# *MUM – Mexico 2019*

# VPN Multisite

Por: Carlo Mata

# Introducción

Los túneles VPN además de seguridad nos permiten la conectividad de redes remotas.

A continuación veremos un caso de éxito, se establecieron 515 túneles VPN utilizando enlaces de Internet LTE

# Objetivos

- ✓ Explicar qué es VPN
- ✓ Aprender a configurar una VPN Punto a Punto
- ✓ Demostración de VPN Punto a Multipunto.

# Programa

- Conceptos de VPN
- Escenario de implementación
- **Implementación:** *VPN Multisite*

# Acerca de la empresa

Somos una empresa que se dedica a la **implementación de proyectos** integrando principalmente equipos de la marca MikroTik, si es necesario combinados con otras marcas.

***Contáctenos***

contacto@xlink.com.mx

# Agradecimientos

***José Miguel Cabrera*** – *Ecatel*

*> Capacitación*

*> Asesoría*

***Eliud Zarate Castillo***


¿Quieres información de los cursos?

***https://ecatel.com.mx/formmx***

# Acerca del Expositor


- **Nombre:** Carlo Manuel Mata Ureña

**Experiencia Laboral:**

- Gerente de Proyectos en Xlink Networks (2015 a la fecha)
- Consultor de Mikrotik (2017 a la fecha)



# Programa

- **Conceptos de VPN**
- Escenario de implementación
- **Implementación:** *VPN Multisite*

# ¿Qué es VPN?

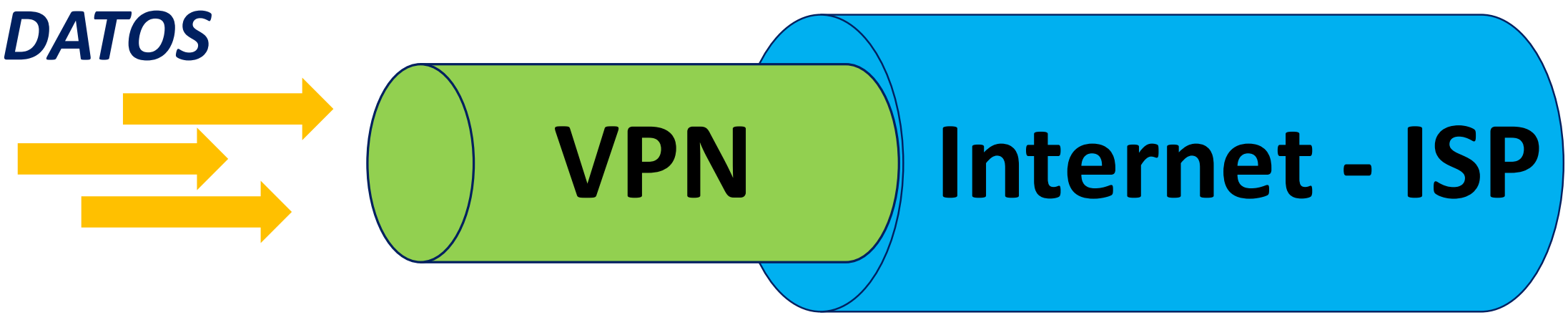
## Virtual Privacy Network

Hay muchas formas de explicarlo. En lo personal, la forma más sencilla es decir que es una red dentro de otra red.

Permite crear un canal o tubo dentro de una red ya existente, en este tubo privado creado por uno mismo, tenemos el control de los datos que pasa por él.

# ¿Qué es VPN?

## Virtual Privacy Network




Si, como se observa en la imagen. Perderás un poco de capacidad al hacer VPN

# ¿Para que sirve un túnel?

Suele utilizarse para transportar un protocolo determinado a través de una red que, en condiciones normales, no lo aceptaría.

Además **puede proveer**: Autenticación, Encriptación y Compresión.

# ¿Para que sirve un túnel?

Hoy día, el uso típico es utilizar VPN para enrutar una red privada LAN a través de Internet (red WAN)

# Tipos de VPN

- Ipsec – tunnel and transport mode, certificate or PSK
- Point to point tunneling

  (OpenVPN, PPTP, PPPoE, L2TP, SSTP)
- Simple tunnels (IPIP, EoIP) IPv4 and IPv6 support
- 6to4 tunnel support (IPv6 over IPv4 network)

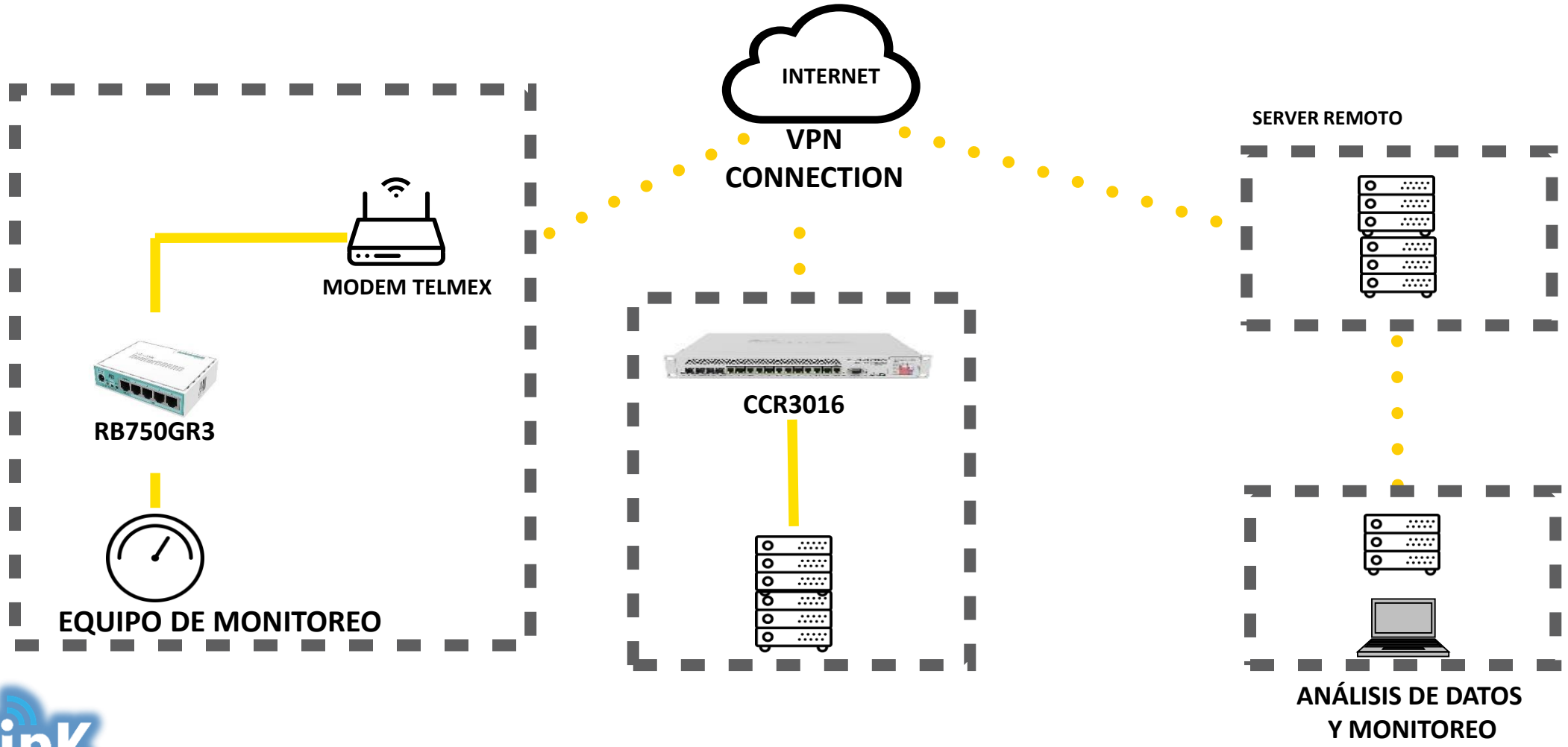
# Point-to-Point Protocol

- Usado para establecer un túnel (conexión directa) entre dos nodos
- PPP puede proveer autenticación, encriptación y compresión
- RouterOS soporta: PPoE, SSTP, PPtP y otros

