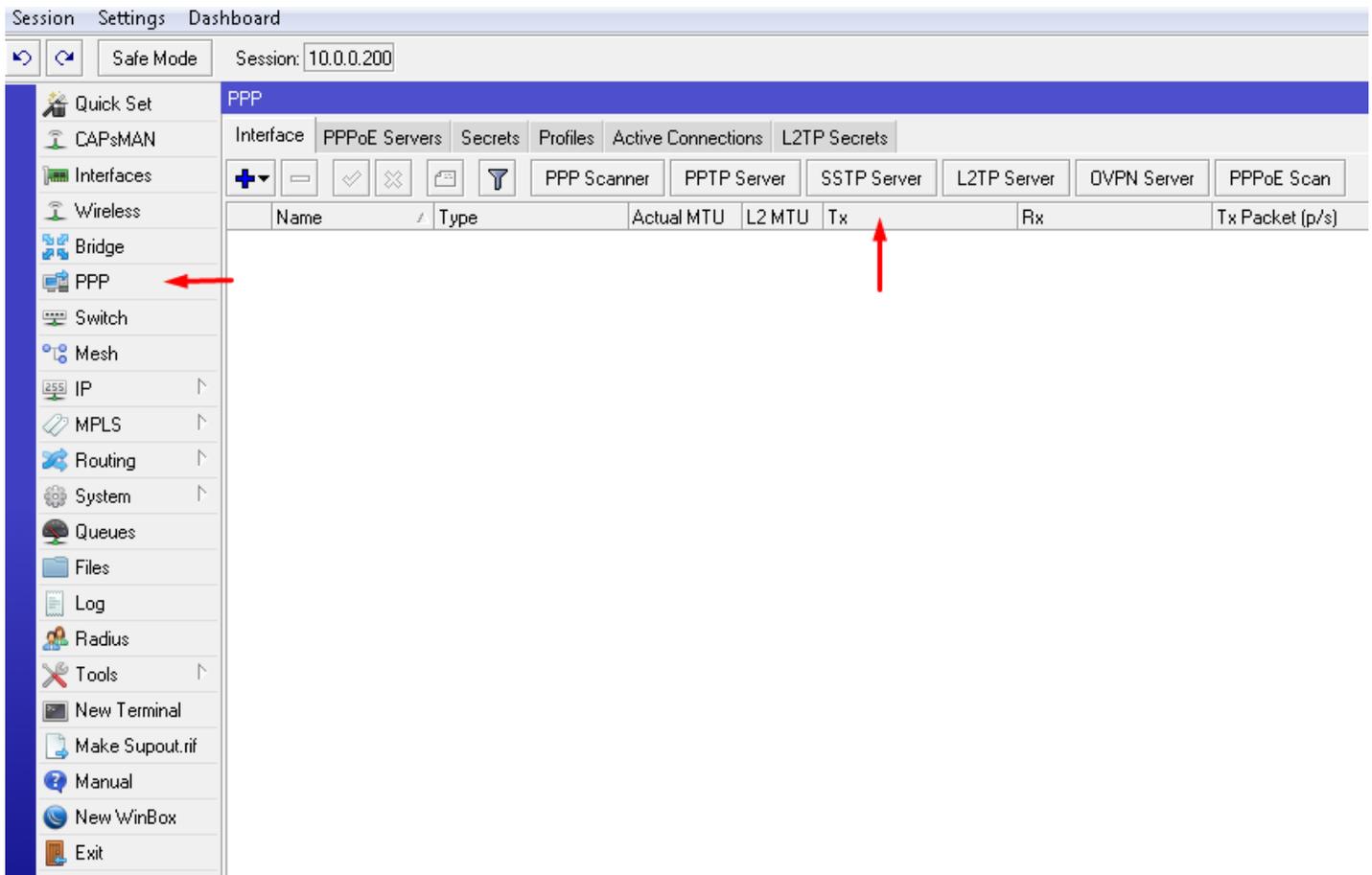


Laboratorio 3.1: Configuración de SSTP server sin Certificados.

