

MTCNA Lab 9

1



LABORATORIO



- VPN son la siglas de **V**irtual **P**rivate **N**etwork (Red Privada Virtual).
- La vpn nos permiten extender nuestra red a través de redes que no son de confianza, por ejemplo internet.
- Básicamente con la vpn vamos a transportar paquetes IP.
- Las vpn pueden empezar la pila OSI desde la capa 2 o directamente desde la capa 3.
- Si empiezan en la capa 2 soportan todos los servicios de capa 2, tales como: dhcp server, PPPoE. También se puede agregar la vpn a un bridge, para así ampliar el dominio de broadcast.

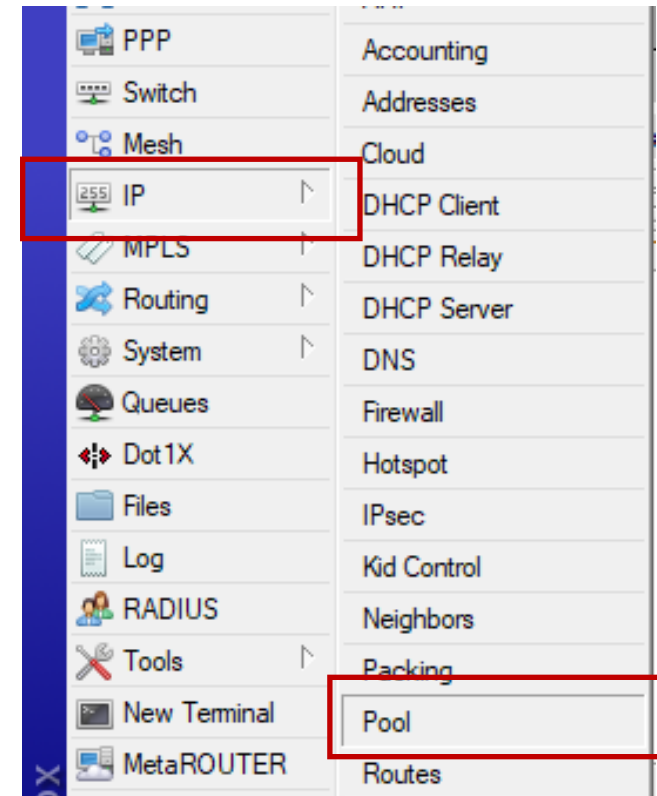
- Hay que tener en cuenta que podemos anidar las vpn siempre y cuando la capa que transporta la exterior es compatible con la capa que necesita la vpn interior para establecerse. Por ejemplo
 - PPPoE over EoIP
 - ✓ Funciona
 - ✓ PPPoE necesita capa 2 para establecerse y EoIP transporta capa 2
 - PPPoE over L2TP
 - × No funciona
 - × PPPoE necesita capa 2 para establecerse y L2TP transporta capa 3
 - PPPoE over L2TP BCP
 - ✓ Funciona
 - ✓ PPPoE necesita capa 2 para establecerse y L2TP con la extensión BCP transporta capa 2.
 - L2TP over PPPoE
 - Funciona
 - L2TP necesita capa 3 para establecerse y PPPoE transporta capa 3.

VPN - Pool

4



- Primero necesitamos crear un Pool para las IP de los clientes.
- Vamos al menú IP y pulsamos en Pool.

