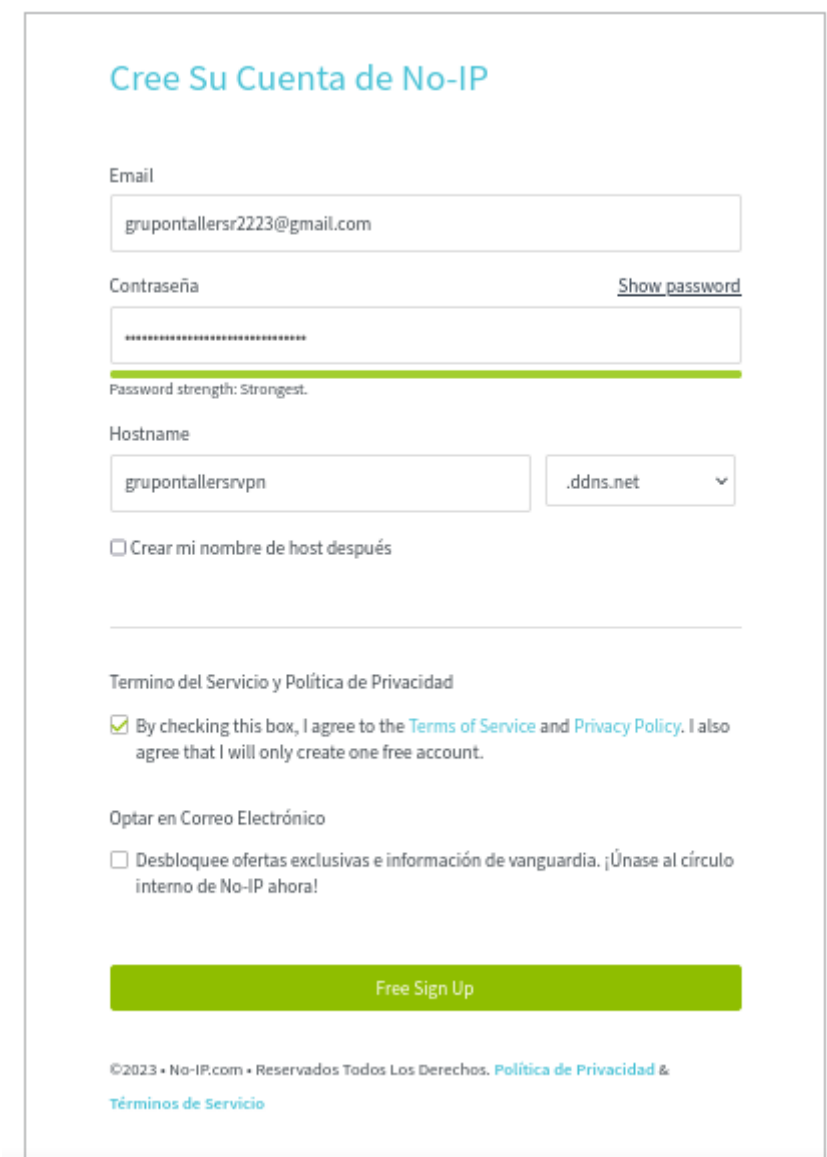


Cree su Nombre de Host Gratuito Ahora

grupontallersrvpn .ddns.net Inscribirse

II. Clic en *Inscribirse* e cubrir os campos do formulario solicitado. Modificar no correo electrónico o carácter *n* polo número do grupo que corresponda e os números *2223* polos correspondentes ao curso académico actual.

**NOTA<sub>2</sub>:** No caso que non teñades xerado o correo electrónico de gmail debes crearlo.



Cree Su Cuenta de No-IP

Email  
grupontallersr2223@gmail.com

Contraseña [Show password](#)  
\*\*\*\*\*

Password strength: Strongest.

Hostname  
grupontallersrvpn .ddns.net

☐ Crear mi nombre de host después

Termino del Servicio y Política de Privacidad  
☒ By checking this box, I agree to the [Terms of Service](#) and [Privacy Policy](#). I also agree that I will only create one free account.

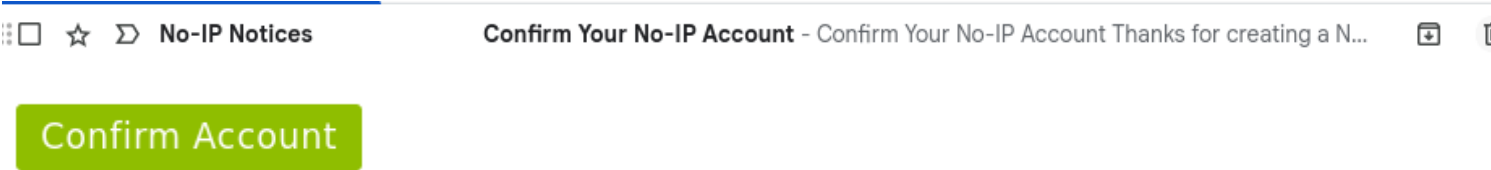
Optar en Correo Electrónico  
☐ Desbloquee ofertas exclusivas e información de vanguardia. ¡Únase al círculo interno de No-IP ahora!

