



Ruteo dinámico con OSPF sobre VPNs con servicio de telefonía IP

demyxperts

Ing. Gustavo Angulo – Venezuela
gangulo@mikrotikxperts.cl



VPN



Agenda

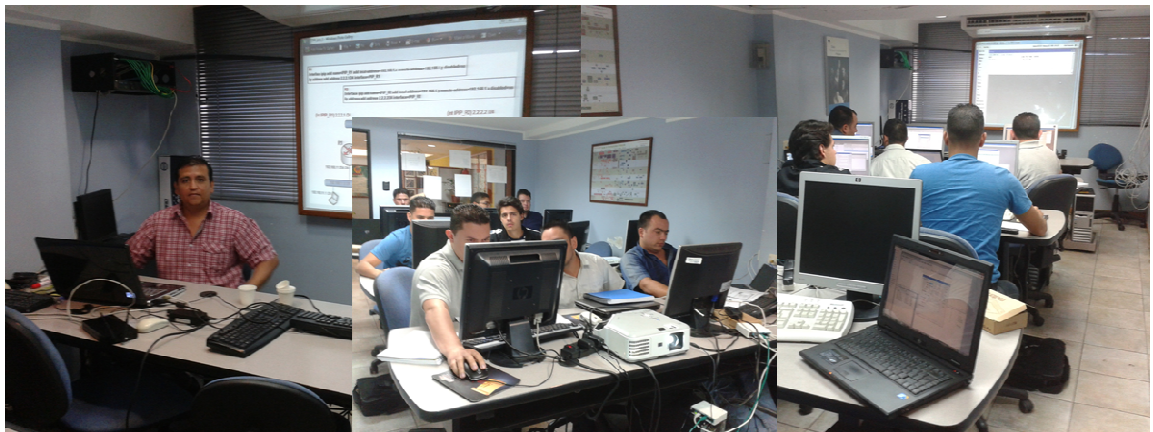
- Presentación
- Academy Xperts
- Requerimientos iniciales
- Direccionamiento
- Recomendaciones de VPN
- Recomendaciones en implementación de OSPF
- Soluciones versátiles
- Preguntas

Presentación

- Gustavo Angulo
 - Ingeniero en Telecomunicaciones
 - Academy Xperts Venezuela / Widuitcorp
 - Mikrotik Certified Trainer
 - MTCNA/MTCTCE/MTCWE/MTCRE/MTCUME/MTCINE
 - Cisco Trainer
 - CCNA/ CCNA Security CCAI