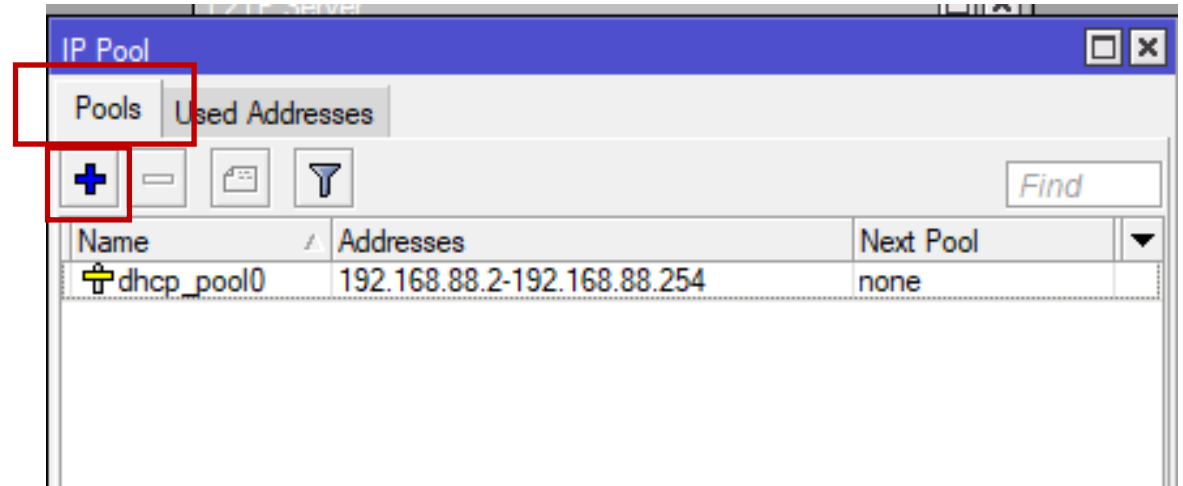


VPN - Pool

5



- Se nos abre la ventana de los pool.
- Seleccionamos la pestaña *Pools*.
 - ✓ Es Posible que esté ya creado el pool que utiliza el servidor de DHCP de la red local.
- Pulsamos el botón de +.



VPN - Pool

6



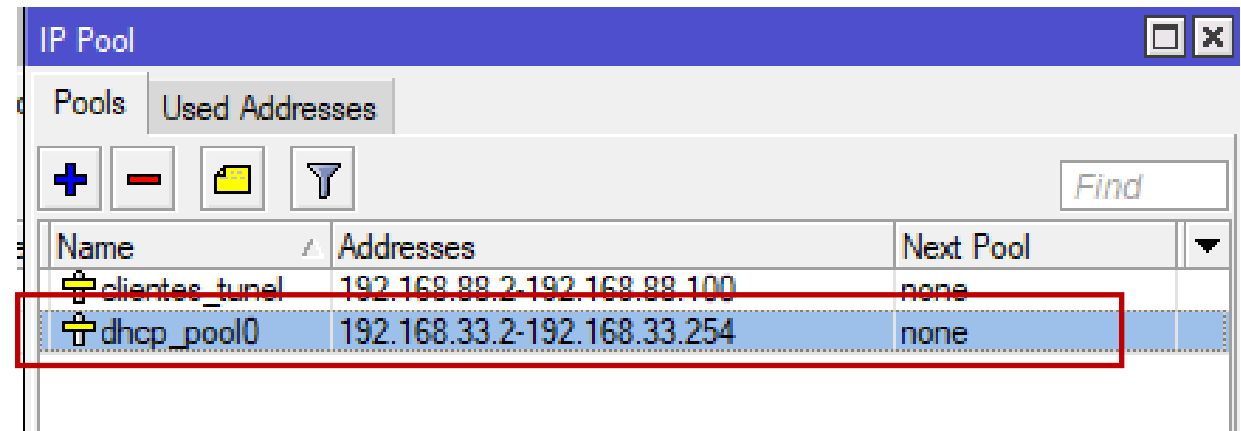
- Se nos abre el diálogo de un nuevo pool.
- En el campo *Name* escribimos el nombre que le daremos al pool, en este caso clientes_túnel.
- En el campo *Addresses* ponemos el rango de direcciones que asignaremos a los clientes, en este caso 192.168.88.2-192.168.88.100.
- Pulsamos el botón *OK*.

VPN - Pool

7



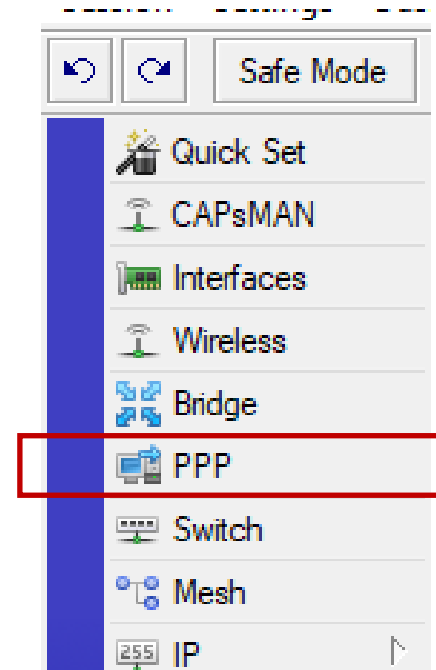
- Volvemos a la ventana de los pool.
- Vemos que se ha creado el pool *clientes_túnel*.