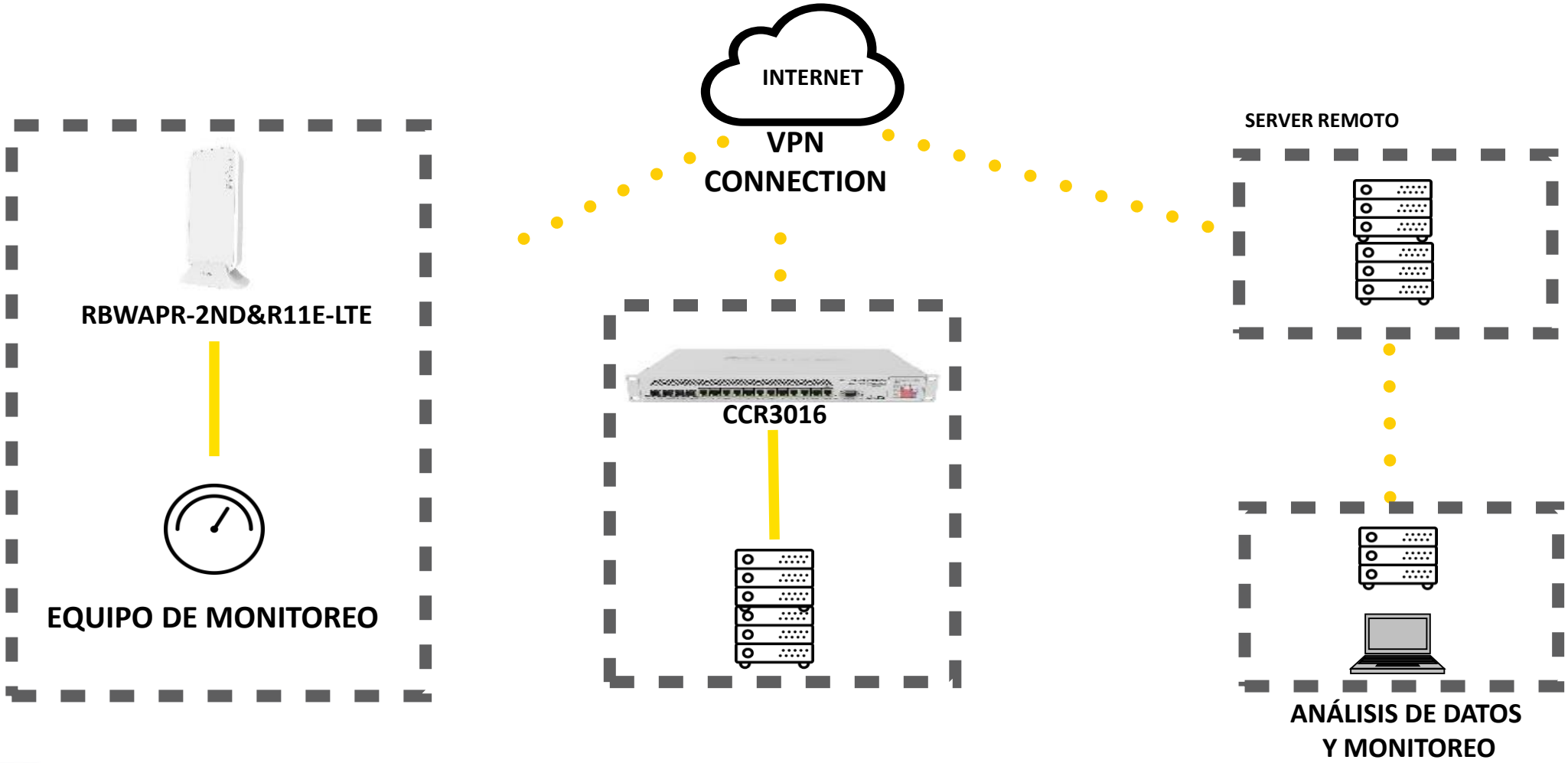
# Programa

- Conceptos de VPN
- **Escenario de implementación**
- **Implementación:** *VPN Multisite*

# Diagrama de Comunicación



# Diagrama de Comunicación



# Equipos Implementados

## RBwAPR-2nD&R11e-LTE


| | |
|---|---|
| 10/100 Ethernet ports | 1 |
| Antenna gain dBi for 2.4 GHz | 2 |
| CPU | QCA9531 |
| CPU core count | 1 |
| CPU nominal frequency | 650 MHz |
| DC jack input Voltage | 9-30 V |
| Dimensions | 185 x 85 x 30 mm |
| LTE Category | 4 (150Mbps Downlink, 50Mbps Uplink) |
| LTE FDD bands | 1 (2100MHz) / 2 (1900MHz) / 3 (1800MHz) / 7 (2600MHz) / 8 (900 MHz) / 20 (800MHz) |
| LTE TDD bands | 38 (2600MHz) / 40 (2300MHz) |
| License level | 4 |
| Max power consumption | 8 W |
| MiniPCI-e slots | 1 |
| PoE in | Passive PoE |
| PoE in input Voltage | 9-30 V |

# Equipos Implementados

## RB912R-2nD-LTm&R11e-LTE


| | |
|---|---|
| 10/100 Ethernet ports | 1 |
| Antenna gain dBi for 2.4 GHz | 2 |
| CPU | QCA9531 |
| CPU core count | 1 |
| CPU nominal frequency | 650 MHz |
| DC jack input Voltage | 8-30 V |
| Dimensions | 139 x 77 x 28,5 mm |
| LTE Category | 4 (150Mbps Downlink, 50Mbps Uplink) |
| LTE FDD bands | 1 (2100MHz) / 2 (1900MHz) / 3 (1800MHz) / 7 (2600MHz) / 8 (900 MHz) / 20 (800MHz) |
| LTE TDD bands | 38 (2600MHz) / 40 (2300MHz) |
| License level | 4 |
| Max power consumption | 9 W |
| MiniPCI-e slots | 1 |
| PoE in | 802.3af/at |
| PoE in input Voltage | 12-57 V |