Free Sign Up

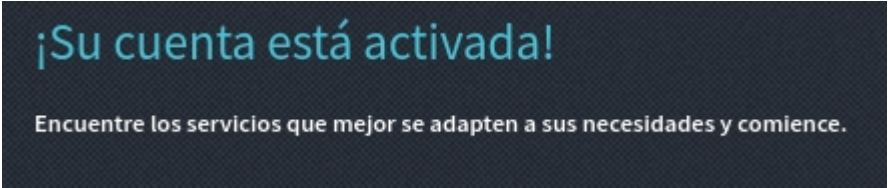
©2023 • No-IP.com • Reservados Todos Los Derechos. [Política de Privacidad](#) & [Términos de Servicio](#)

III. Clic en *Free Sign Up*

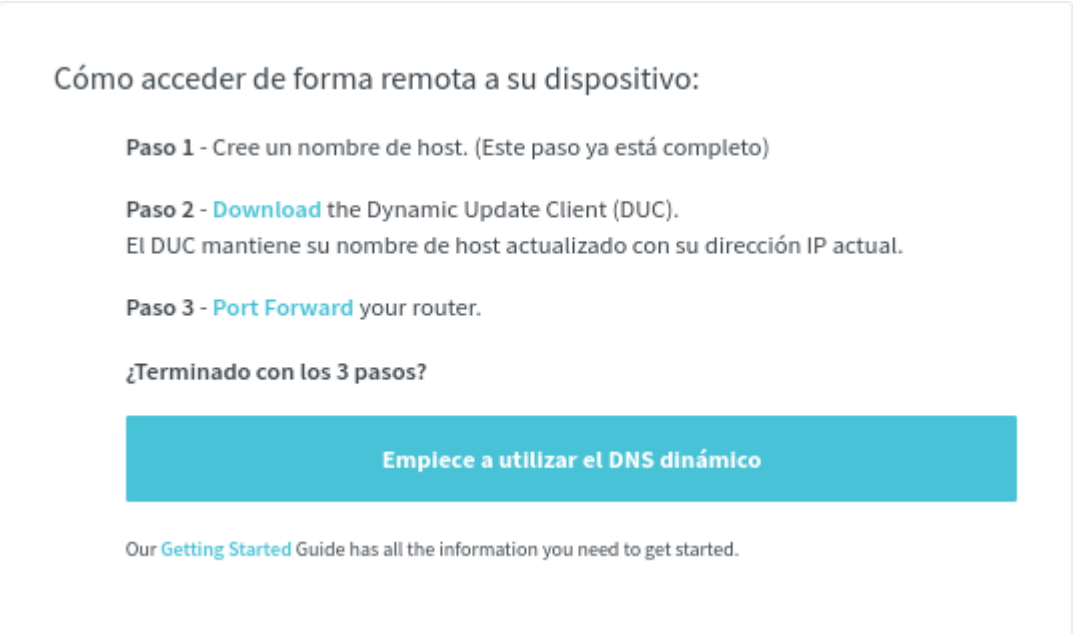
IV. Automaticamente accederemos á conta recién xerada na interface de *no-ip* indicándonos que temos que acceder ao correo electrónico que configuramos no formulario e activar a conta *no-ip*. Polo tanto accedemos á conta do correo electrónico e activamos a conta *no-ip* abrindo o correo recibido e facendo clic en *Confirm Account* :



V. Conta activada:



VI. Deberíamos seguir cos pasos indicados:



Así, Paso 2 → <https://www.noip.com/es-MX/download>

Pero non é necesario, xa que o Paso 2 e o Paso 3 conseguímolos configurando a conta de *no-ip* no router. Así, tiñamos a seguinte información na axuda:

### Para configurar un DNS dinámico

1. Seleccione el proveedor de servicios de DNS dinámico.
2. Introduzca el nombre de usuario y la contraseña de la cuenta de DNS dinámico.
3. Introduzca el nombre de dominio que recibió del proveedor de servicios de DNS dinámico.
4. Haga clic en Iniciar sesión y haga clic en Guardar.

### Nota:

Si desea usar una nueva cuenta DDNS, primero cierre la sesión y luego inicie sesión con la nueva cuenta.



Polo cal, agora introducimos usuario e contrasinal de *no-ip* na configuración *Dynamic DNS*. Pero primeiro debemos xerar un Nombre de usuario na nosa conta *no-ip*, co cal dirixirse a URL <https://my.noip.com/account> e configuralo:

Información básica

Correo electrónico

grupo7tallersr@gmail.com

Cambiar correo electrónico

Contraseña

.....

Cambiar contraseña

Nombre de usuario

Agregar nombre de usuario

Facer clic en *Agregar nombre de usuario* e insertar o voso nome de usuario:

Actualizar nombre de usuario

Nota : Actualizar su contraseña puede afectar a todos los clientes de actualización dinámica (DUC de No-IP o dispositivos integrados), excepto Windows DUC v3.0 y versiones posteriores. Para crear contraseñas de cuentas y credenciales DDNS individuales, [cree un grupo](#).

