

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

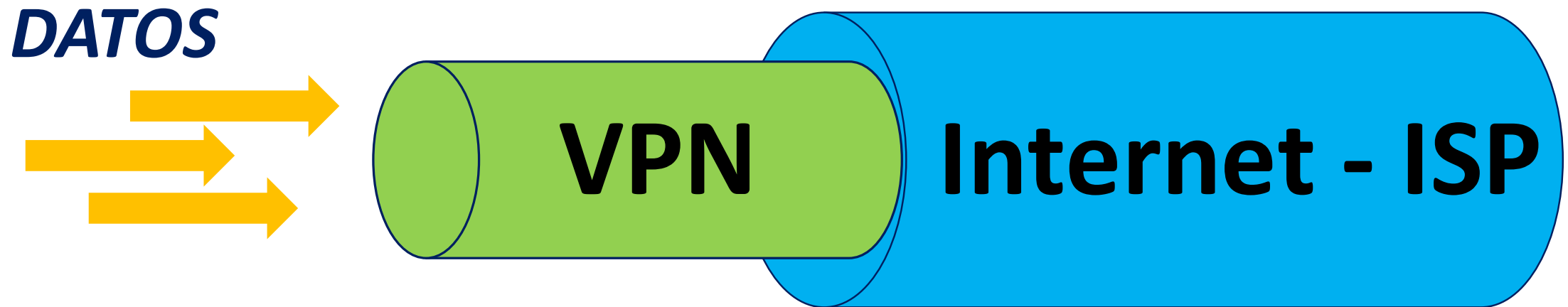
Hay muchas formas de explicarlo. En lo personal, la forma más sencilla es decir que es una red dentro de otra red.