# Equipos Implementados

**RB750GR3**

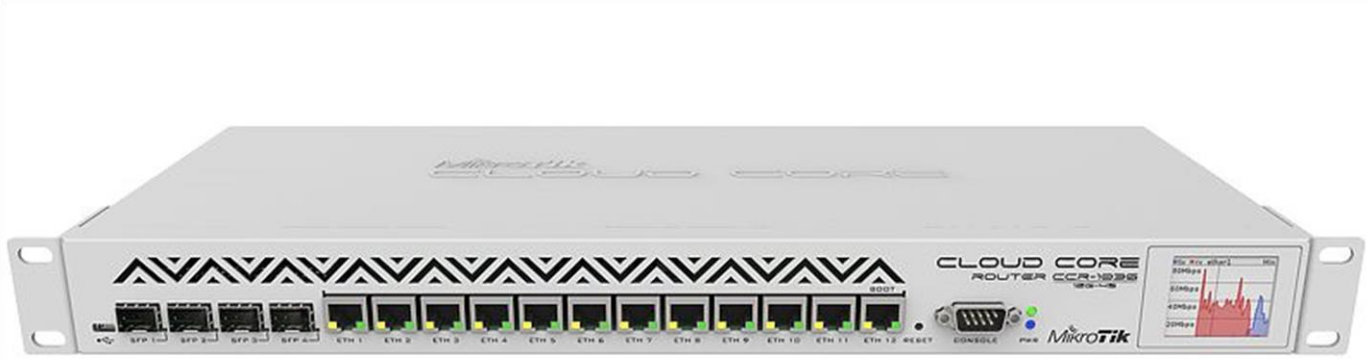

| | |
|---|---|
| 10/100/1000 Ethernet ports | 5 |
| Architecture | MMIPS |
| CPU | MT7621A |
| CPU core count | 2 |
| CPU nominal frequency | 880 MHz |
| DC jack input Voltage | 8-30 V |
| Dimensions | 113x89x28mm |
| Size of RAM | 256 MB |
| License level | 4 |
| Max power consumption | 10 W |
| PoE in | Passice PoE |
| PoE in input Voltage | 8-30 V |

# Equipos Implementados

## RBLHGR&R11e-LTE

| | |
|---|---|
| 10/100 Ethernet ports | 1 |
| CPU | QCA9531 |
| CPU core count | 1 |
| CPU nominal frequency | 650 MHz |
| DC jack input Voltage | 9-30 V |
| Dimensions | 391 x 391 x 227 mm |
| LTE Category | 4 (150Mbps Downlink, 50Mbps Uplink) |
| LTE FDD bands | 1 (2100MHz) / 2 (1900MHz) / 3 (1800MHz) / 7 (2600MHz) / 8 (900 MHz) / 20 (800MHz) |
| LTE TDD bands | 38 (2600MHz) / 40 (2300MHz) |
| License level | 3 |
| Max power consumption | 6 W |
| MiniPCI-e slots | 1 |
| PoE in | 802.3af/at |
| PoE in input Voltage | 12-57 V |

# Equipos Implementados




Dentro del CCR1036 se configuraron 515 secrets.

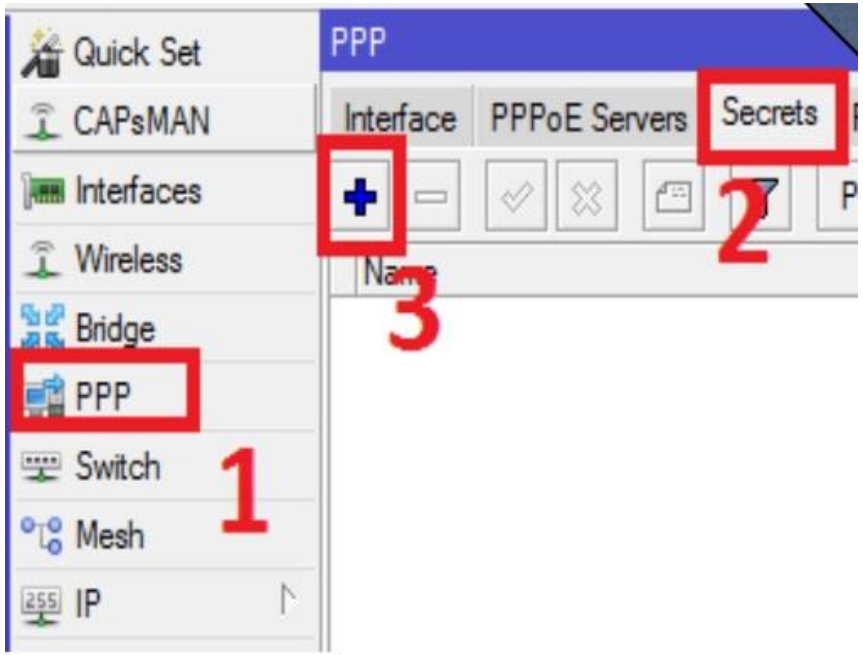
A cada una se le dio una dirección IP para enrutar la VPN

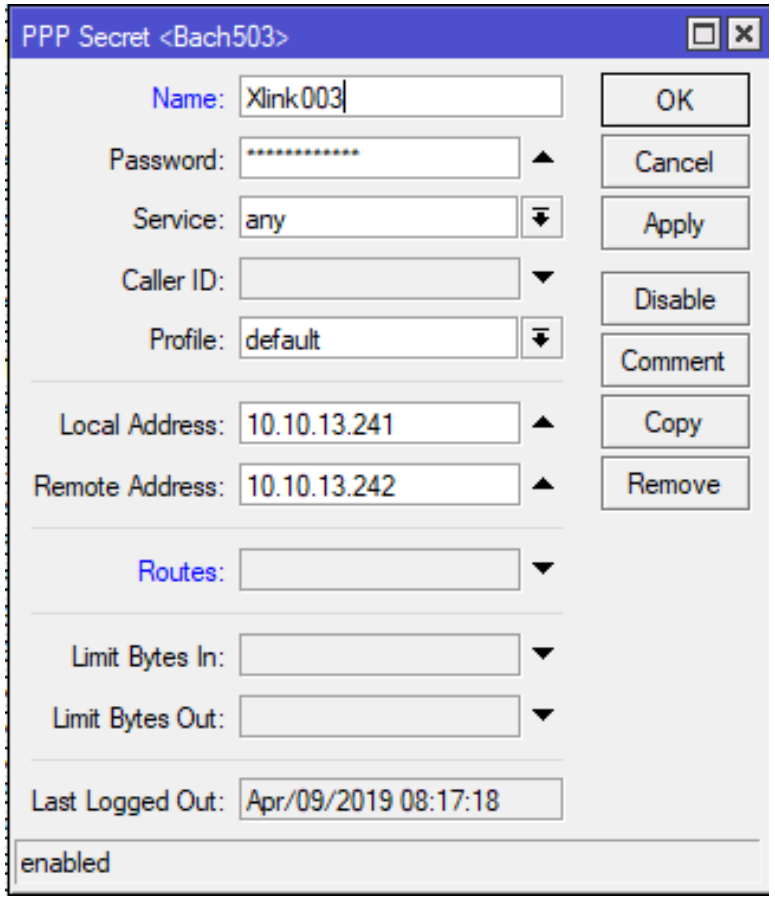
Y se declaro en primera instancia una ruta estatica para cada VPN