Nuevo nombre de usuario

gruPontallersr2223

Cancelar

Guardar

Facer clic en *Guardar*

Tamén é necesario actualizar o *Huso Horario* na configuración da conta *no-ip* (+1):

Información de hora e idioma

Idioma

Espanol

Huso horario

GMT+01:00 - Brussels, Copenhagen, Madrid, Paris

Guardar

Agora si cubrir no router os campos do formulario *Dynamic DNS* → *Iniciar sesión* → *Guardar*

Configuración Dinámico de DNS

Proveedor de servicio:

☐ TP-Link

☐ Dyndns

☒ NO-IP

[Ir al registro ...](#)

Nombre de usuario:

gruPontallersr2223@gmail.com

Código secreto:

.....

Nombre de dominio:

gruPontallersrvpn.ddns.net

Iniciar sesión

Cerrar sesión

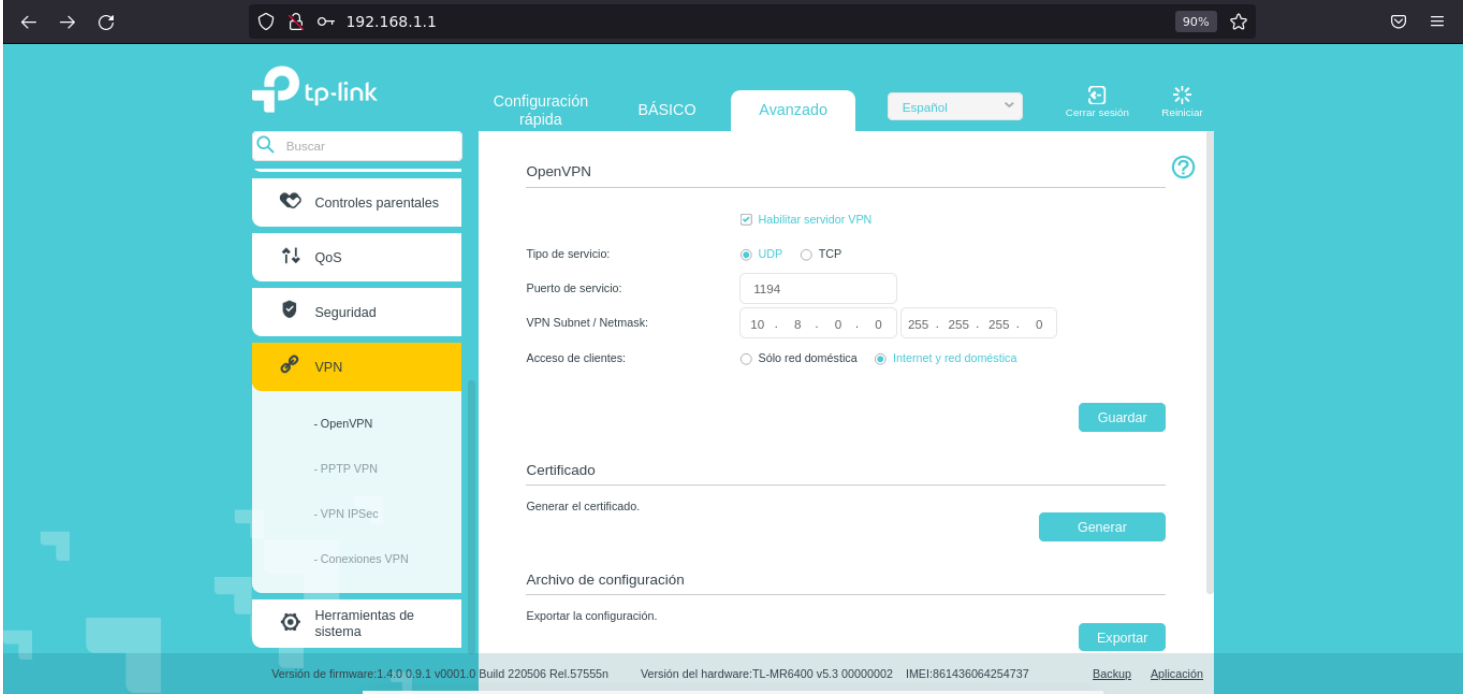
Desconectado

Guardar

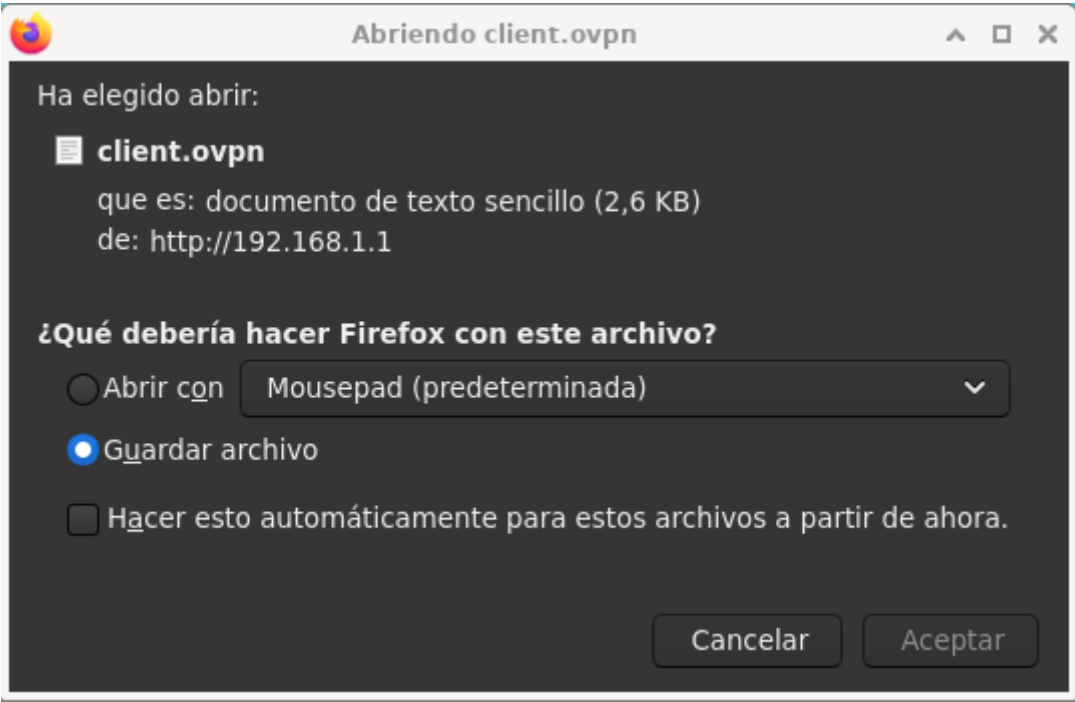
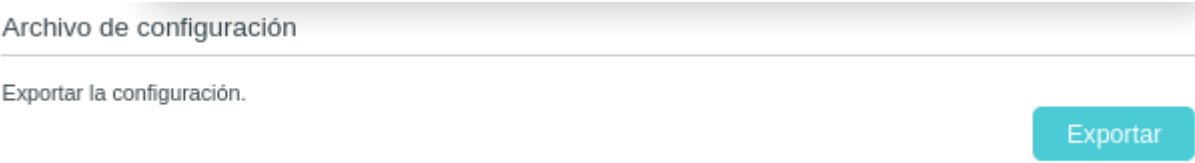




- e) Avisar ao docente para revisión ☐\_2
- f) Agora que xa temos todos os prerequisites realizados xa podemos configurar a conta VPN. Así:



- g) Falta exportar o certificado para que o poidan empregar os clientes na súa conexión VPN:



5. **Cientes VPN:** Podemos proceder como se indica na axuda do router:

### Guía de instalación de cliente VPN

Antes de configurar el servidor OpenVPN, configure el Servicio DNS Dinámico (recomendado) o asigne una dirección IP estática para el puerto WAN. Y asegúrese de que el puerto externo de configuración de NAT no sea el puerto de servicio y que la Hora del sistema esté sincronizada con Internet.

### Para conectar los dispositivos cliente al servidor OpenVPN:

1. Seleccione Activar servidor VPN.
2. Configure los parámetros del servidor OpenVPN (Tipo de servicio, Puerto de servicio, Acceso de cliente y Máscara de red / máscara de VPN) y haga clic en Guardar.
3. Haga clic en Exportar para guardar el archivo de configuración.
4. En los dispositivos cliente, descargue e instale la utilidad de cliente OpenVPN desde el sitio web [openvpn.net](https://openvpn.net). Las plataformas oficiales compatibles incluyen Windows, Mac OSX y Linux.