Name	Addresses	Next Pool
clientes_tunel	192.168.88.2-192.168.88.100	none
dhcp_pool0	192.168.33.2-192.168.33.254	none

➤ Ahora vamos a la parte de PPP.

- Para ello vamos al menú *PPP*.

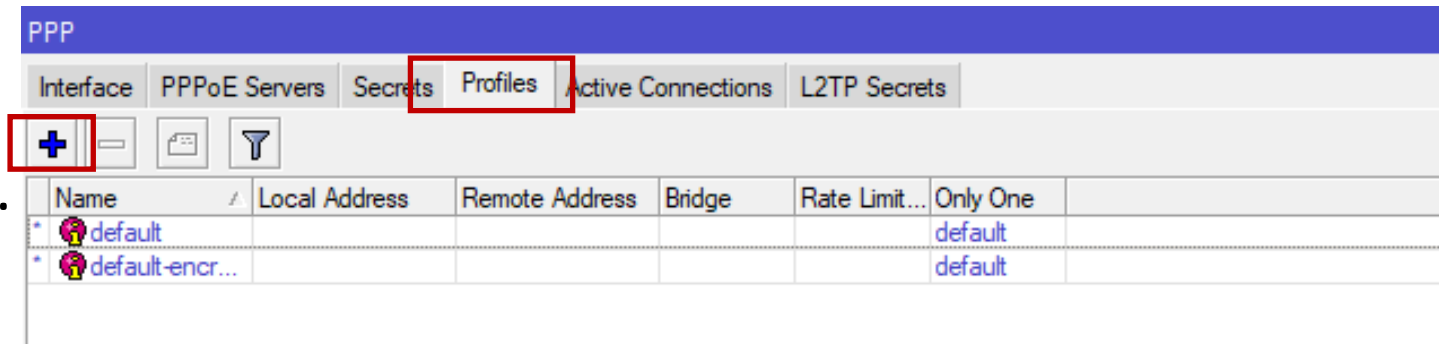


VPN - Profile

9



- Se nos abre la ventana del PPP.
- Seleccionamos la pestaña de Profile.
- Nos aparecen los perfiles por defecto.
 - ✓ default: sin cifrado.
 - ✓ default-encryption: con cifrado.
- Le damos al botón de +.
- En el perfil de usuario parametrizaremos las opciones comunes a todos los usuarios.



VPN - Profile

10



- Se nos abre el diálogo de un nuevo perfil.
- En el campo *Name* escribimos el nombre del perfil. En este caso “clientes”.
- En el campo *Local Address*, escribimos la dirección IP que tendrá en router en su extremos del túnel, en este caso 192.168.33.1
- En el campo *Remote Address*, escribimos la ip que tendrá el equipo cliente del túnel. Podemos poner una ip o un pool de direcciones. En este caso clientes_tunnel.
- En el campo *DNS Server* pondremos 8.8.8.8.
- Le damos al botón de *OK*.

New PPP Profile

General Protocols Limits Queue Scripts

Name: clientes

Local Address: 192.168.33.1

Remote Address: clientes_tunnel

Bridge:

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server: 8.8.8.8

WINS Server:

Change TCP MSS

☐ no ☐ yes ☒ default

VPN - Profile

11



- Ahora en Profiles vemos nuestro recién creado perfil.