Objetivos: Configurar un Túnel SSTP server en su Router MikroTik.

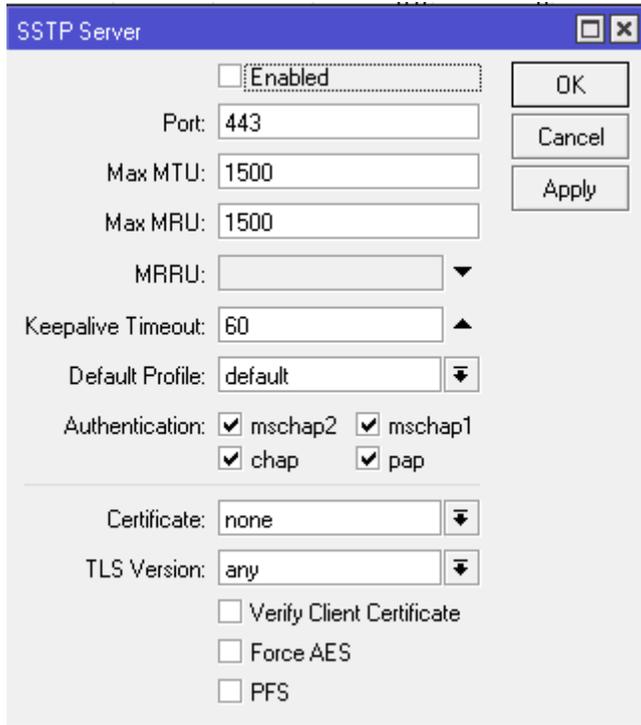
Paso 1: Una vez dentro de nuestro Winbox nos dirigimos a la pestaña PPP luego allí seleccionamos SSTP server,



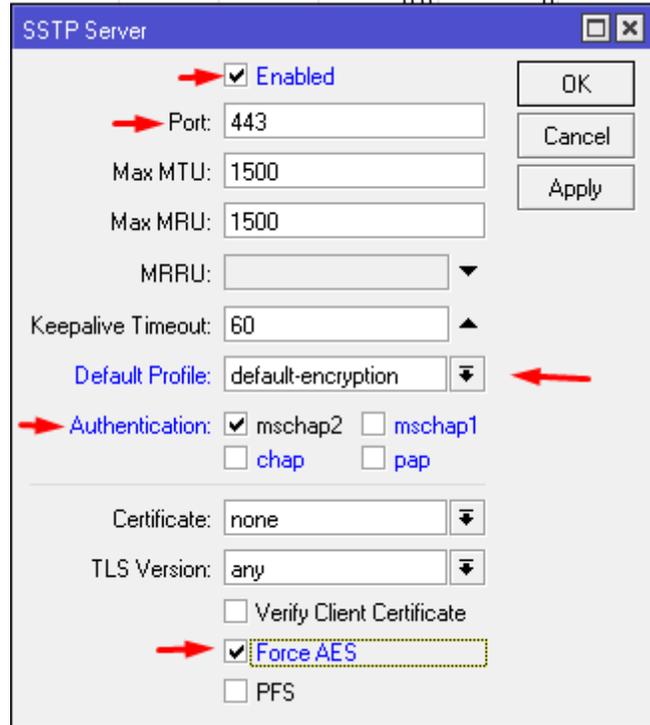
3.1

Paso 2: Al momento de abrir la pestaña de configuración SSTP Server podemos ver como esta deshabilitado y toda la configuración por defecto del servicio como nos muestra la imagen 3.2.

Ahora habilitaremos el SSTP, Seleccionamos el puerto, aplicamos la Authentication: mschp2 solamente, colocamos el default profile y por último forzamos para que el protocolo AES esté presente en la conexión tal y como se muestra en la imagen 3.3.