5. Inicie la utilidad de cliente OpenVPN y agregue una nueva conexión VPN utilizando el archivo de configuración guardado para conectar el dispositivo cliente al servidor VPN.

Nota: para obtener más información sobre los clientes OpenVPN, visite el sitio web [openvpn.net](https://openvpn.net).

Pero imos empregar outros clientes gráficos para poder establecer a conexión vpn mediante openvpn.

## 6. CGNAT Activado?

### **Definición CGNAT:**

CGNAT (Carrier-Grade Network Address Translation)(Tradución de Direccións de Rede de Nivel de Portador) é unha técnica que se utiliza nos provedores de servizos de Internet (ISP) para conservar e compartir direccións IP públicas entre varios clientes. En resumo, CGNAT é unha solución para enfrontar a escaseza de direccións IP públicas IPv4.

Á medida que a demanda de direccións IP públicas IPv4 aumentou exponencialmente debido ao crecemento de Internet e a proliferación de dispositivos conectados, a cantidade de direccións IPv4 dispoñibles tórnase limitada. Para solucionar este problema, os ISP implementan CGNAT para compartir un conxunto limitado de direccións IP públicas entre varios clientes.

### **Funcionamento CGNAT:**

1. Os clientes dun ISP reciben direccións IP privadas dentro dun rango específico (por exemplo, 10.0.0.0/8 ou 192.168.0.0/16) nas súas redes locais.
2. Cando un dispositivo na rede local dun cliente desexa comunicarse coa Internet, o router ou gateway do ISP realiza unha tradución da dirección de rede, convertendo a dirección IP privada do cliente nunha dirección IP pública compartida.
3. Os paquetes de datos enviados desde o dispositivo do cliente a través da dirección IP pública compartida pasan polo CGNAT do ISP. O CGNAT mantén unha táboa de tradución que asocia a dirección IP pública compartida coa dirección IP privada orixinal do cliente.
4. Cando os paquetes de datos de resposta regresan desde a Internet á dirección IP pública compartida, o CGNAT redirixeos ao cliente correcto segundo a táboa de tradución.