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

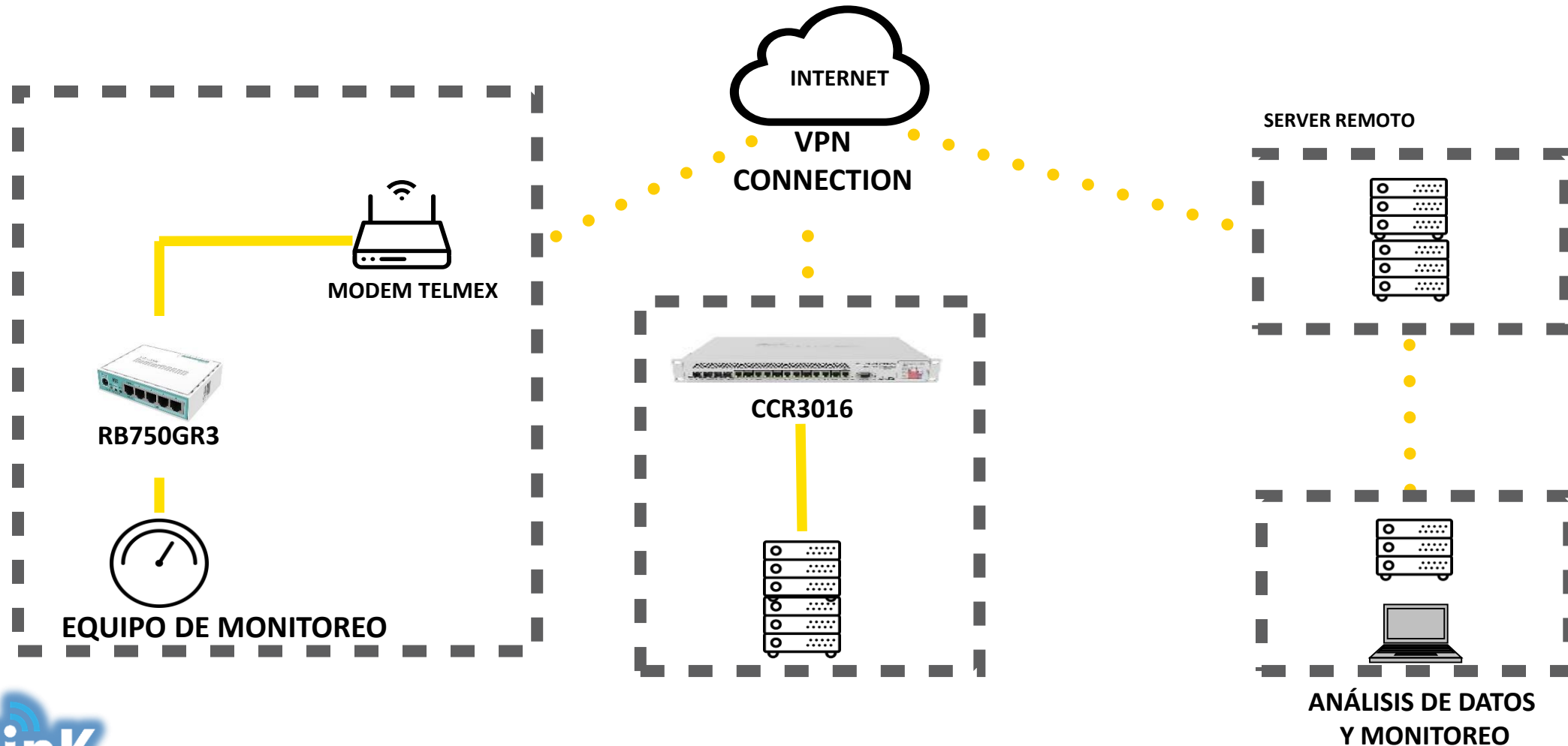
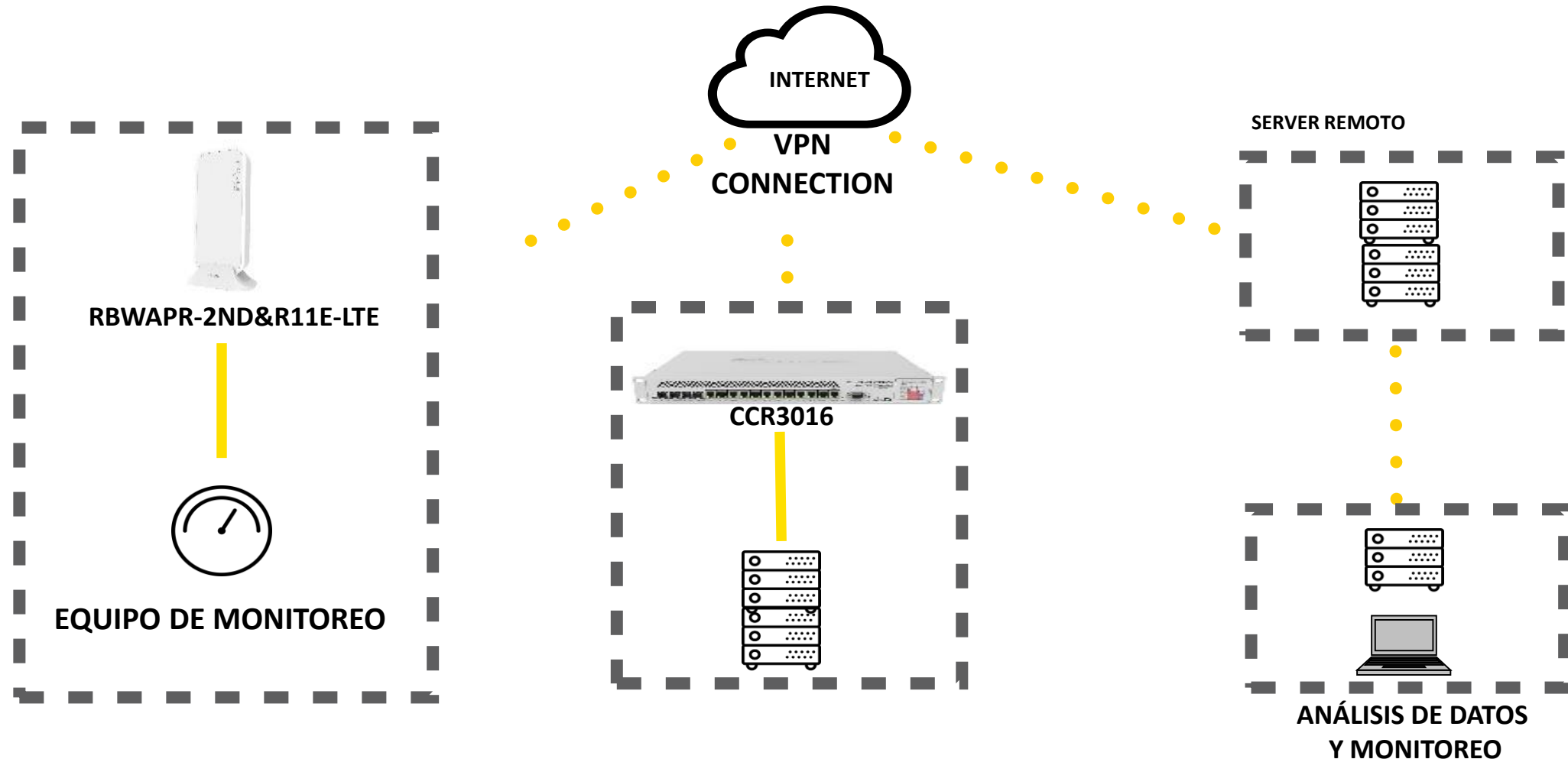