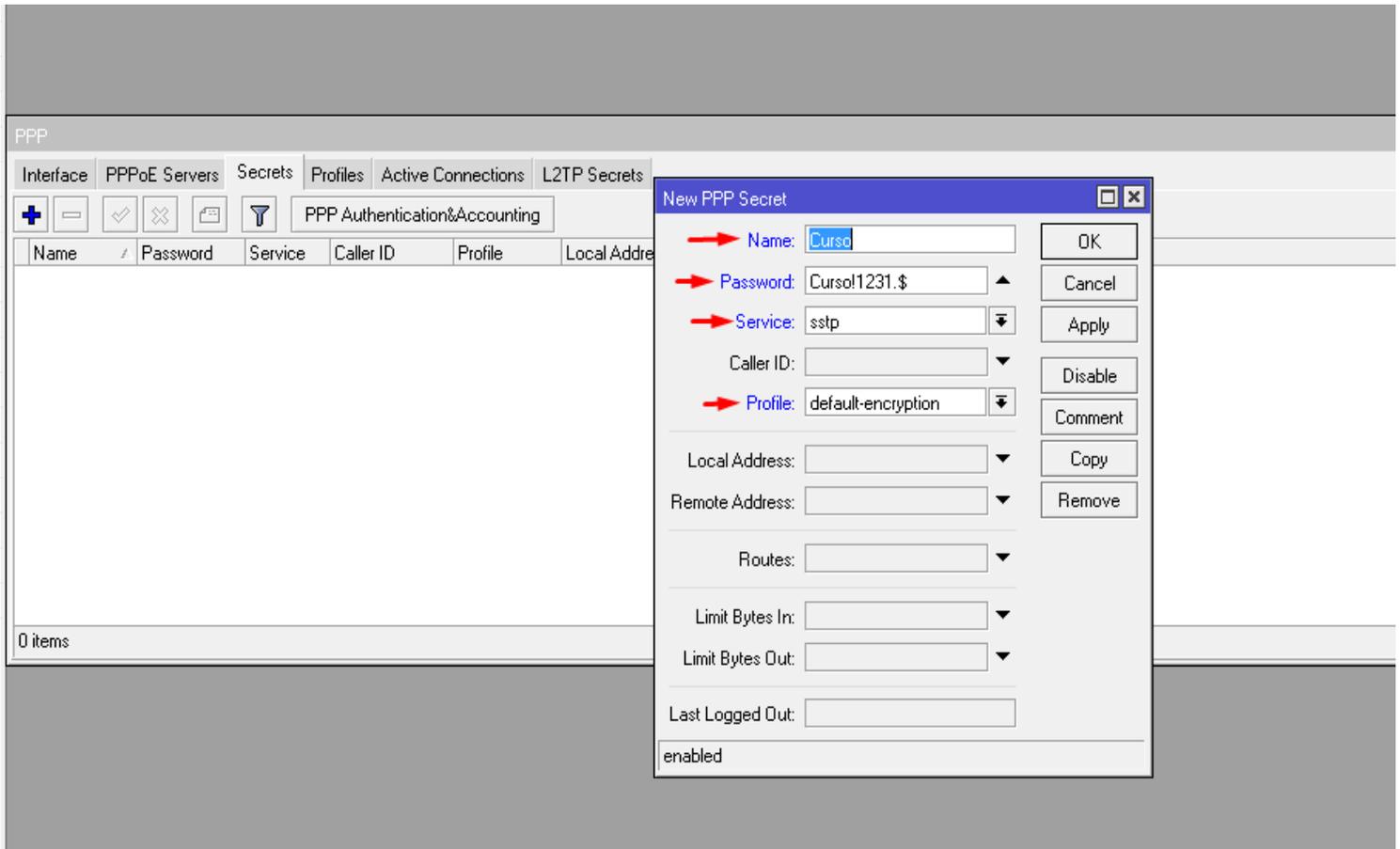


3.2



3.3

Paso 3: Ahora procedemos a crear las credenciales de nuestro cliente SSTP, para ello nos dirigimos a la pestaña secret, una vez allí le damos al signo de + y nos mostrara la ventana de configuración, especificamos el Name, Password, Service y por últimos Profile, el servicio SSTP.



