

MTCNA módulo 9 Túneles

1

MikroTik

07 | Túneles



- El protocolo PPP (Point-to-Point Protocol) es usado para establecer un túnel (conexión directa) entre dos nodos
- PPP proporciona: autenticación de la conexión, encriptación y compresión
- RouterOS soporta varios tipos de túneles como PPPoE, SSTP, PPTP y .. otros

- Es un PPP sobre Ethernet, es decir, es un protocolo de **Capa 2**.
Se utiliza para controlar el acceso a la red
- Proporciona autenticación, encriptación y compresión
- PPPoE se puede usar para distribuir direcciones IP a los clientes

- La mayoría de los sistemas operativos tiene un cliente PPPoE instalado por defecto
- RouterOS soporta tanto el cliente como el servidor PPPoE

- Si hay mas de un servidor PPPoE en el dominio de broadcast, también se debe especificar el servicio
- En caso contrario el cliente conectará con el primer servidor de PPPoE que le responda

- Define un rango de direcciones para distribuir por los servicios del RouterOS
- Es utilizado por los clientes de DHCP, PPP y HotSpot
- Las direcciones se obtienen automáticamente del pool

- Profile define las reglas usadas por los servidores PPP para sus clientes
- Es un método para establecer la misma configuración en muchos clientes

MTCNA módulo 9 PPP Profile

8



PPP

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

Name	Local Address	Remote Address	Bridge	Rate Limit (rx/tx)	Only One
default					default
default-encryption					default

New PPP Profile

General | Protocols | Limits | Queue | Scripts

Name: profile1

Local Address: 192.168.200.1

Remote Address: ppp_pool

Bridge: ppp_pool

Bridge Port Priority:

Incoming Filter:

Outgoing Filter:

Address List:

DNS Server:

WINS Server:

Change TCP MSS

Use UPnP

OK Cancel Apply Comment Copy Remove

New PPP Profile

General | Protocols | Limits | Queue | Scripts

Use MPLS

Use Compression

Use Encryption

OK Cancel Apply Comment Copy Remove

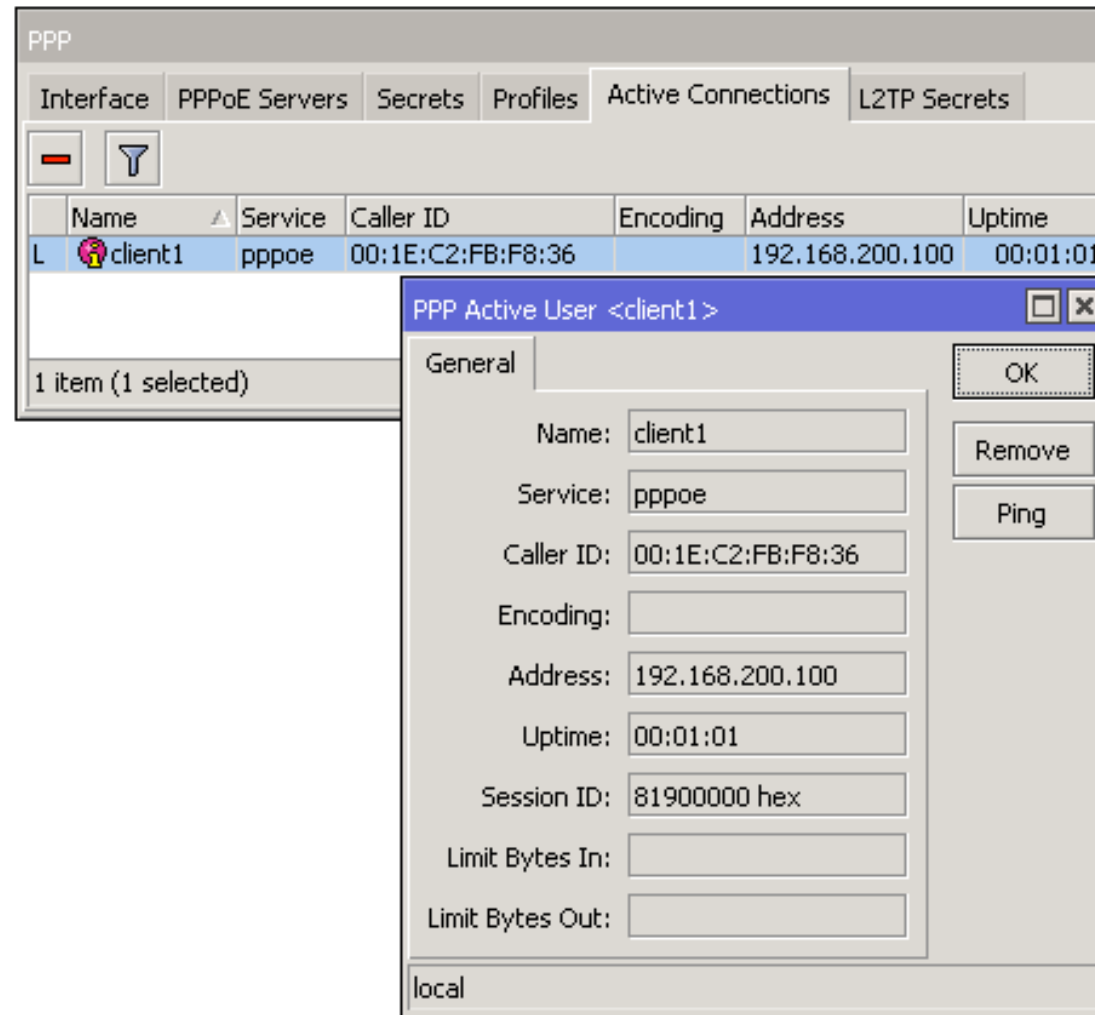
Establecer la dirección local y la remota del tunel