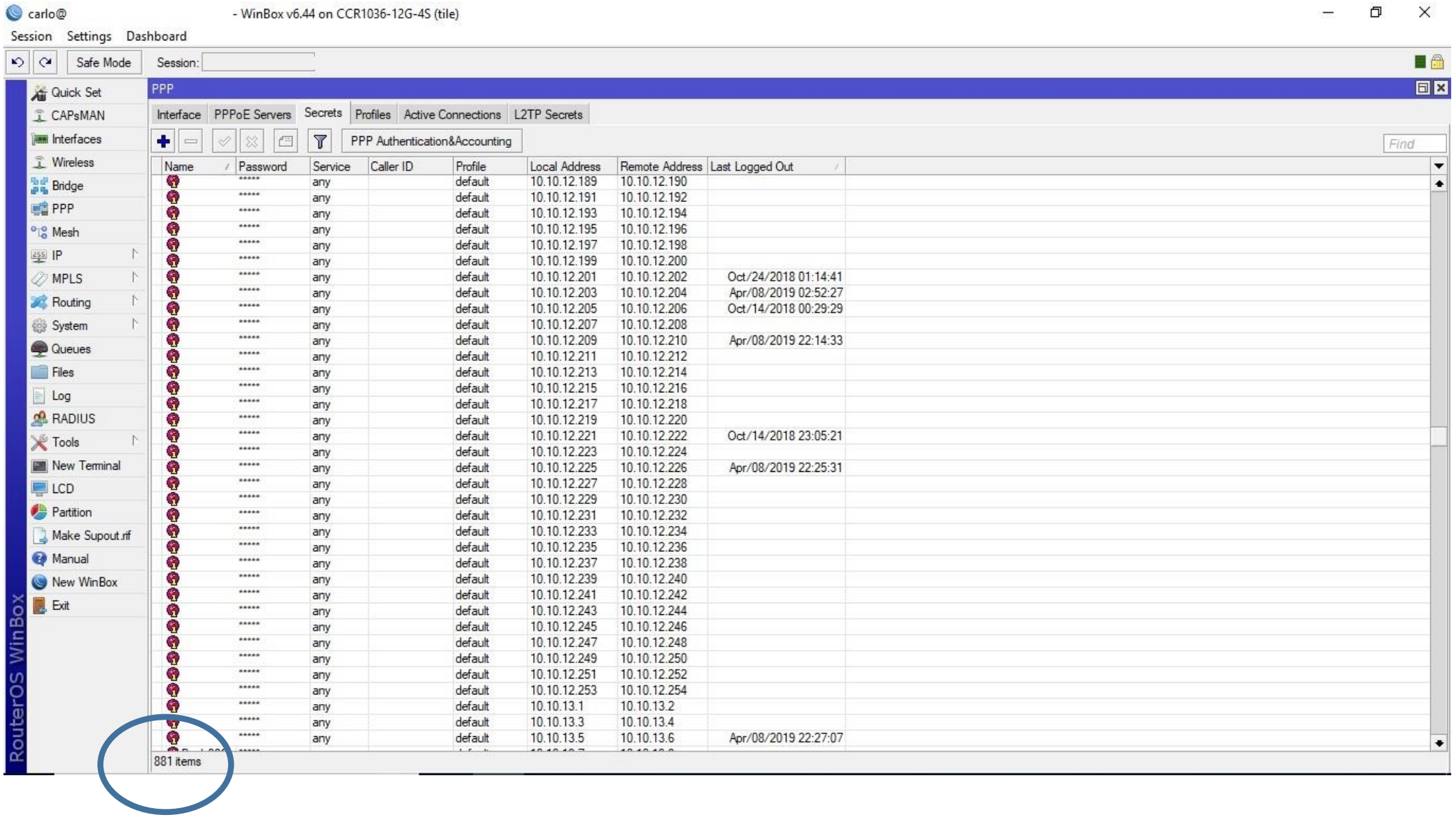
# Programa

- Conceptos de VPN
- Escenario de implementación
- **Implementación:** *VPN Multisite*

# Implementación

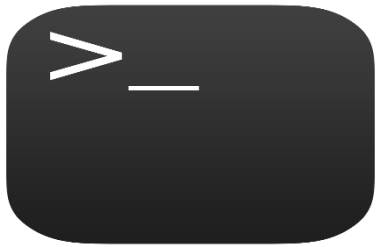


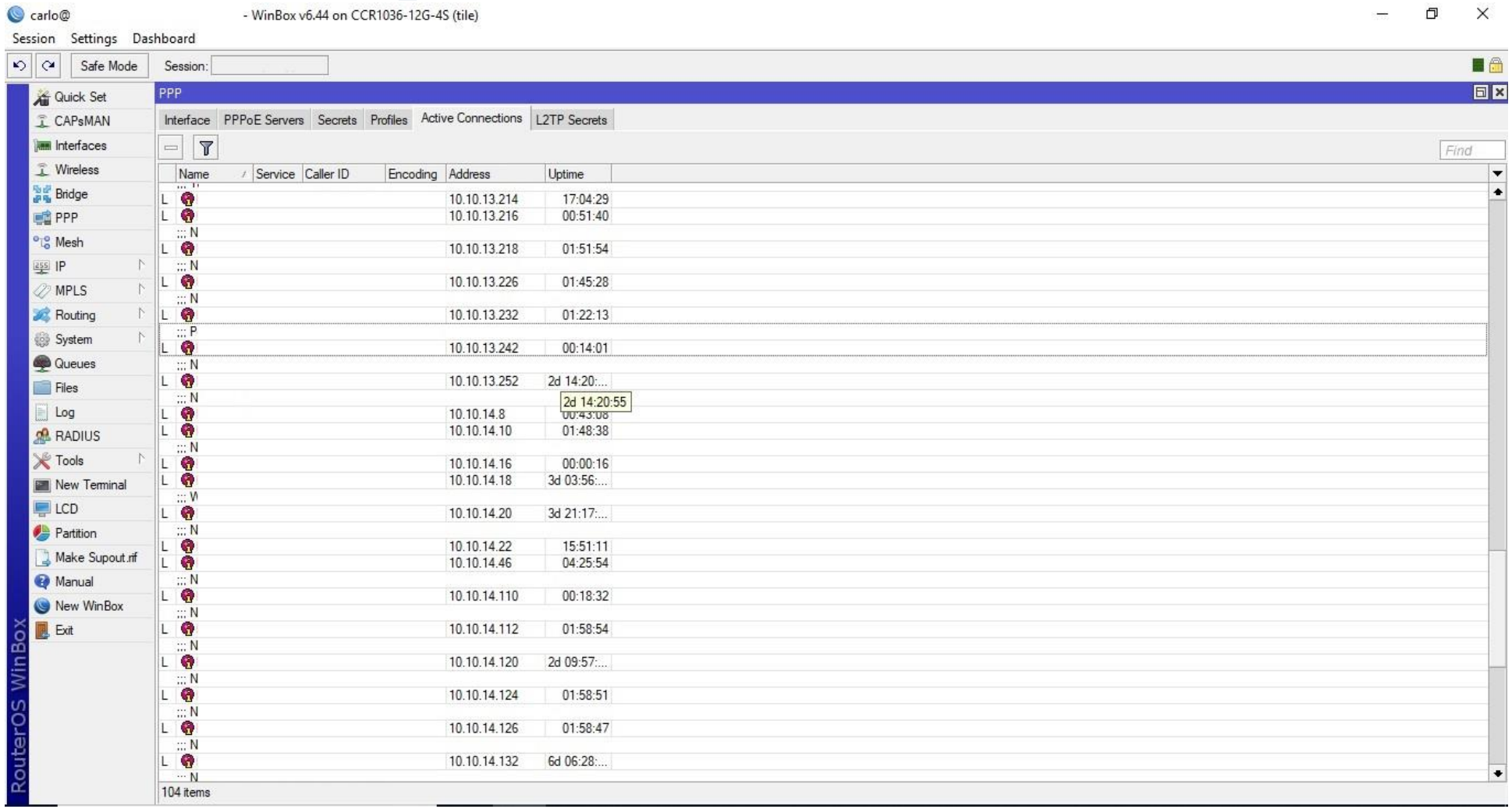

carlo@
- WinBox v6.44 on CCR1036-12G-4S (tile)
Session Settings Dashboard
Safe Mode
Session:
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
LCD
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
PPP
Interface
PPPoE Servers
Secrets
Profiles
Active Connections
L2TP Secrets
PPP Authentication&Accounting
Find
Name
Password
Service
Caller ID
Profile
Local Address
Remote Address
Last Logged Out
881 items