The screenshot shows the Mikrotik WinBox interface. The main window is titled 'PPP' and has several tabs: 'Interface', 'PPPoE Servers', 'Secrets', 'Profiles', 'Active Connections', and 'L2TP Secrets'. The 'Secrets' tab is selected, and the 'PPP Authentication & Accounting' window is open. A 'New PPP Secret' dialog box is displayed in the foreground. The dialog has the following fields and values:

- Name: Curso
- Password: Curso!1231.\$
- Service: sstp
- Profile: default-encryption
- Local Address: (empty)
- Remote Address: (empty)
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: (empty)

The 'enabled' checkbox at the bottom of the dialog is checked. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

3.4

Paso 4: Ahora procedemos a crear la regla en nuestro firewall aceptando el tráfico entrante del puerto 443 en nuestro Mikrotik como vemos en la imagen 3.5.

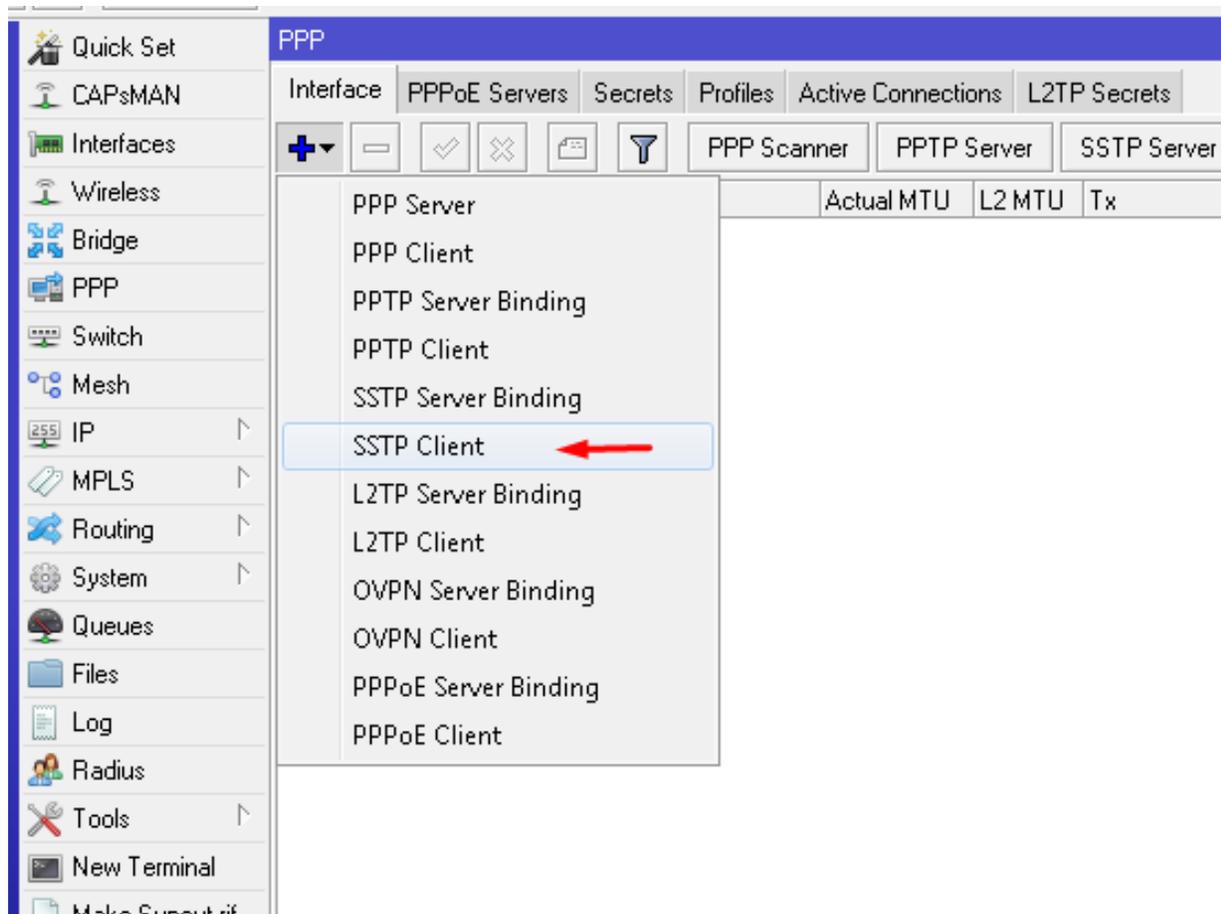