Es aconsejable el utilizar encriptación

- Base de datos local de usuarios PPP
- Se pueden configurar el nombre de usuario, la contraseña y otras características específicas del usuario
- El resto de características se aplican desde el perfil PPP seleccionado
- Los secretos PPP anulan las correspondientes características del perfil

- El servidor de PPPoE se ejecuta sobre un interfaz
- No se puede configurar en un interfaz que forma parte de un bridge
- O bien eliminamos el bridge, o bien definimos el servidor de PPPoE sobre el interfaz del bridge
- Por razones de seguridad no debemos utilizar direcciones IP en el interfaz que configuramos el servidor PPPoE

- Nos ofrece información acerca de los usuarios PPP activos



PPP

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

	Name	Service	Caller ID	Encoding	Address	Uptime
L	client1	pppoe	00:1E:C2:FB:F8:36		192.168.200.100	00:01:01

1 item (1 selected)

PPP Active User <client1>

General

Name: client1

Service: pppoe

Caller ID: 00:1E:C2:FB:F8:36

Encoding:

Address: 192.168.200.100

Uptime: 00:01:01

Session ID: 81900000 hex

Limit Bytes In:

Limit Bytes Out:

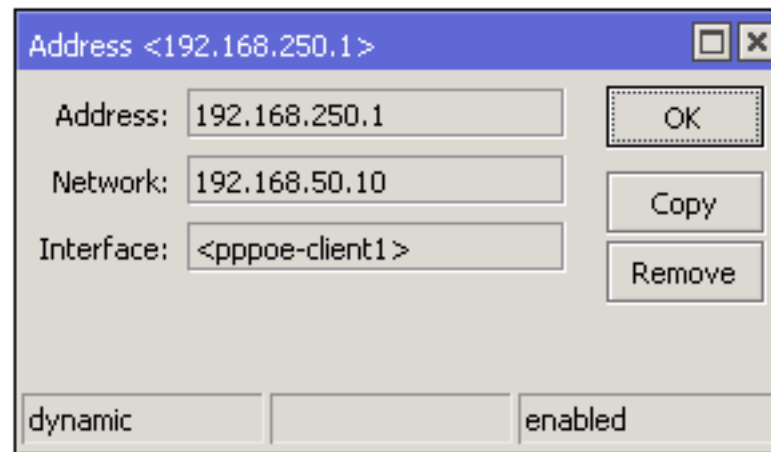
OK

Remove

Ping

local

- Cuando se establece una conexión entre un cliente y un servidor, se asigna una direcciónes /32
- Desde el punto de vista del cliente, su dirección de red (o gateway) es el otro extremo del túnel (router)