Diagrama de Comunicación



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	Passive PoE
PoE in input Voltage	8-30 V

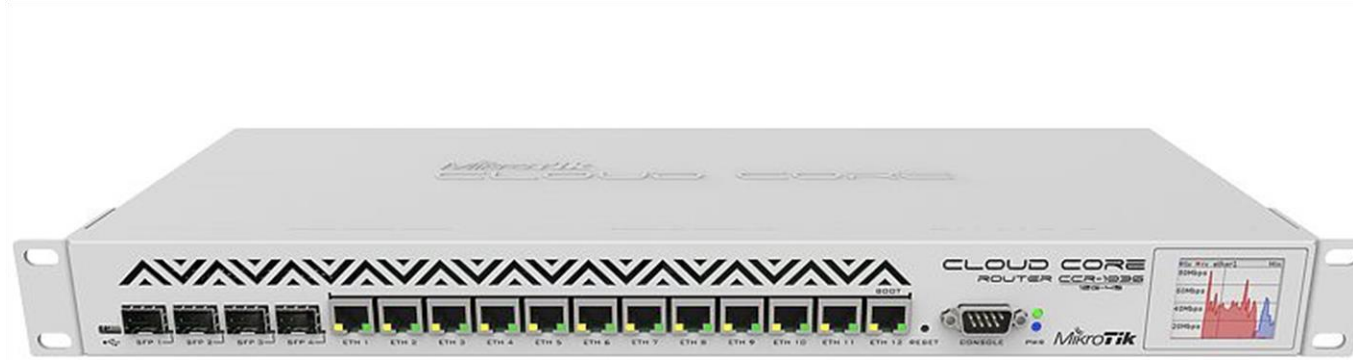
Equipos Implementados

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

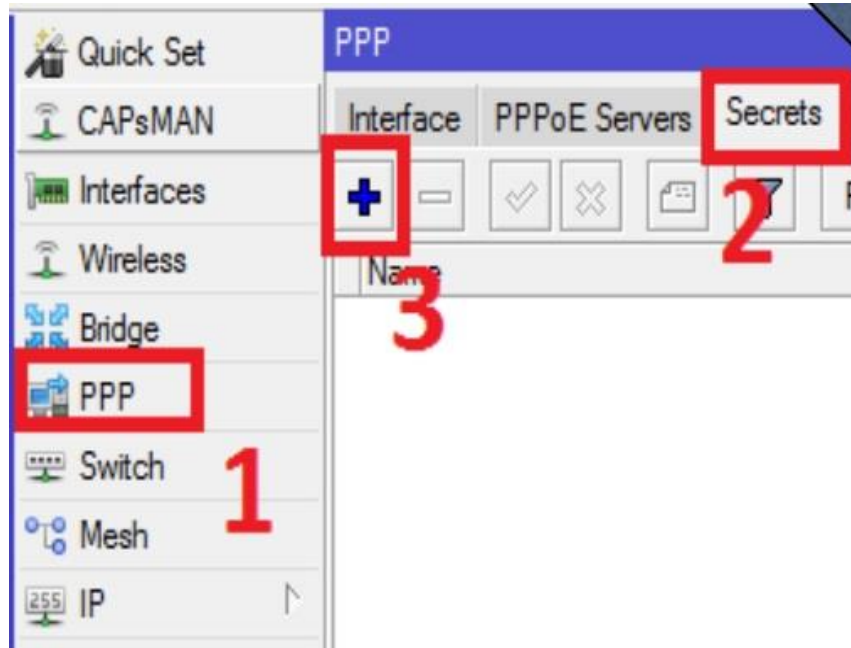
Y se declaro en primera instancia una ruta estatica para cada VPN