# Agregando Secrets por medio de Script

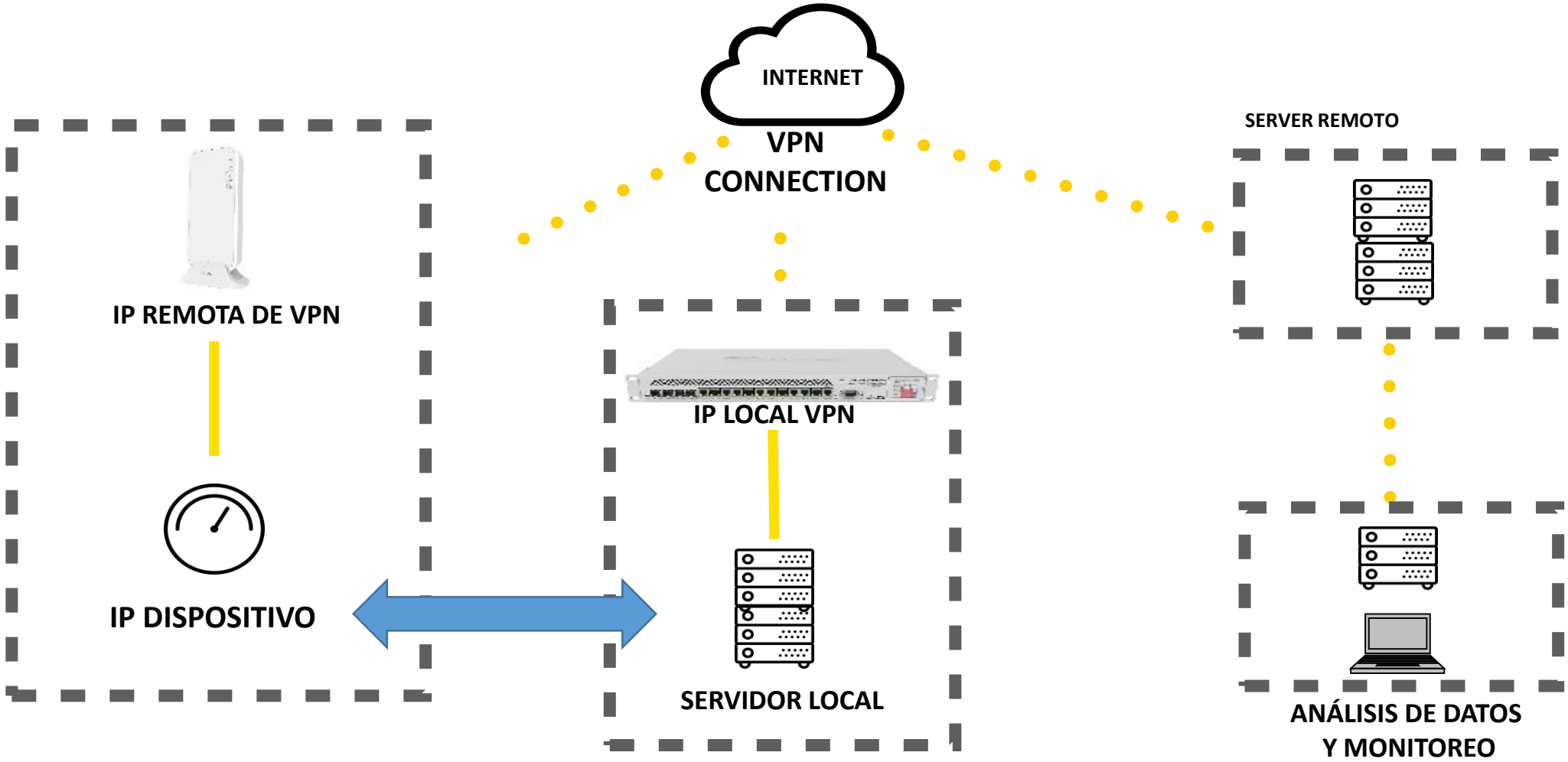
```
/ppp secret
add local-address=10.10.10.1 name=Xlink002 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.2
add local-address=10.10.10.3 name=Xlink003 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.4
add local-address=10.10.10.5 name=Xlink004 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.6
add local-address=10.10.10.7 name=Xlink005 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.8
add local-address=10.10.10.9 name=Xlink006 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.10
add local-address=10.10.10.11 name=Xlink007 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.12
add local-address=10.10.10.13 name=Xlink008 password=LaContraseñaQueQueremos \
    remote-address=10.10.10.14
```