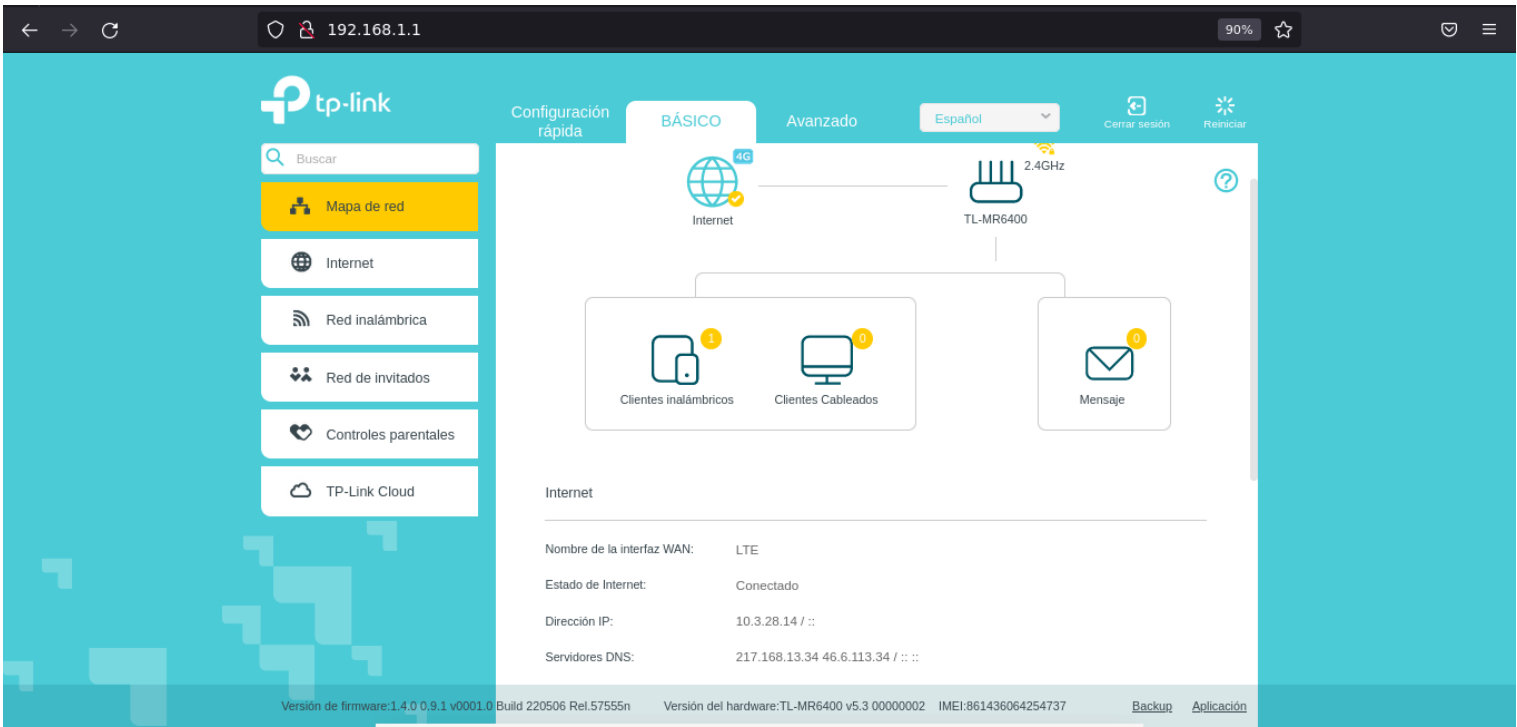
Esta técnica permite que varios clientes compartan a mesma dirección IP pública, o que estende o uso de direccións IPv4 e atrasa a necesidade de migrar a IPv6, que ofrece un espazo de direccións moito máis amplo.

Non obstante, CGNAT tamén pode ter algunhas limitacións, como dificultar o acceso a servizos de rede desde o exterior (como servidores VPN, web ou xogos en liña) debido á tradución de direccións e á falta dunha dirección IP pública dedicada para cada cliente.

En resumo, CGNAT é unha solución temporal para a escaseza de direccións IPv4 e permite aos ISP seguir proporcionando servizos de Internet a un gran número de clientes mentres se planifica e se migra gradualmente a IPv6, que ofrece un espazo de direccións IP moito máis grande e evita a necesidade de CGNAT.