Address <192.168.250.1>

Address: 192.168.250.1

Network: 192.168.50.10

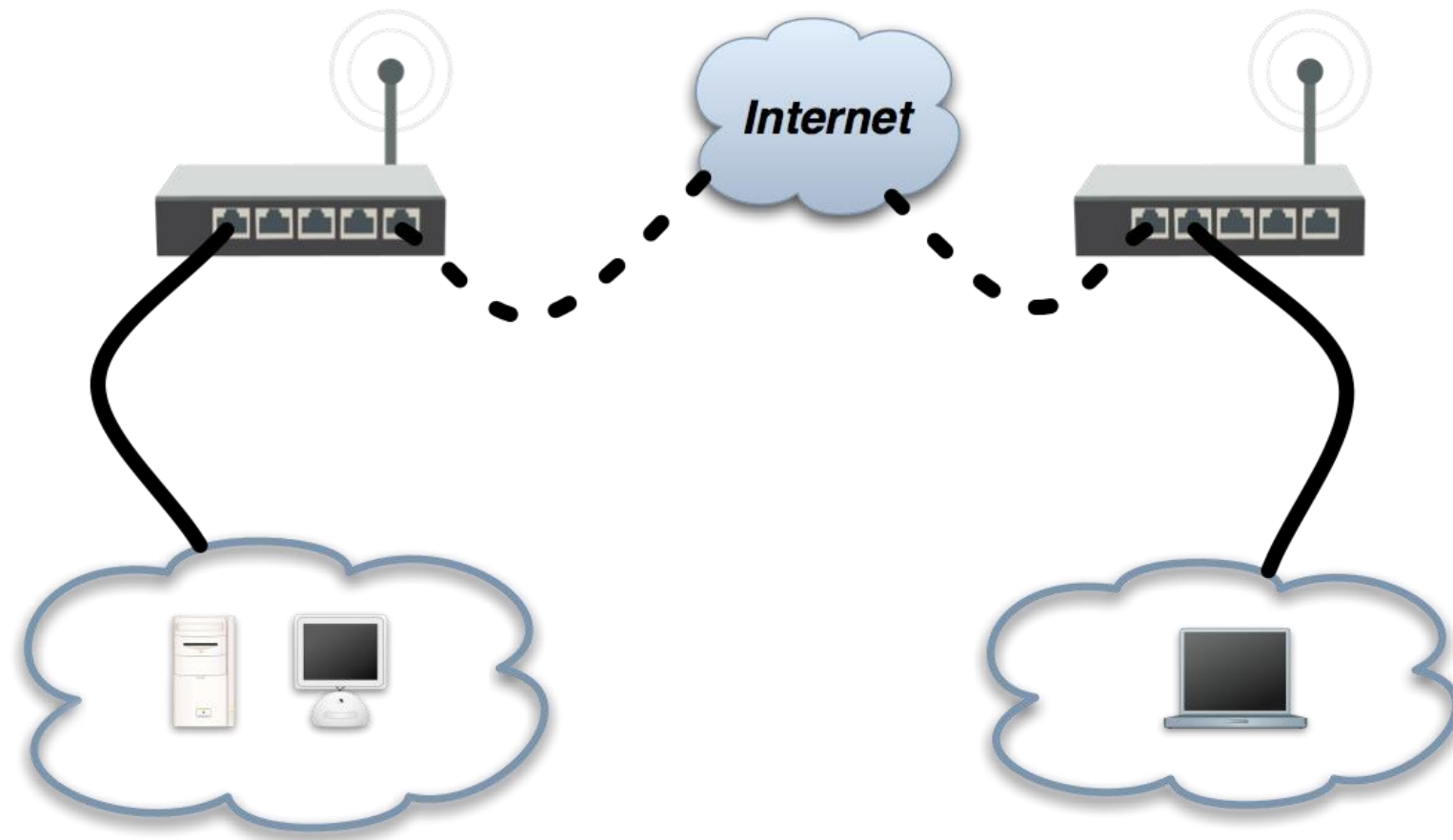
Interface: <pppoe-client1>

dynamic enabled

- La mascara de subred no es relevante cuando se utiliza direccionamiento PPP
- El direccionamiento PPP ahorra 2 direcciones IP
- Si el otro dispositivo no soporta el direccionamiento PPP, se debe utilizar un direccionamiento /30

- PPTP (Point-to-Point Tunneling Protocol) proporciona tuneles encriptados sobre IP
- Se pueden utilizar para crear conexiones seguras entre redes locales sobre internet
- RouterOS soporta ambos tipos: cliente y servidor

- Utiliza el puerto tcp 1723 y el protocolo IP número 47 (GRE – Generic Routing Encapsulation)
- Se usan NAT helpers para soportar PPTP en redes NATeadas



- Utilizar *'Add Default Route'* para enviar todo el tráfico a través de un túnel PPTP
- Utilizar rutas estáticas para enviar tráfico específico a través de un túnel PPTP
- **¡ Atención !** PPTP ya no se considera seguro, utilizarlo con precaución.
- En su lugar utilizar L2tp con Ipsec, SSTP, OpenVPN u otros

- SSTP (Secured Socket Tunnelling Protocol) proporciona un tunel encriptado sobre IP
- Utiliza el puerto tcp 443 (el mismo que el HTTPS)
- RouterOS soporta tanto el cliente como el servidor
- SSTP está disponible a partir de windows vista 7 SP1

- En linux existe una versión Open Source del cliente y del servidor
- Cómo es identico al tráfico de HTTPS, normalmente SSTP puede pasar a través de los firewall sin ningún tipo de configuración específica

- Utilizar *'Add Default Route'* para enviar todo el tráfico a través de un túnel SSTP
- Utilizar rutas estáticas para enviar tráfico específico a través de un túnel SSTP

- NO es necesario un certificado SSL para conectar dos dispositivos mikrotik
- Para conectar desde windows, es necesario un certificado válido
- Se puede generar mediante una CA interna