# Implementación



# Diagrama de Comunicación

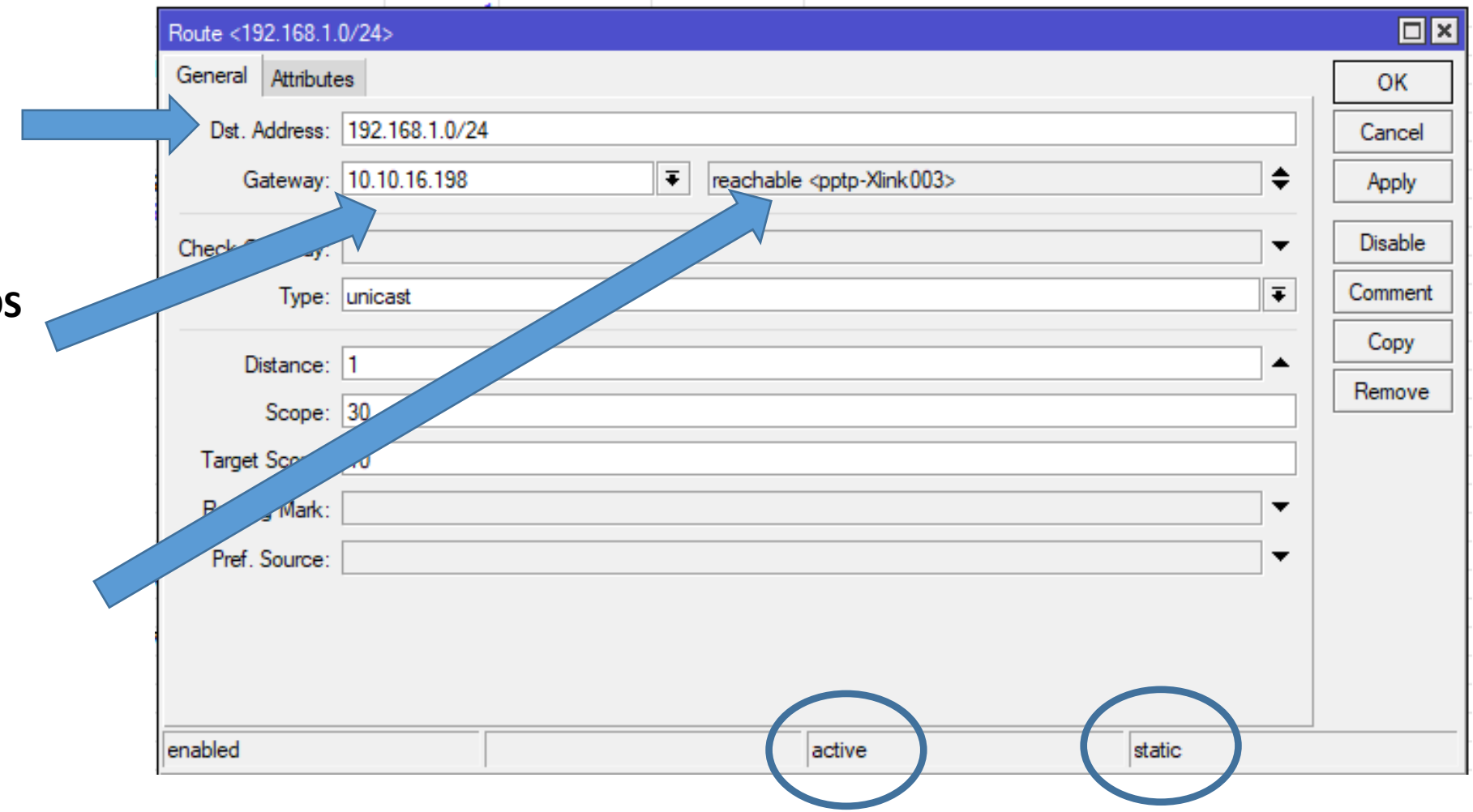


# Implementación de Rutas Estáticas

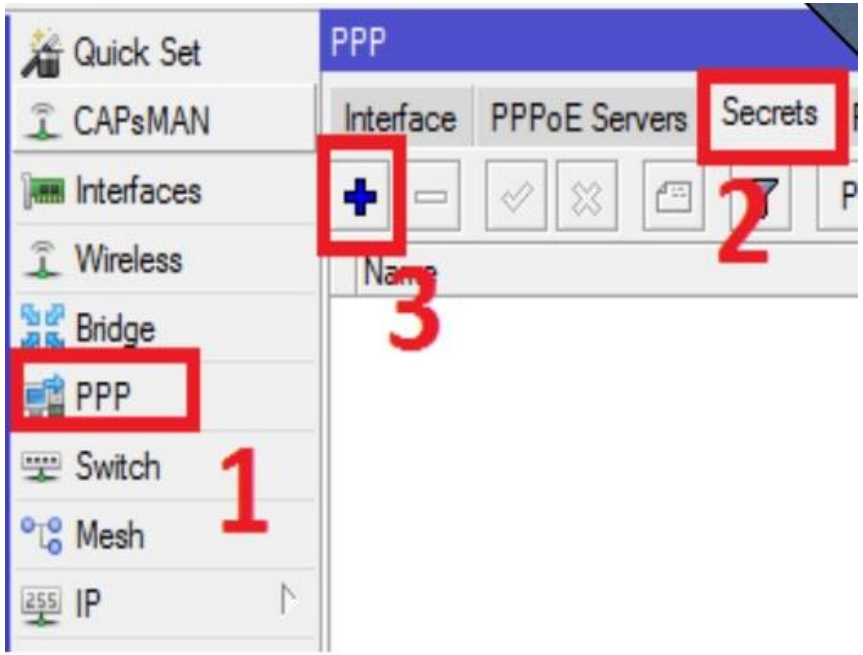
**IP LOCAL O SEGMENTO DEL DISPOSITIVO REMOTO A LA CUAL QUEREMOS TENER ACCESO**

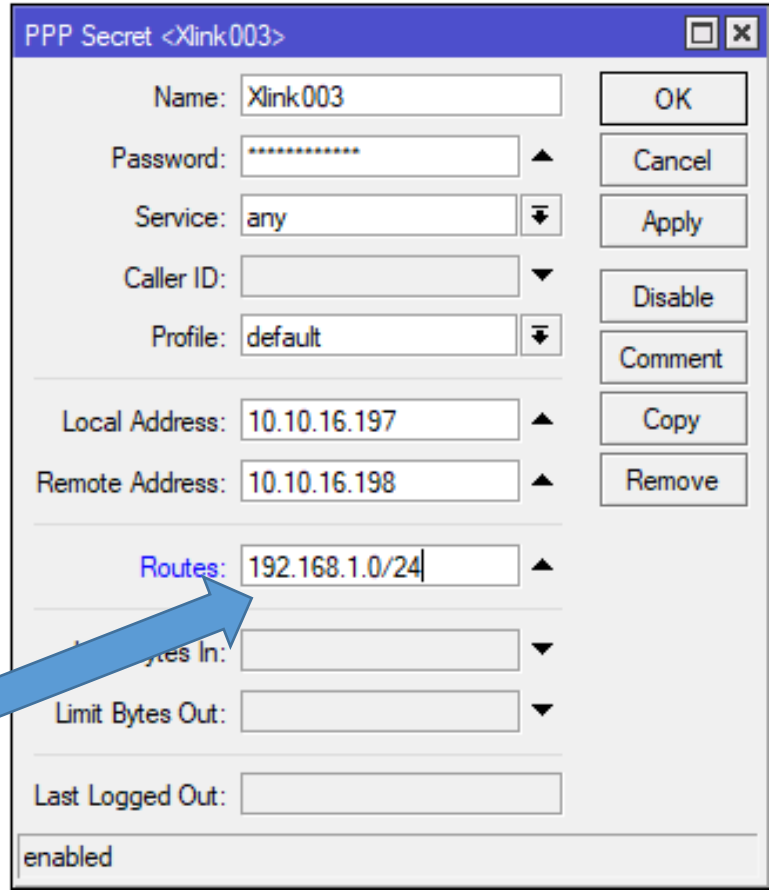
**IP REMOTE DECLARADA EN LOS SECRETS – AHORA NUESTRO GATEWAY PARA ALCANZAR EL DISPOSITIVO.**