PPP

Interface

PPPoE Servers

Secrets

Profiles

Active Connections

L2TP Secrets









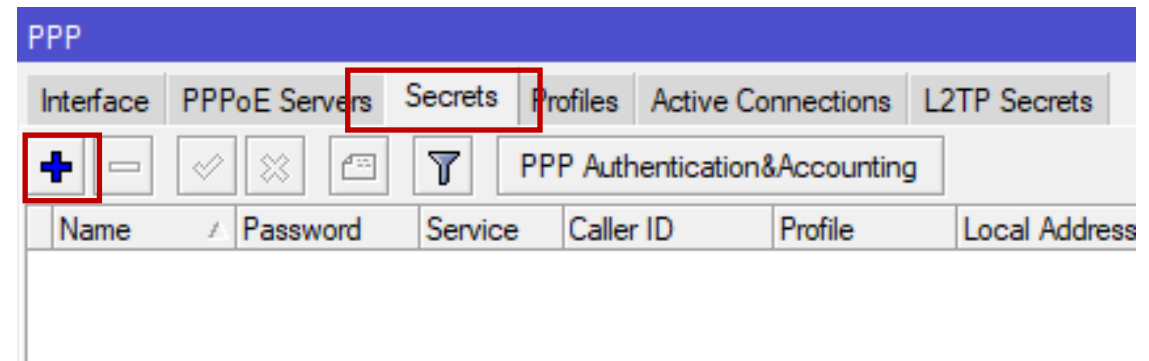
Name	Local Address	Remote Address	Bridge	Rate Limit...	Only One
 clientes	192.168.33.1	clientes_tunnel			default
 default					default
*  default-encr...					default

VPN - Secrets

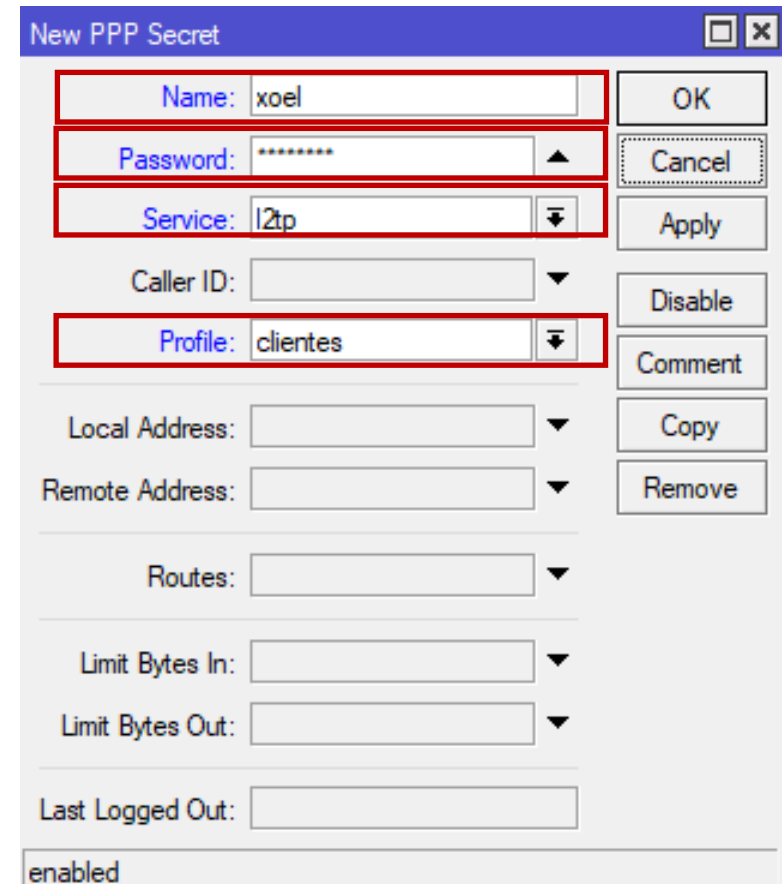
12



- Ahora vamos a crear el usuario y contraseña del cliente.
- Para ello pulsamos en la pestaña *Secrets*.
- Pulsamos en el botón +.



- Se nos abre el diálogo de un nuevo usuario.
- En el campo *Name* ponemos el nombre del usuario, en el ejemplo *xoel*.
- En el campo *Password* ponemos la contraseña, en el ejemplo *esmisecreto*.
- En el campo *Service* seleccionamos *l2tp* para que únicamente se pueda conectar por el servicio de L2TP.
- En el campo *Profile*, escribimos el perfil que hemos creado anteriormente, “*clientes*”.