#	Action	Chain	Src. Address	Dst. Address	Proto...	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
::: Basic Firewall											
0	✗ drop	Basic_Fire...								0 B	
1	🔗 jump	input								44.2 KiB	6
2	🔗 jump	forward								0 B	
::: Portscan drop											
3	✗ drop	input								0 B	
::: Port scan detection											
4	➡ add...	input			6 (tcp)					0 B	
::: Dos attack drop											
5	🚫 tarpit	input			6 (tcp)					0 B	
::: Dos attack detect											
6	➡ add...	input			6 (tcp)					0 B	
::: BLOQUEA DURANTE 24 horas quien haga 5 intentos seguidos de login SSH!											
7	✗ drop	input			6 (tcp)		22			0 B	
8	➡ add...	input			6 (tcp)		22			0 B	
9	➡ add...	input			6 (tcp)		22			0 B	
::: BLOQUEA DURANTE 24 horas quien haga 5 intentos seguidos de login winbox!											
10	✗ drop	input			6 (tcp)		8291			0 B	
11	➡ add...	input			6 (tcp)		8291			0 B	
12	➡ add...	input			6 (tcp)		8291			0 B	
13	➡ add...	input			6 (tcp)		8291			0 B	
::: Allow Traffic SSTP ←											
14	✅ acc...	input			6 (tcp)		443			0 B	