Programa



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

Implementación



PPP Secret <Bach503>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

carlo@ - WinBox v6.44 on CCR1036-12G-4S (tile)

Session Settings Dashboard

Safe Mode Session:

RouterOS WinBox

Quick Set CAPsMAN Interfaces Wireless Bridge PPP Mesh IP MPLS Routing System Queues Files Log RADIUS Tools New Terminal LCD Partition Make Supout.tif Manual New WinBox Exit

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

PPP Authentication&Accounting Find

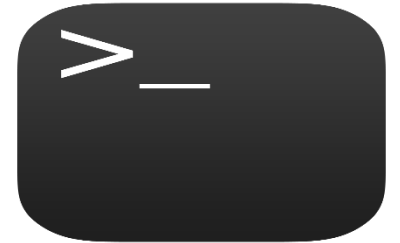
Name	Password	Service	Caller ID	Profile	Local Address	Remote Address	Last Logged Out
	****	any		default	10.10.12.189	10.10.12.190	
	****	any		default	10.10.12.191	10.10.12.192	
	****	any		default	10.10.12.193	10.10.12.194	
	****	any		default	10.10.12.195	10.10.12.196	
	****	any		default	10.10.12.197	10.10.12.198	
	****	any		default	10.10.12.199	10.10.12.200	
	****	any		default	10.10.12.201	10.10.12.202	Oct/24/2018 01:14:41
	****	any		default	10.10.12.203	10.10.12.204	Apr/08/2019 02:52:27
	****	any		default	10.10.12.205	10.10.12.206	Oct/14/2018 00:29:29
	****	any		default	10.10.12.207	10.10.12.208	
	****	any		default	10.10.12.209	10.10.12.210	Apr/08/2019 22:14:33
	****	any		default	10.10.12.211	10.10.12.212	
	****	any		default	10.10.12.213	10.10.12.214	
	****	any		default	10.10.12.215	10.10.12.216	
	****	any		default	10.10.12.217	10.10.12.218	
	****	any		default	10.10.12.219	10.10.12.220	
	****	any		default	10.10.12.221	10.10.12.222	Oct/14/2018 23:05:21
	****	any		default	10.10.12.223	10.10.12.224	
	****	any		default	10.10.12.225	10.10.12.226	Apr/08/2019 22:25:31
	****	any		default	10.10.12.227	10.10.12.228	
	****	any		default	10.10.12.229	10.10.12.230	
	****	any		default	10.10.12.231	10.10.12.232	
	****	any		default	10.10.12.233	10.10.12.234	
	****	any		default	10.10.12.235	10.10.12.236	
	****	any		default	10.10.12.237	10.10.12.238	
	****	any		default	10.10.12.239	10.10.12.240	
	****	any		default	10.10.12.241	10.10.12.242	
	****	any		default	10.10.12.243	10.10.12.244	
	****	any		default	10.10.12.245	10.10.12.246	
	****	any		default	10.10.12.247	10.10.12.248	
	****	any		default	10.10.12.249	10.10.12.250	
	****	any		default	10.10.12.251	10.10.12.252	
	****	any		default	10.10.12.253	10.10.12.254	
	****	any		default	10.10.13.1	10.10.13.2	
	****	any		default	10.10.13.3	10.10.13.4	
	****	any		default	10.10.13.5	10.10.13.6	Apr/08/2019 22:27:07

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

carlo@ - WinBox v6.44 on CCR1036-12G-4S (tile)

Session Settings Dashboard

Safe Mode Session:

RouterOS WinBox

PPP

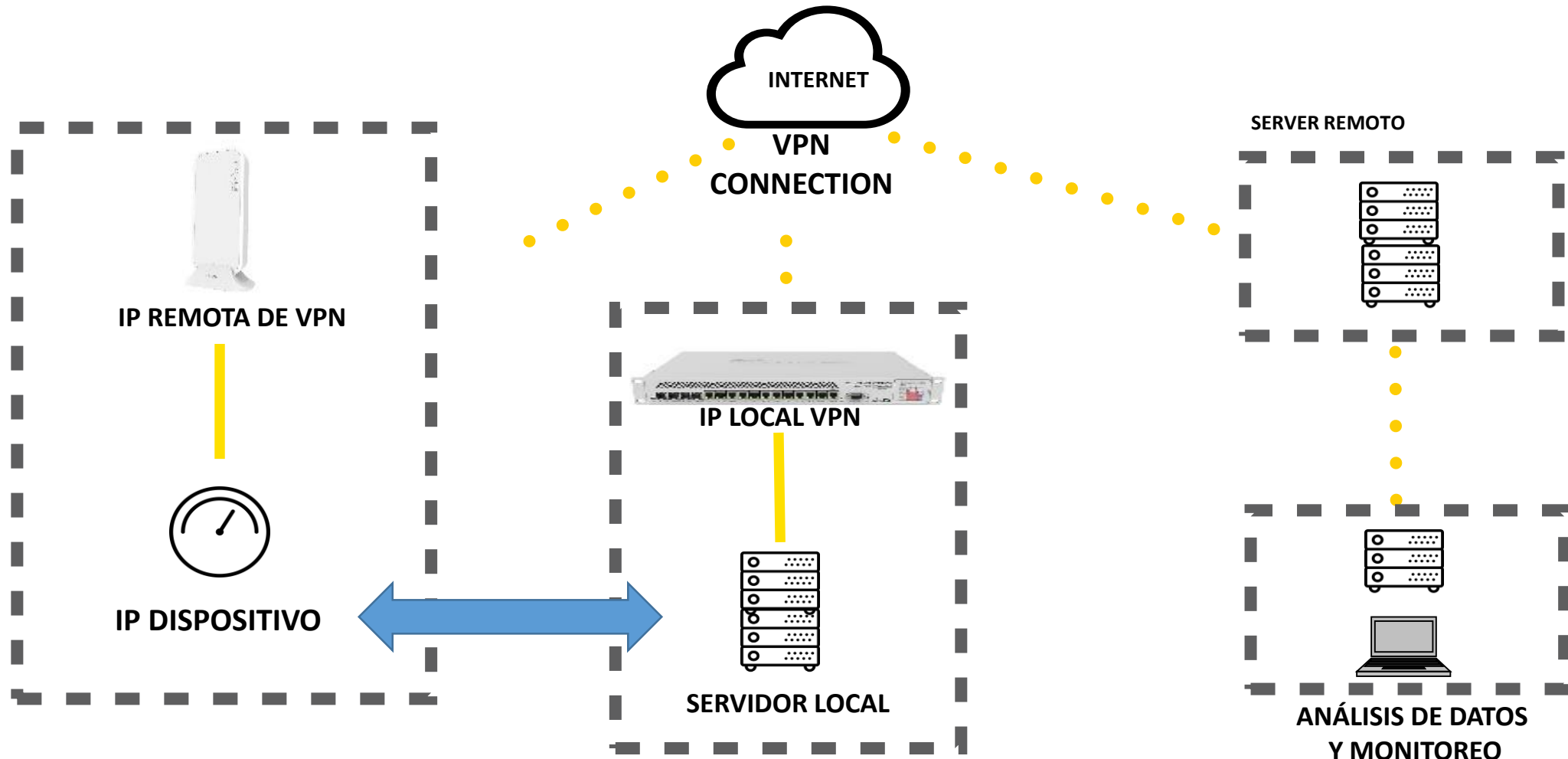
Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