New PPP Secret

Name: xoel

Password: *****

Service: l2tp

Caller ID:

Profile: clientes

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

OK

Cancel

Apply

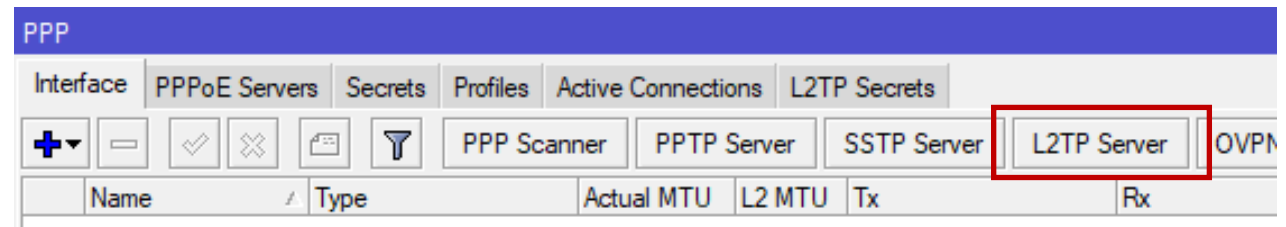
Disable

Comment

Copy

Remove

- Ahora vamos a configurar el servidor de L2TP.
- Seleccionamos la pestaña *Interface*.
- Para activar el servidor pulsamos en el botón *L2TP Server*.

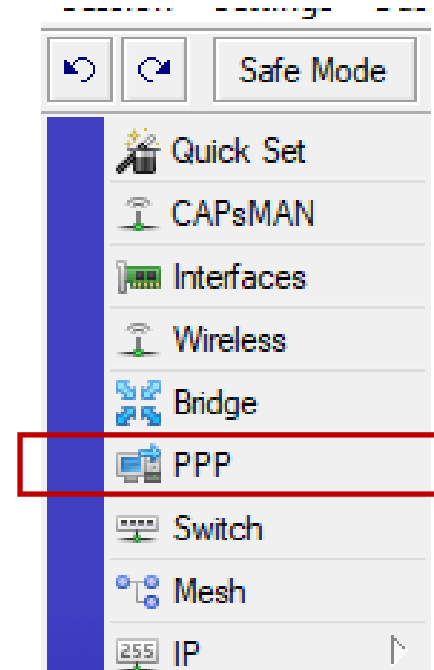


- Se nos abre el diálogo de la configuración del servidor L2TP.
 - Marcamos la opción de *Enabled*.
 - En las opciones de *Authentication* desmarcamos *chap* y *pap*.
 - Pulsamos *OK*.
- Únicamente se configura un servidor L2TP. Este servidor responderá por todas las direcciones IP que tiene el router.
- Con la opción Use IPsec estamos securizando el túnel L2TP sobre un túnel IPsec de forma transparente. Es decir, L2TP no usará GRE sino que utilizará IKEv1.