3.5

Laboratorio 3.1.2: Configuración de SSTP Cliente sin Certificados en Mikrotik.

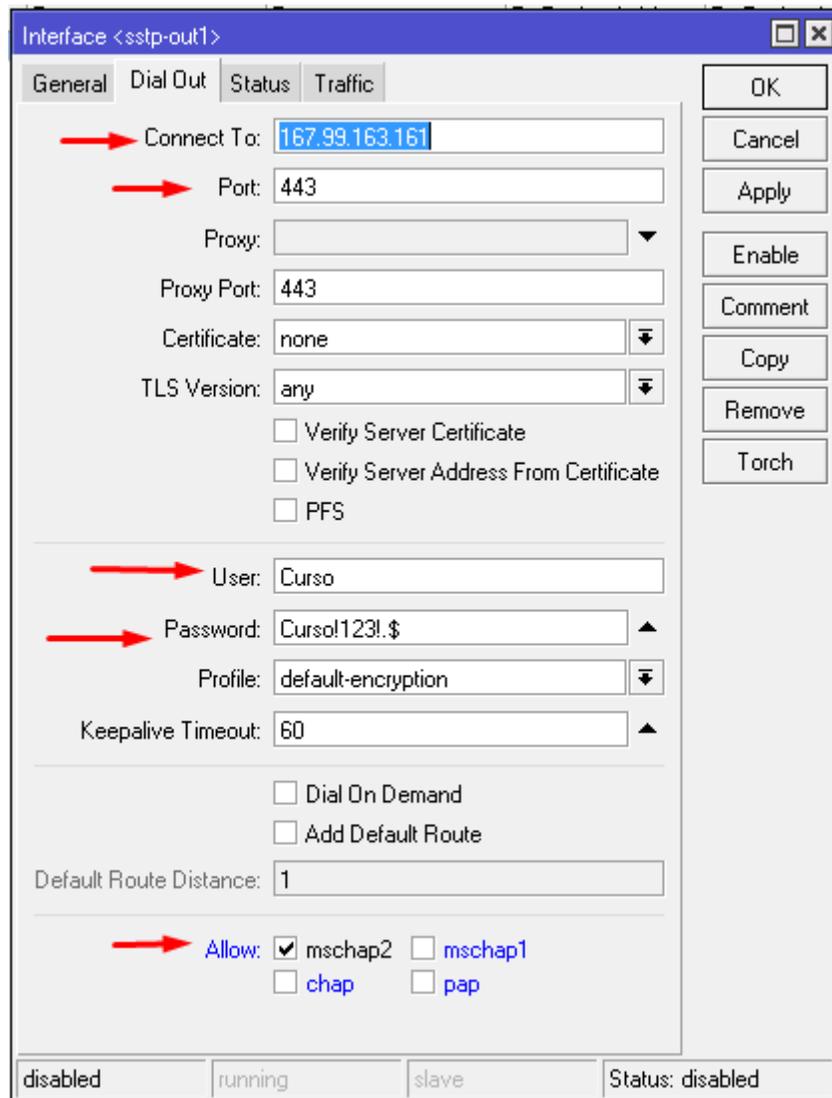
Objetivos: Configurar un SSTP Client en Mikrotik.

Paso 1: en esta ocasión nos dirigimos a otro Router MikroTik donde configuraremos nuestro cliente SSTP, para ello volvemos a la pestaña PPP-Interface una vez allí seleccionamos el signo de + y elegimos SSTP client como veremos en la imagen 3.6.



3.6

Paso 2: luego se nos abrirá una ventana para la configuración del SSTP cliente, vamos a la Pestaña Dial Out allí nos aparecerá todos los campos para configurar los siguientes campos Connect to: Dirección IP del server SSTP, Port: puerto por donde saldrá la comunicación User: usuario cliente, Password: password cliente, luego Permitimos solamente Mschap2, ver imagen 3.7.



Interface <sstp-out1>

General Dial Out Status Traffic

Connect To: 167.99.163.161

Port: 443

Proxy: [dropdown]