Find

Name	Service	Caller ID	Encoding	Address	Uptime
L				10.10.13.214	17:04:29
L				10.10.13.216	00:51:40
...	N				
L				10.10.13.218	01:51:54
...	N				
L				10.10.13.226	01:45:28
...	N				
L				10.10.13.232	01:22:13
...	P				
L				10.10.13.242	00:14:01
...	N				
L				10.10.13.252	2d 14:20:...
...	N				
L				10.10.14.8	2d 14:20:55
L				10.10.14.10	00:43:08
...	N				
L				10.10.14.16	01:48:38
L				10.10.14.18	00:00:16
...	V				
L				10.10.14.20	3d 03:56:...
...	N				
L				10.10.14.22	3d 21:17:...
L				10.10.14.46	15:51:11
...	N				
L				10.10.14.110	04:25:54
...	N				
L				10.10.14.112	00:18:32
...	N				
L				10.10.14.112	01:58:54
...	N				
L				10.10.14.120	2d 09:57:...
...	N				
L				10.10.14.124	01:58:51
...	N				
L				10.10.14.126	01:58:47
...	N				
L				10.10.14.132	01:58:47
...	N				
L				10.10.14.132	6d 06:28:...
...	N				

104 items

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

Route <192.168.1.0/24>

General Attributes

Dst. Address: 192.168.1.0/24

Gateway: 10.10.16.198 reachable <pptp-Xlink003>

Check Gateway: [dropdown]

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

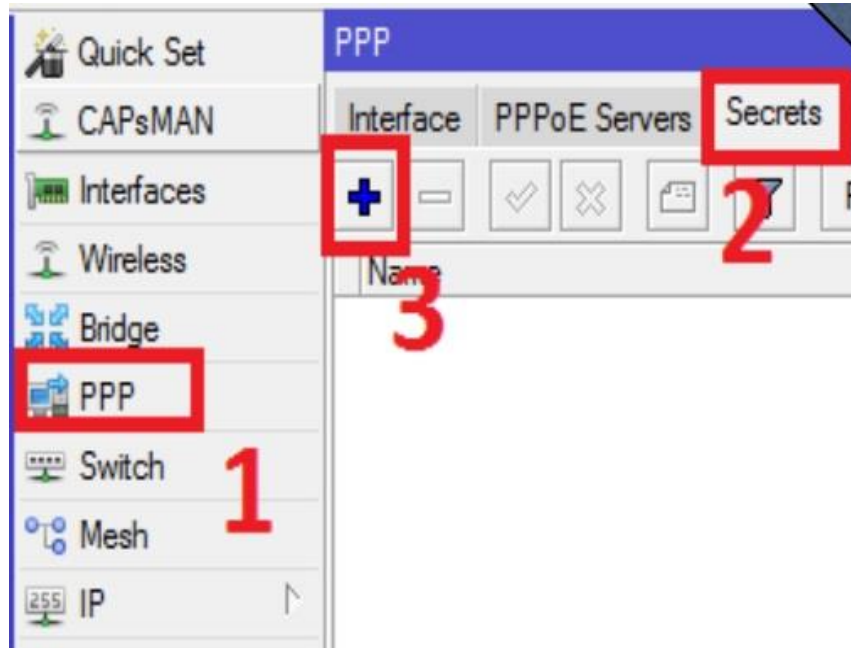
Precedence Mark: [dropdown]

Pref. Source: [dropdown]

enabled active static

OK Cancel Apply Disable Comment Copy Remove

Implementación Ruta Dinámica



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

PPP Secret <Xlink003>

Name: Xlink003

Password:

Service: any

Caller ID:

Profile: default

Local Address: 10.10.16.197

Remote Address: 10.10.16.198

Routes: 192.168.1.0/24

Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

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

Route <192.168.1.0/24>

General Attributes

Dst. Address: 192.168.1.0/24

Gateway: <pptp-Xlink003> reachable

Check G

Type: unicast

Distance: 1

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK

Copy

Remove

dynamic active static

Etiquetas de Rutas

Route List

Routes | Nexthops | Rules | VRF

+ - ✓ ✗ [icon] [icon]

Dst. Address [dropdown] in [dropdown] 192.168.1.0/24

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	▶ 192.168.1.0/24	10.10.16.198 reachable <pptp-Xlink003>	1		
DS	▶ 192.168.1.0/24	<pptp-Xlink003> reachable	1		

AS = Ruta Estática Activa

DS = Ruta Estática Dinámica

Route List

Routes | Nexthops | Rules | VRF

+ - ✓ ✗ [icon] [icon]

Dst. Address [dropdown] in [dropdown] 192.168.1.0/24

Find [input] all [dropdown]

+ - Filter

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
XS	▶ 192.168.1.0/24	10.10.16.198	1		
DAS	▶ 192.168.1.0/24	<pptp-Xlink003> reachable	1		