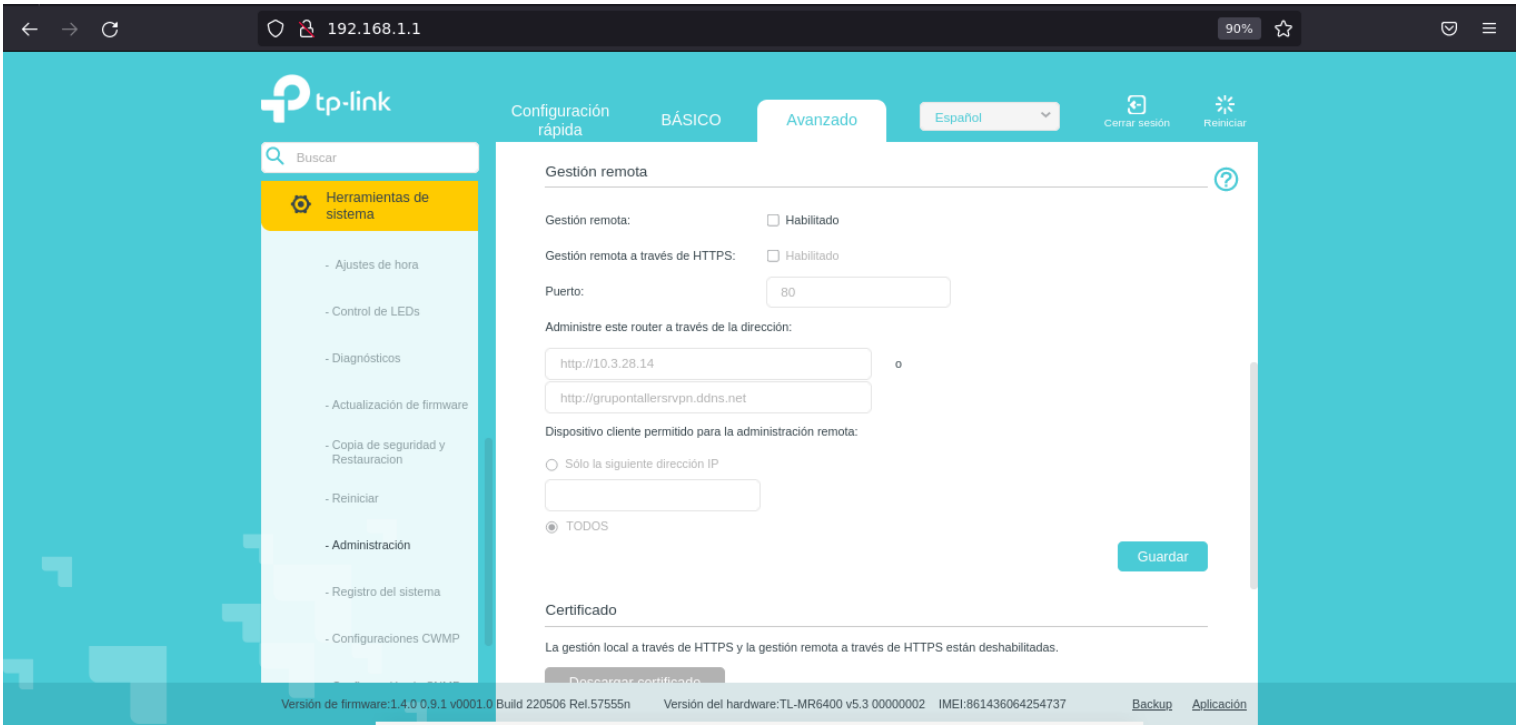
Para determinar se o router TL-MR6400 está detrás dunha conexión CGNAT, segue estes pasos:

1. Accede á configuración do router TL-MR6400 a través dun navegador web ingresando a dirección IP do router na barra de direccións. A dirección IP predeterminada do router TP-Link é tipicamente 192.168.0.1 ou 192.168.1.1. Se cambiaches a dirección IP do router, utiliza a nova dirección que configuraches.
2. Unha vez dentro da configuración do router, busca a sección de "BÁSICO" → "Mapa de red" → "Internet" → "Dirección IP". Deberías atopar alí a dirección IP pública que o router está a recibir do proveedor de servizos de Internet (ISP). Esta dirección IP é a que o ISP asigna ao router para identificalo en Internet.



Tamén pódese atopar esa información en:

"Avanzado" → "Herramientas del sistema" → "Administración" → "Gestión Remota"



3. Anota a dirección IP pública que se mostra na configuración do router na *Táboa3. CGNAT*
4. Logo, abre un navegador web e accede a un sitio web que te mostre a túa dirección IP pública actual, como "https://www.whatismyip.com/" ou "https://www.whatismyip.net/" e anota a dirección IP pública que se mostra na configuración do router na *Táboa3. CGNAT*
5. Compara a dirección IP pública obtida no paso 3 coa dirección IP pública mostrada no sitio web, no paso 4. Se ambas as direccións IP son diferentes, isto indica que o router TL-MR6400 está detrás dunha conexión CGNAT.

Se as direccións IP públicas son diferentes, o router TL-MR6400 está detrás dun CGNAT implementado polo ISP. Isto pode afectar a configuración de certos servizos ou aplicacións que requiren acceso externo a dispositivos na túa rede local, como servidores VPN ou servidores web.

E se as direccións IP públicas son iguais, o router TL-MR6400 non está detrás dun CGNAT implementado polo ISP, sendo posible o acceso externo de clientes a dispositivos na túa rede local, como servidores VPN ou servidores web.