Proxy Port: 443

Certificate: none

TLS Version: any

Verify Server Certificate

Verify Server Address From Certificate

PFS

User: Curso

Password: Curso!123!.\$

Profile: default-encryption

Keepalive Timeout: 60

Dial On Demand

Add Default Route

Default Route Distance: 1

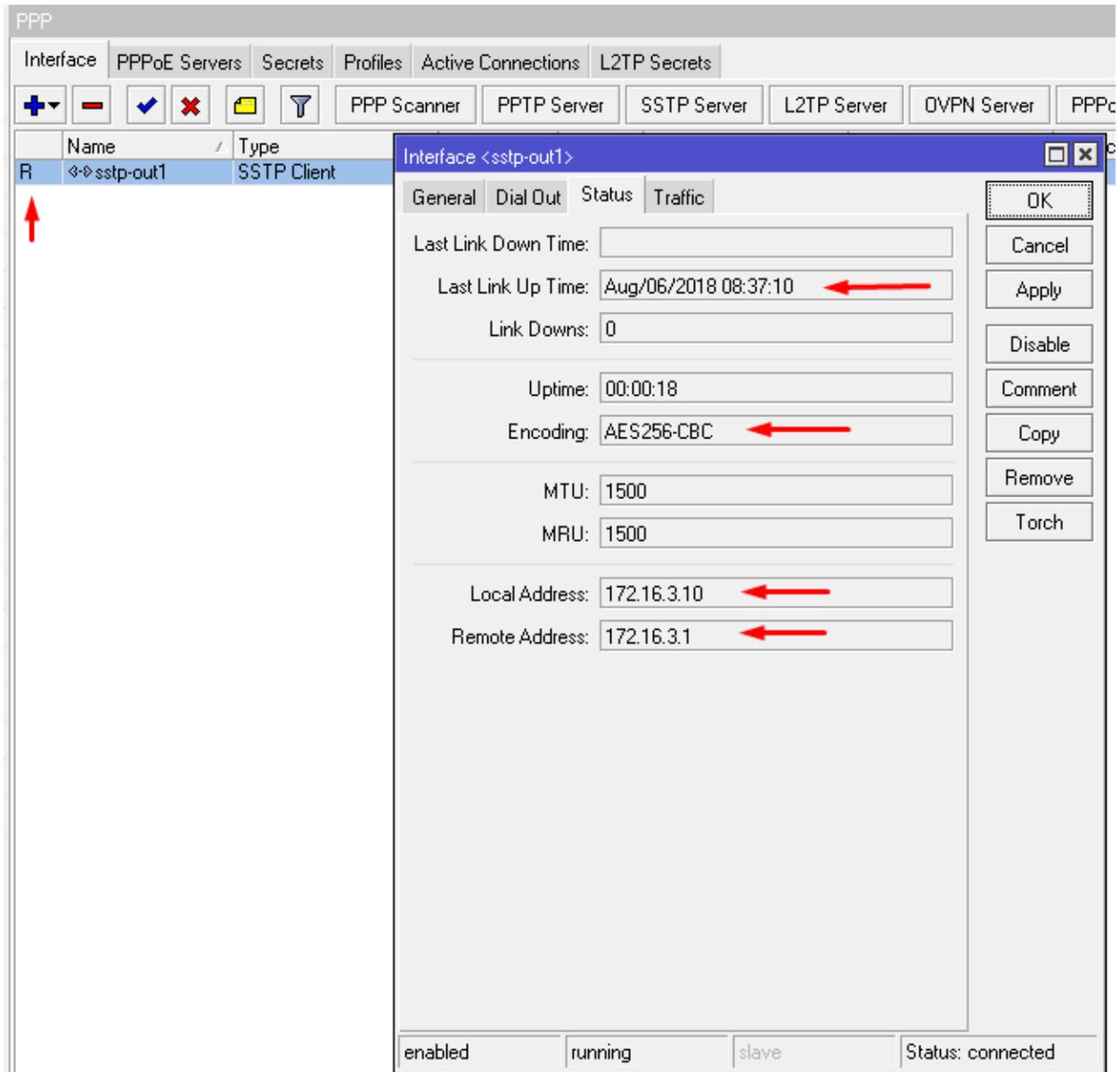
Allow: mschap2 mschap1
 chap pap

disabled running slave Status: disabled

OK
Cancel
Apply
Enable
Comment
Copy
Remove
Torch

3.7

Paso 3: en este paso veremos cómo se estableció nuestro túnel y la información que este nos provee de dicha conexión: En qué tiempo se levanto el túnel, el tiempo que tiene trabajando sin fallas, la encriptación del túnel que en este caso será AES256 por ultimo el Local address: que es su IP dinámica otorgada por el server SSTP y Remote Address: que es la IP del server SSTP. Ver imagen 3.8.



PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections | L2TP Secrets

PPP Scanner | PPTP Server | SSTP Server | L2TP Server | OVPN Server | PPPoE

Name	Type
R sstp-out1	SSTP Client

Interface <sstp-out1>

General | Dial Out | Status | Traffic

Last Link Down Time:

Last Link Up Time: Aug/06/2018 08:37:10

Link Downs: 0

Uptime: 00:00:18

Encoding: AES256-CBC

MTU: 1500

MRU: 1500

Local Address: 172.16.3.10

Remote Address: 172.16.3.1

enabled | running | slave | Status: connected

3.8