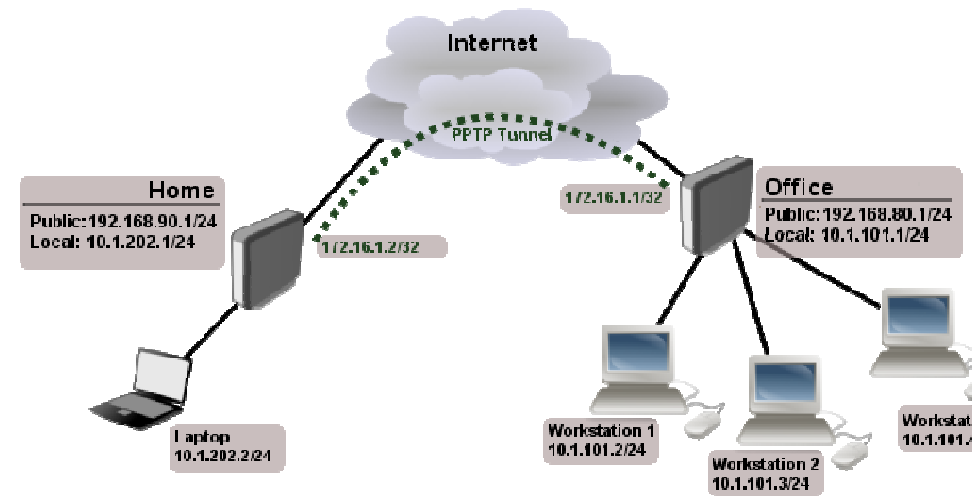
Academy Xperts

- Desde 2011 Academy Xperts imparte cursos en casi toda Latinoamérica



Requerimiento inicial

- Empresa “XYZ “ tiene sedes en:
 - Caracas
 - Maracay
 - Bogotá
 - Barranquilla
 - Barranquilla Zona Franca
 - Miami
 - Guayaquil
- La empresa requiere:
 - Compartir bases de datos
 - Soporte remoto.
 - Llamadas telefónicas vía VoIP entre sedes.



Direccionamiento

- Antes de comenzar es necesario tener un proyecto ordenado y coherente para la asignación de direcciones:
- Direcciones LAN
 - Maracay: 10.0.0.0/24
 - Caracas: 10.0.1.0/24
 - Barranquilla ZF : 10.0.2.0/24
 - Guayaquil : 10.0.3.0/24
 - Barranquilla: 10.0.4.0/24
 - Bogotá : 10.0.5.0/24
 - ~~Bogotá2: 10.0.6.0/24~~
 - Miami 10.0.7.0/24

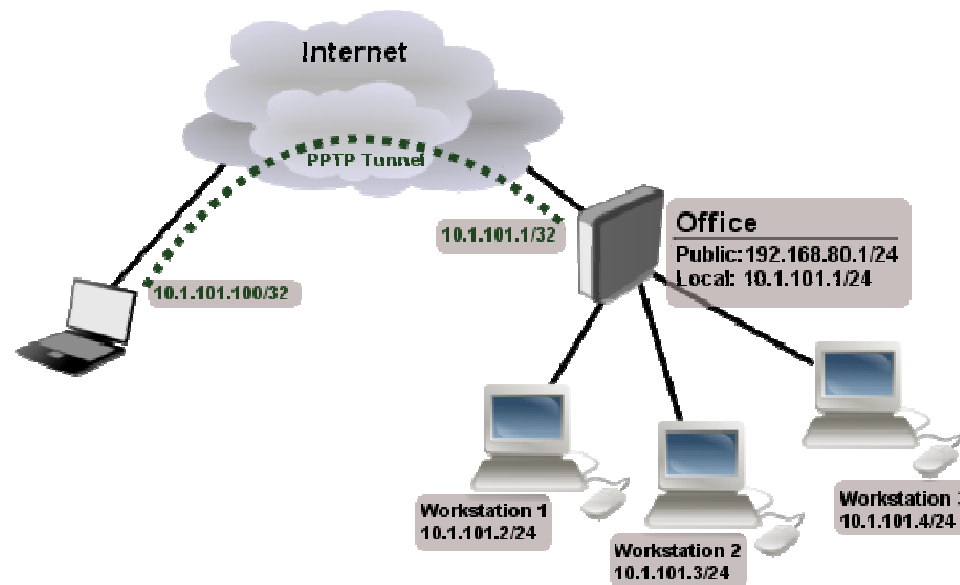
Equipos utilizados

- En 2009 se empezó con RB450, en 2013 se realizó la migración completa a equipos RB2011 con mejores prestaciones.



VPN Remote access(teletrabajo)

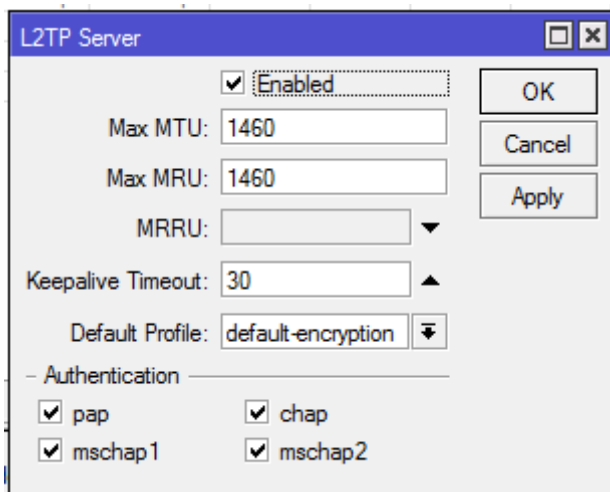
Este tipo de VPN permite establecer una conexión entre un PC y un router para acceder a servicios corporativos desde una red pública.