**En calquera caso, seguiremos coa práctica tendo en conta que se se está detrás dun CGNAT non será posible a conexión de clientes VPN co noso router.**

7. Avisar ao docente para revisión ☐₃

## 8. Clientes VPN

### a) Cliente gráfico GNU/Linux → NetworkManager OpenVPN

#### Portátil: Empregar o portátil como cliente VPN GNU/Linux

Existen varios clientes gráficos de OpenVPN dispoñibles para distribucións GNU/Linux como Debian. Un dos clientes máis populares e amplamente utilizado é "NetworkManager-openvpn". A continuación, proporciónase un procedemento xeral para utilizar NetworkManager-openvpn en Debian (ou en sistemas baseados en Debian):

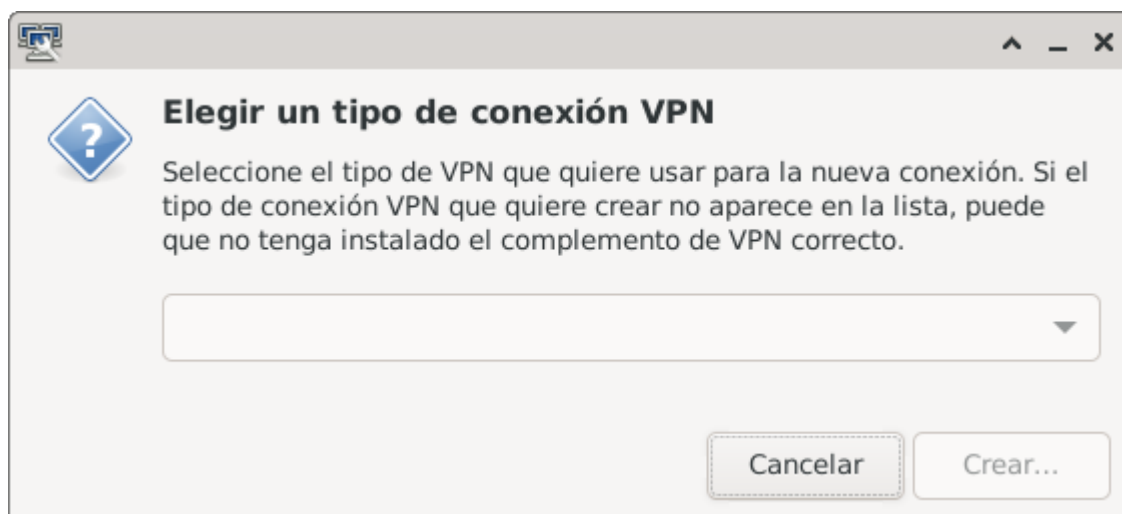
1. Nunha consola executar:

```
$ setxkbmap es
```

```
$ sudo apt update && sudo apt-get install network-manager
```

2. Engadir unha nova conexión VPN no cliente gráfico NetworkManager:

NetworkManager → Conexiones VPN → Añadir una conexión VPN



3. É preciso ter instalado o paquete "network-manager-openvpn" para habilitar o soporte de OpenVPN en NetworkManager:

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

4. Reinicia o servizo NetworkManager para asegurarte de que os cambios se aplican correctamente:

```
$ sudo systemctl restart NetworkManager
```

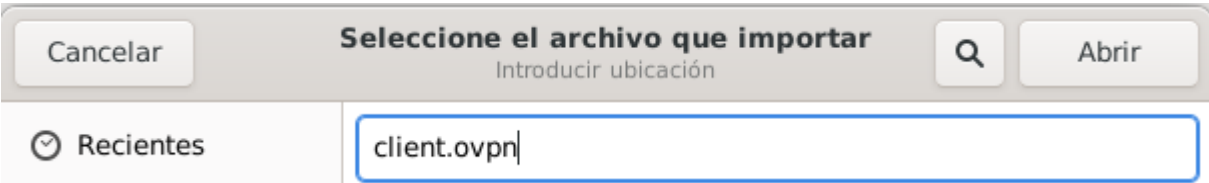
5. Agora, deberíades poder atopar unha nova opción de conexión VPN no menú de rede do voso entorno de escritorio (ver paso 2.)



6. Na configuración de VPN, selecciona a opción para engadir unha nova conexión e escolle "Importar una configuración VPN guardada..."



7. Localiza e selecciona o arquivo de configuración de OpenVPN que exportáchedes dende o router TP-Link TL-MR6400.



8. Completa calquera campo adicional necesario, como as credenciais de autenticación, segundo a configuración da túa conexión VPN.



9. Garda a configuración e intenta establecer a conexión VPN seleccionando a nova conexión no menú de rede.

10. Avisar ao docente para revisión ☐4

**NOTA<sub>3</sub>:** Ten en conta que os pasos específicos poden variar lixeiramente segundo o entorno de escritorio que estás a utilizar na túa distribución Debian. Asegúrate de consultar a documentación do entorno de escritorio ou os recursos específicos da túa distribución para obter instrucións máis detalladas.