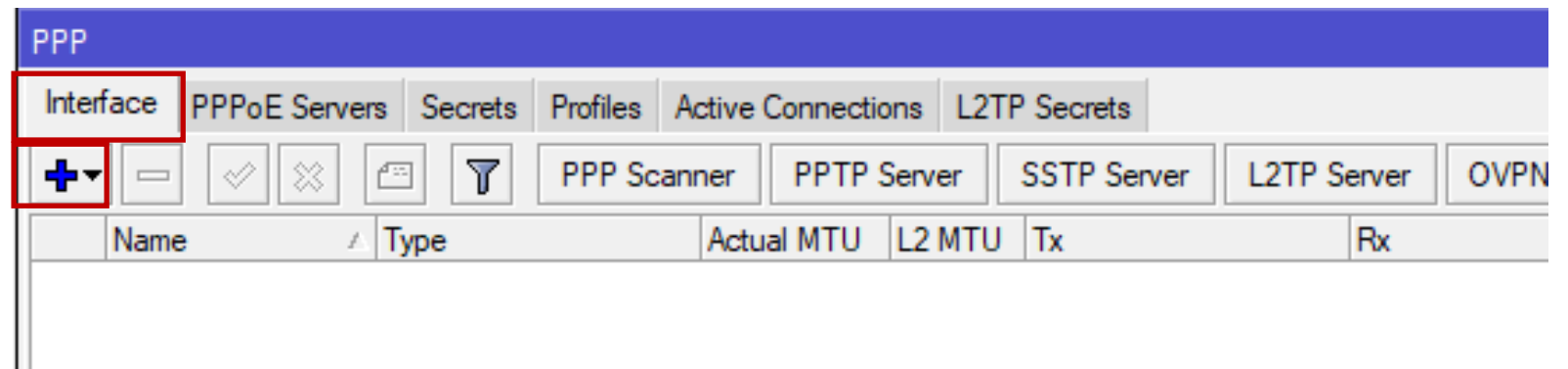
The screenshot shows the 'L2TP Server' configuration window. The 'Enabled' checkbox is checked and highlighted with a red box. The 'Authentication' section shows 'mschap2' and 'mschap1' checked, while 'chap' and 'pap' are unchecked. The 'OK' button is also highlighted with a red box. Other fields include Max MTU: 1450, Max MRU: 1450, MRRU: (empty), Keepalive Timeout: 30, Default Profile: default-encryption, Max Sessions: (empty), Use IPsec: no, IPsec Secret: (empty), Caller ID Type: ip address, One Session Per Host: unchecked, and Allow Fast Path: unchecked.

- Para configurar el cliente cliente vamos a utilizar el router R2:

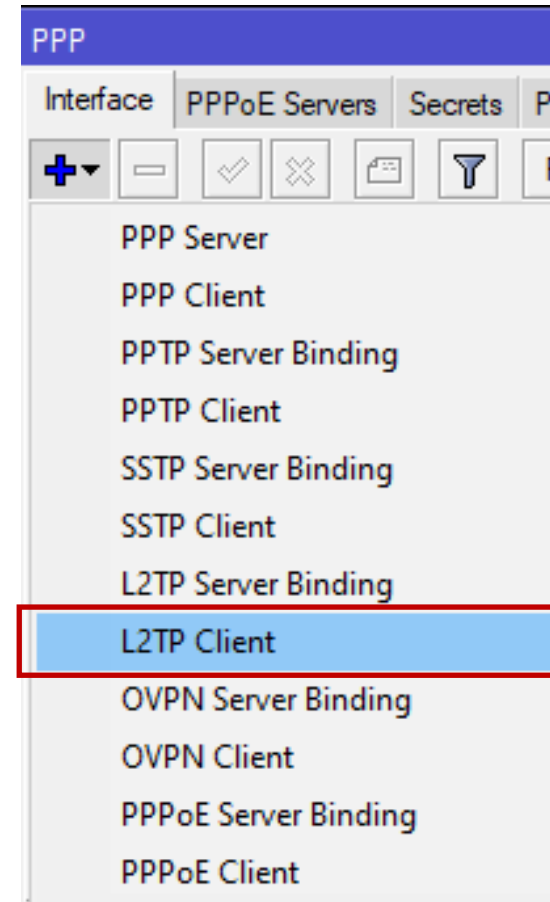
- Vamos al menú *PPP*.



- Vamos al menú PPP.
- Nos posicionamos en la pestaña *Interfaces*.
- Pulsamos el botón de +.



- Seleccionamos *L2TP Client*.



VPN - Cliente

20



- Nos aparece el dialogo de crear un cliente L2TP.
- Nos posicionamos en la pestaña *Dial Out*.
- En el campo *Connect To* ponemos la ip del servidor 192.168.101.1.
- En el campo *User* ponemos el nombre del usuario, en el ejemplo *xoel*.
- En el campo *Password* ponemos la contraseña, en el ejemplo *esmisecreto*.
- Marcamos el campo de *Add Default Route*.
- En el campo *Allow* desmarcamos la opción *chap* y *pap*.
- Pulsamos el botón de *OK*.

VPN - Cliente

21



- Ahora en la ventana PPP vemos nuestros cliente que acabamos de crear.
- En el momento que conecta con el Servidor se pone en estado R (Running).
- Si vamos al IP -> Addresses veremos la IP que nos ha asignado el servidor de túneles.