**INTERFAZ POR LA CUAL ALCANZAREMOS NUESTRA IP DECLARADA**



# Implementación Ruta Dinámica



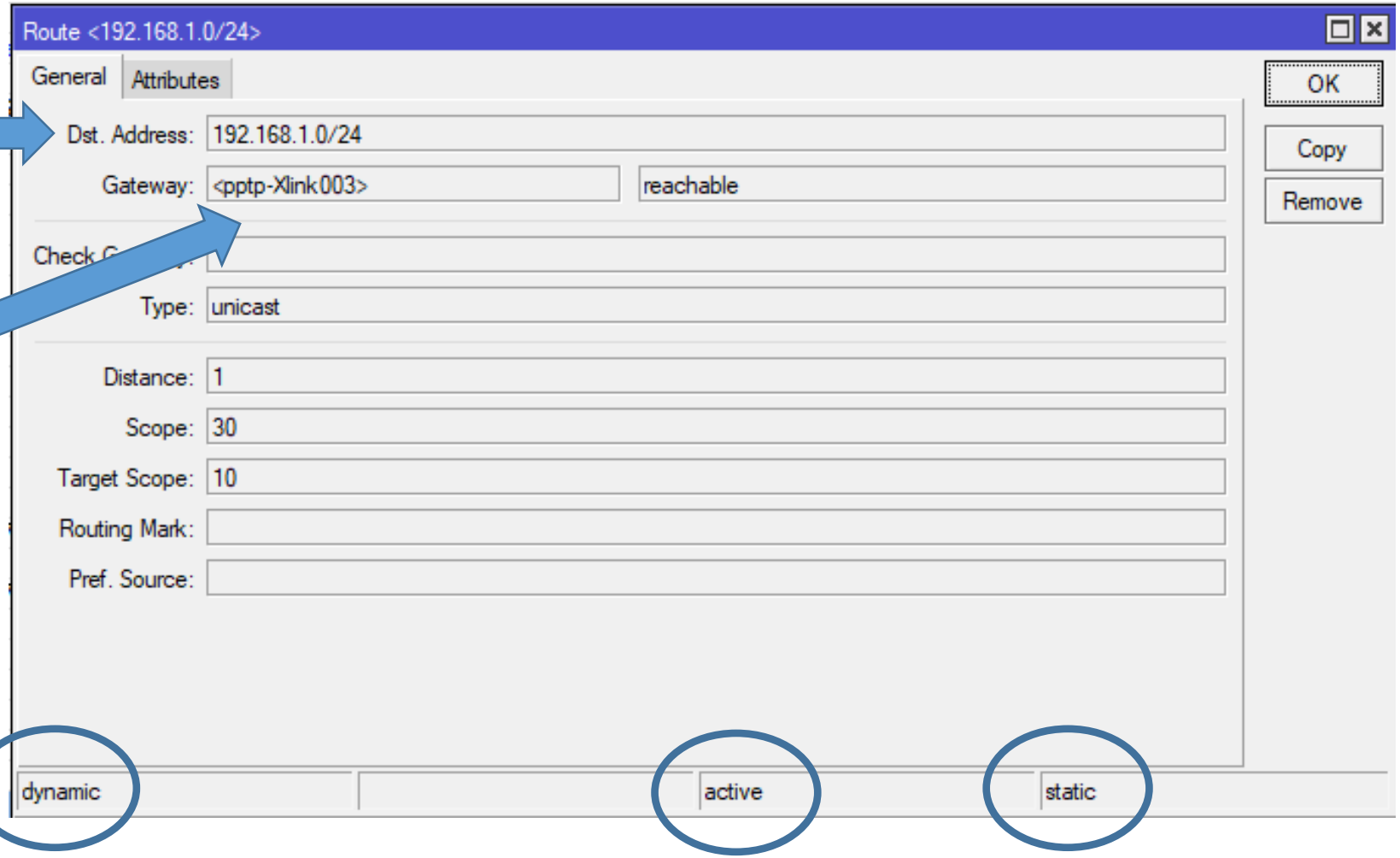

**DECLARACION DE IP O SEGMENTO AL CUAL QUEREMOS ALCANZAR POR MEDIO DE ESTE SECRET**

# Implementación de Rutas Dinámicas

**IP LOCAL O SEGMENTO DEL DISPOSITIVO REMOTO A LA CUAL QUEREMOS TENER ACCESO**

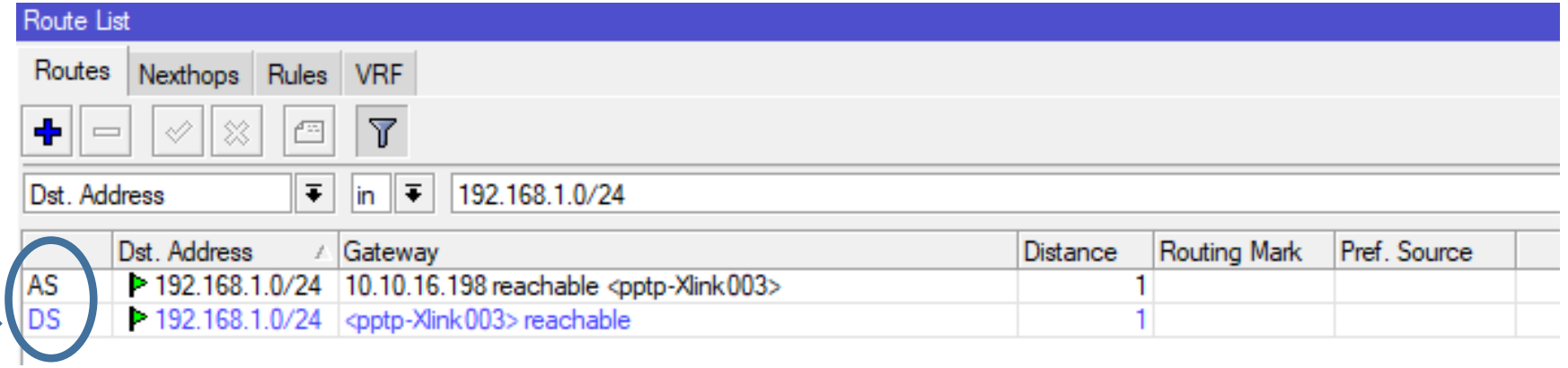
**YA NO ES NECESARIO DECLARAR UN GATEWAY, AL ESPECIFICAR EN EL SECRET SABE POR DONDE IRSE**