## b) Cliente gráficoAndroid → OpenVPN Connect

### Móviles Android

Existen varios clientes gráficos de OpenVPN dispoñibles para dispositivos móbiles Android que che permiten conectarte a unha conexión OpenVPN. Un dos clientes máis populares e amplamente utilizado é "OpenVPN Connect". A continuación, proporciónase un procedemento xeral para utilizar OpenVPN Connect nun teléfono móbil Android:

1. Instalar a aplicación "OpenVPN Connect" dende Google Play Store e seguir o proceso de instalación normal.
2. Unha vez instalado, abrir a aplicación "OpenVPN Connect" no teléfono móbil Android.
3. Transferir o certificado de cliente necesario e o arquivo de configuración que exportaches dende o router TP-Link TL-MR6400 ao teléfono móbil. Pódese facer mediante correo electrónico, almacenamento na nube ou outra forma de transferencia de arquivos.

4. No teléfono móbil, abrir a aplicación "OpenVPN Connect" e seleccionar a opción de importar a configuración ou o arquivo de configuración.
5. Localizar e seleccionar o arquivo de configuración de OpenVPN que se transferiu ao teléfono móbil.
6. A aplicación importará automaticamente a configuración e mostrará unha lista de perfís VPN dispoñibles.
7. Seleccionar o perfil VPN correspondente á conexión OpenVPN configurada no router TP-Link TL-MR6400.
8. Introducir as credenciais de autenticación se é necesario.
9. Tocar o botón de conexión para establecer a conexión VPN.
10. Unha vez completados estes pasos, OpenVPN Connect intentará establecer a conexión utilizando a configuración proporcionada. Se a conexión é exitosa, verase unha mensaxe indicando que se está conectado ao router TP-Link TL-MR6400 a través de OpenVPN.
11. Cubrir a *Táboa2. VPN: Móviles alumnado*
12. Avisar ao docente para revisión ☐ 5

**NOTA:** Recorda que os pasos específicos poden variar lixeiramente dependendo da versión da aplicación "OpenVPN Connect" e da configuración exacta da túa conexión OpenVPN.

## 9. Razoa. Contesta brevemente:

- a) Definir NTP. Por que é necesario para que funcionen as conexións VPN?
- b) Definir IP Estática ofrecida polo ISP.
- c) Definir IP Dinámica ofrecida polo ISP.
- d) Se o noso ISP ofrecenos unha IP Dinámica, por que e para que configurar Dynamic DNS no router do noso domicilio?
- e) Definir VPN.
- f) Pódese acceder mediante unha conexión VPN a servidores configurados nun domicilio?
- g) Pódese mediante unha conexión VPN acceder a un domicilio e saír a Internet como se estivésemos "in situ" no domicilio?
- h) Imaxinemos que unha páxina web soamente deixa acceder dende unha localización dentro de Galicia. Poderíades fóra de Galicia acceder a esa páxina web? Como?
- i) Para que serve o comando GNU/Linux `traceroute`
- j) Existen diferencias ao executar o comando seguinte nunha consola nun cliente GNU/Linux (Portátil):  

```
$ traceroute www.google.es
```

Nunha conexión VPN e nunha conexión a Internet non VPN(WiFi ou ethernet)?

- k) CGNAT: Executa e explica o que fan os seguintes comandos:

```
$ wget -qO- https://ipinfo.io/ip
$ host grupontallersrvpn.ddns.net
$ dig grupontallersrvpn.ddns.net
$ nslookup grupontallersrvpn.ddns.net
```

Compara a saída coa *Táboa3. CGNAT*. Que acontece? Que podes concluír con respecto a CGNAT?

l) CGNAT: Executa e explica o que fan os seguintes comandos:

```
$ wget -qO- https://ipinfo.io/ip  
$ host grupontallersrvpn.ddns.net 8.8.8.8  
$ dig @8.8.8.8 grupontallersrvpn.ddns.net  
$ nslookup grupontallersrvpn.ddns.net 8.8.8.8
```

Compara a saída coa *Táboa3*. CGNAT. Que acontece? Que podes concluír con respecto a CGNAT?

Que ten de diferente este apartado co anterior?

m) Se o noso ISP ten activado CGNAT e configuramos VPN no router, é posible que os clientes externos á nosa rede poidan acceder coa nosa conexión VPN configurada? Fai un diagrama que explique a túa resposta.

n) Se o noso ISP ten activado CGNAT e configuramos NAT Forwarding(redirección de portos) no router, é posible que os clientes externos á nosa rede poidan acceder a un servidor web que temos configurado nun equipo pertencente á nosa rede? Fai un diagrama que explique a túa resposta.

10. Avisar ao docente para a entrega e revisión da práctica. ☐ 6

Táboa 1: Móviles alumnado

Móbil alumnado	MAC-Address
1	
2	
3	

Táboa 2: VPN: Móviles alumnado

Móbil alumnado	MAC-Address
1	
2	
3	

Táboa 3: CGNAT

Fonte	IP Pública
Router TL-MR6400	
<a href="https://www.whatismyip.com/">https://www.whatismyip.com/</a>	
<a href="https://www.whatismyip.net/">https://www.whatismyip.net/</a>	

Revisión:

☐1

☐2

☐3

☐4

☐5

☐6