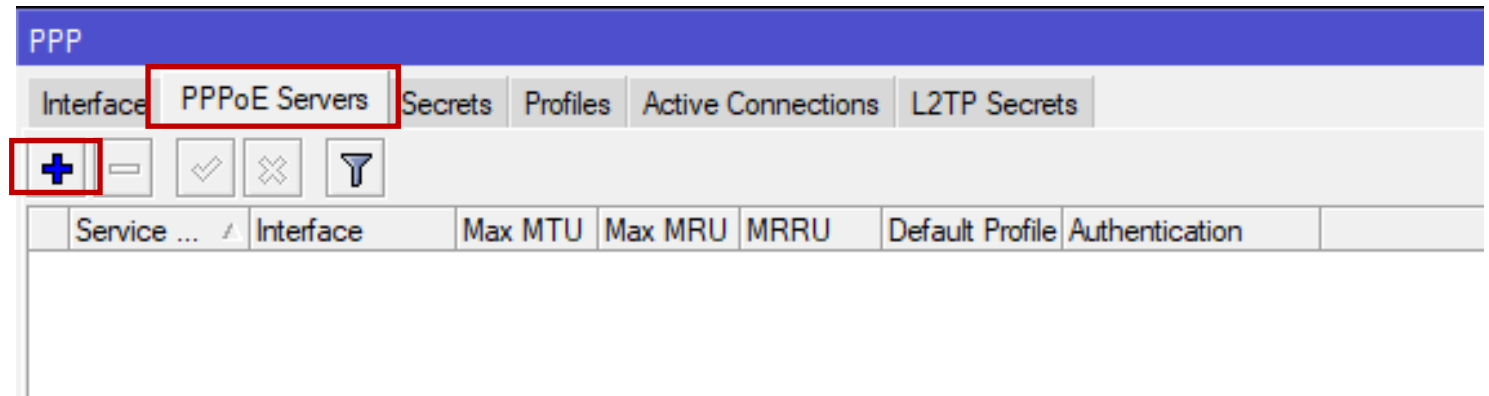
PPP							
Interface		PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets	
+ - [Icons] PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server							
Name	Type	Actual MTU	L2 MTU	Tx	Rx		
l2tp-out1	L2TP Client				0 bps	0 bps	

PPP							
Interface		PPPoE Servers	Secrets	Profiles	Active Connections	L2TP Secrets	
+ - [Icons] PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server							
Name	Type	Actual MTU	L2 MTU	Tx	Rx		
R l2tp-out1	L2TP Client	1450			0 bps	0 bps	

Address List			
+ - [Icons] Find			
	Address	Network	Interface
D	192.168.33.2	192.168.33.1	l2tp-out1
D	192.168.88.73/24	192.168.88.0	ether1

- Desde R2 podemos hacer ping a internet a través del tunel.
- Si ejecutamos la herramienta traceroute veremos que pasamos por la 192.168.33.1 que es la ip R1 en el tunel.
- Hemos configurado una vpn a través de una red IP. Como el cliente L2TP únicamente necesita la IP del servidor, podemos hacer un tunel entre el instituto y nuestra casa de forma segura.
- Hay que tener en cuenta que en el servidor, deberemos de abrir los puertos necesarios para que el cliente se pueda conectar.
- En el caso de L2TP deberemos de abrir el protocolo GRE (47) y el puerto 1701 UDP.

- El servidor PPPoE tiene su propia pestaña.
- Si queremos configurar uno deberemos seleccionar la pestaña *PPPoE Servers* dentro de la ventana de *PPP*.
- Pulsamos el botón de +.



- Se nos abre el diálogo de un nuevo servidor PPPoE.
- En el campo *Service Name* ponemos el nombre del servicio. Es un campo opcional (aunque no tenga la flecha arriba), podemos borrarlo para que no haya un nombre definido.
- En el campo *Interface* seleccionaremos en interfaz en el que queremos que escuche el servidor.
- En el campo *Authentication* desmarcamos las opciones de *pap* y *chap*.