**AHORA NUESTRA RUTA ES DINÁMICA**



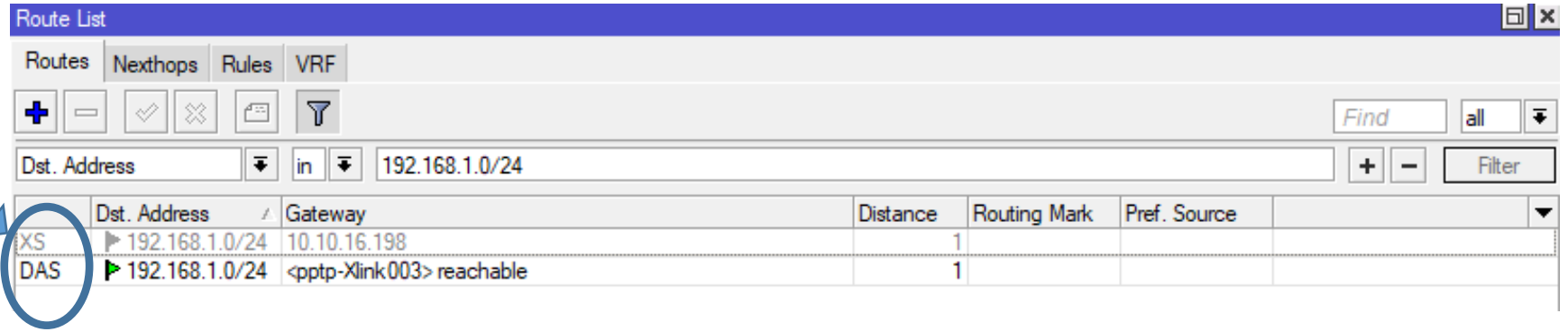
# Etiquetas de Rutas

AS = Ruta Estática Activa
DS = Ruta Estática Dinámica

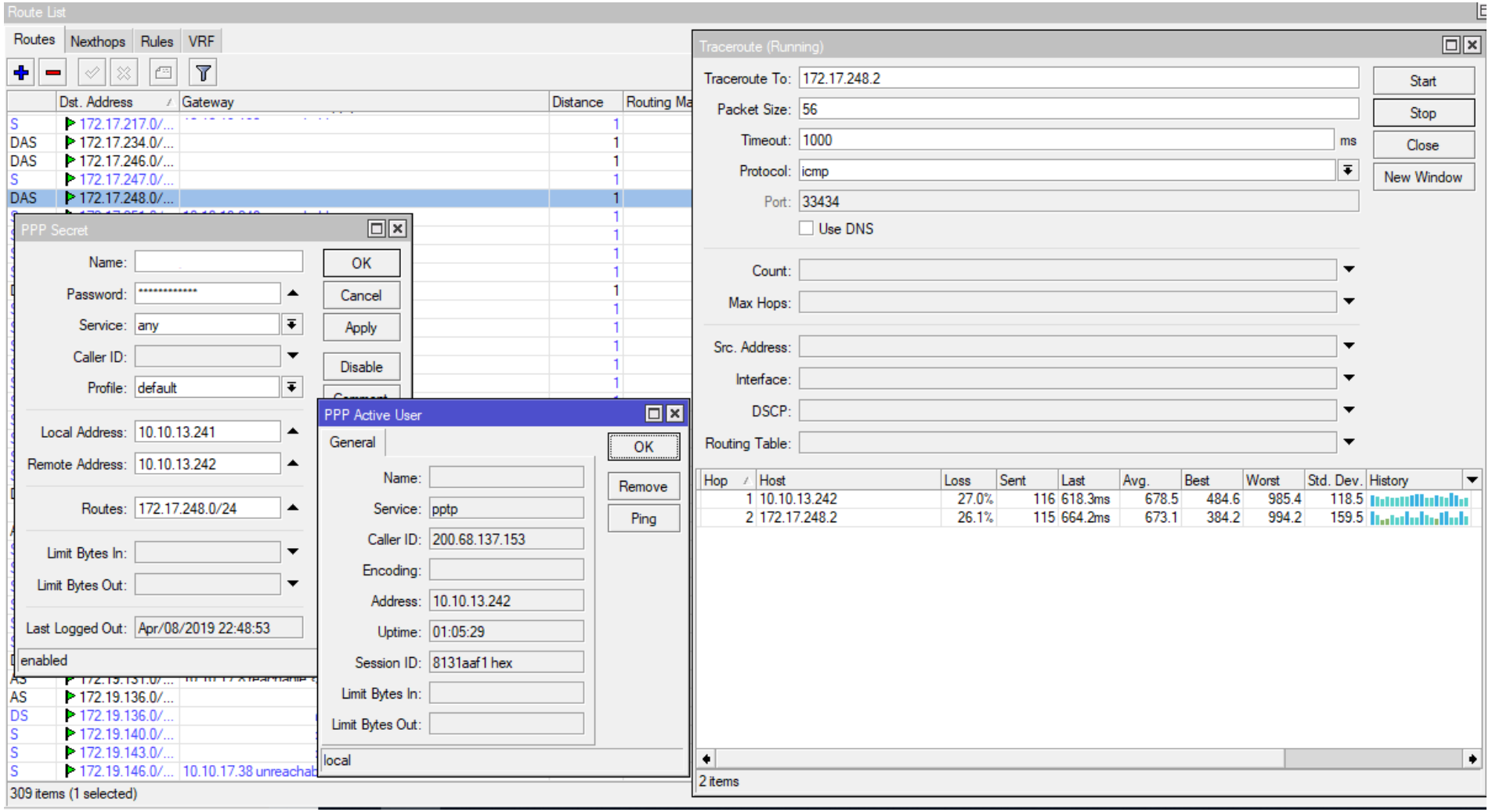



XS = Ruta Estática Desactivada

DSA = Ruta Estática Dinámica Activa

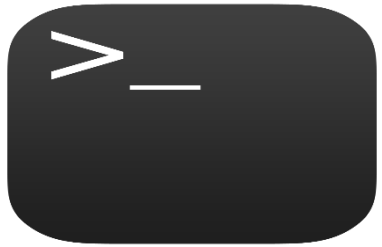


# Demostración

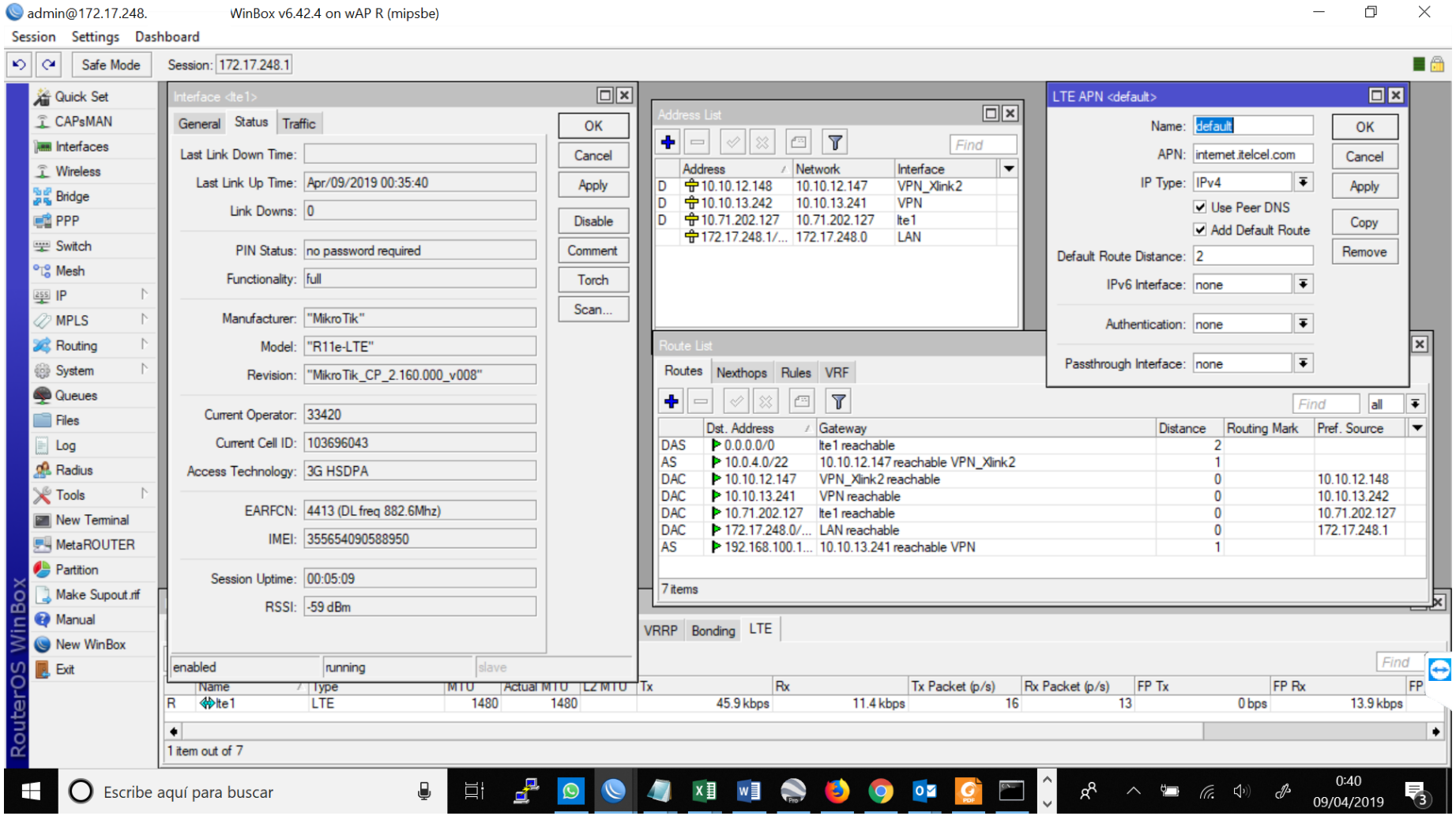


# Configuración LTE

```
/interface lte
set [ find ] add-default-route=yes apn=internet.itelcel.com authentication=\
    chap band=1,3,7,20,8,2,38,40 default-route-distance=1 mac-address=\
    AC:FF:FF:00:00:00 name=lte1 password=webgprs2002 use-peer-dns=yes user=\
    webgprs
/interface pptp-client
add connect-to=dominioalcualconectar disabled=no name=VPN \
    password=************ user=Xlink003
/ip address
add address=172.17.248.1/30 interface=ether1 network=172.17.248.0
/ip firewall nat
add action=masquerade chain=srcnat out-interface=lte1
/ip route
add distance=1 dst-address=192.168.100.0/24 gateway=10.10.16.197
/system identity
set name=Xlink003
```



# Winbox Equipo Remoto



# Implementaciones Físicas



# ¡Gracias!

## ¿DUDAS?

**Cel. 2293564126**

**carlomata@Xlink.com.mx**