XS = Ruta Estática Desactivada

DSA = Ruta Estática Dinámica
Activa



Demostración

Route List

Routes Nexthops Rules VRF

Route List Table:

	Dest. Address	Gateway	Distance	Routing Ma
S	172.17.217.0/...		1	
DAS	172.17.234.0/...		1	
DAS	172.17.246.0/...		1	
S	172.17.247.0/...		1	
DAS	172.17.248.0/...		1	

PPP Secret

Name:

Password:

Service: any

Caller ID:

Profile: default

Local Address: 10.10.13.241

Remote Address: 10.10.13.242

Routes: 172.17.248.0/24

Limit Bytes In:

Limit Bytes Out:

Last Logged Out: Apr/08/2019 22:48:53

enabled

PPP Active User

General

Name:

Service: pptp

Caller ID: 200.68.137.153

Encoding:

Address: 10.10.13.242

Uptime: 01:05:29

Session ID: 8131aaf1 hex

Limit Bytes In:

Limit Bytes Out:

local

Traceroute (Running)

Traceroute To: 172.17.248.2

Packet Size: 56

Timeout: 1000 ms

Protocol: icmp

Port: 33434

☐ Use DNS

Count:

Max Hops:

Src. Address:

Interface:

DSCP:

Routing Table:

Traceroute Results Table:

Hop	/	Host	Loss	Sent	Last	Avg.	Best	Worst	Std. Dev.	History
1		10.10.13.242	27.0%	116	618.3ms	678.5	484.6	985.4	118.5	
2		172.17.248.2	26.1%	115	664.2ms	673.1	384.2	994.2	159.5	

309 items (1 selected)

2 items

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

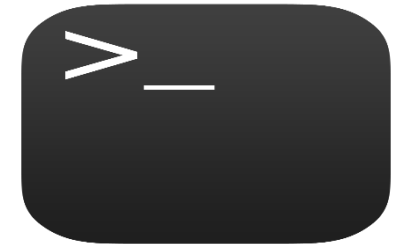
/interface pptp-client
add connect-to=dominioalcualconectar disabled=no name=VPN \
    password=***** user=Xlink003

/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

admin@172.17.248. WinBox v6.42.4 on wAP R (mipsbe)

Session Settings Dashboard

Safe Mode Session: 172.17.248.1

RouterOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rf
Manual
New WinBox
Exit

Interface <lte1>

General Status Traffic

Last Link Down Time:
Last Link Up Time: Apr/09/2019 00:35:40
Link Downs: 0
PIN Status: no password required
Functionality: full
Manufacturer: "MikroTik"
Model: "R11e-LTE"
Revision: "MikroTik_CP_2.160.000_v008"
Current Operator: 33420
Current Cell ID: 103696043
Access Technology: 3G HSDPA
EARFCN: 4413 (DL freq 882.6Mhz)
IMEI: 355654090588950
Session Uptime: 00:05:09
RSSI: -59 dBm

OK
Cancel
Apply
Disable
Comment
Torch
Scan...

Address List

	Address	Network	Interface
D	10.10.12.148	10.10.12.147	VPN_Xlink2
D	10.10.13.242	10.10.13.241	VPN
D	10.71.202.127	10.71.202.127	lte1
	172.17.248.1/...	172.17.248.0	LAN

Route List

Routes Nexthops Rules VRF

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	lte1 reachable	2		
AS	10.0.4.0/22	10.10.12.147 reachable VPN_Xlink2	1		
DAC	10.10.12.147	VPN_Xlink2 reachable	0		10.10.12.148
DAC	10.10.13.241	VPN reachable	0		10.10.13.242
DAC	10.71.202.127	lte1 reachable	0		10.71.202.127
DAC	172.17.248.0/...	LAN reachable	0		172.17.248.1
AS	192.168.100.1...	10.10.13.241 reachable VPN	1		

7 items

VRRP Bonding LTE

	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP
R	lte1	LTE	1480	1480		45.9 kbps	11.4 kbps	16	13	0 bps	13.9 kbps	

1 item out of 7

Write here to search

0:40 09/04/2019

Implementaciones Físicas





¡Gracias!

¿DUDAS?

Cel. 2293564126

carlomata@Xlink.com.mx