Pasos para configurar una VPN remote access

- En MikroTik constituye 2 pasos esenciales para habilitar el servidor
 - Habilitación del servicio
 - Creación de Secret con credenciales de acceso , dirección local y remota.

1



L2TP Server

☒ Enabled

Max MTU: 1460

Max MRU: 1460

MRRU:

Keepalive Timeout: 30

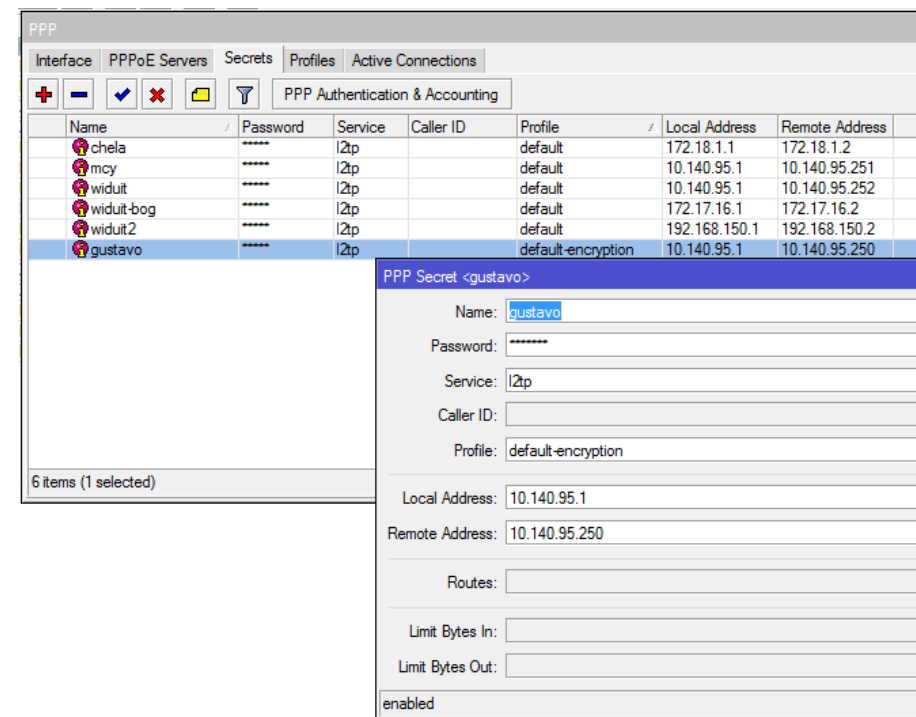
Default Profile: default-encryption

Authentication

☒ pap ☒ chap

☒ mschap1 ☒ mschap2

2



PPP

Interface PPPoE Servers Secrets Profiles Active Connections

PPP Authentication & Accounting

Name	Password	Service	Caller ID	Profile	Local Address	Remote Address
chela	*****	l2tp		default	172.18.1.1	172.18.1.2
mcy	*****	l2tp		default	10.140.95.1	10.140.95.251
widuit	*****	l2tp		default	10.140.95.1	10.140.95.252
widuit-bog	*****	l2tp		default	172.17.16.1	172.17.16.2
widuit2	*****	l2tp		default	192.168.150.1	192.168.150.2
gustavo	*****	l2tp		default-encryption	10.140.95.1	10.140.95.250

6 items (1 selected)

PPP Secret <gustavo>

Name: gustavo

Password: *****

Service: l2tp

Caller ID:

Profile: default-encryption

Local Address: 10.140.95.1

Remote Address: 10.140.95.250

Routes:

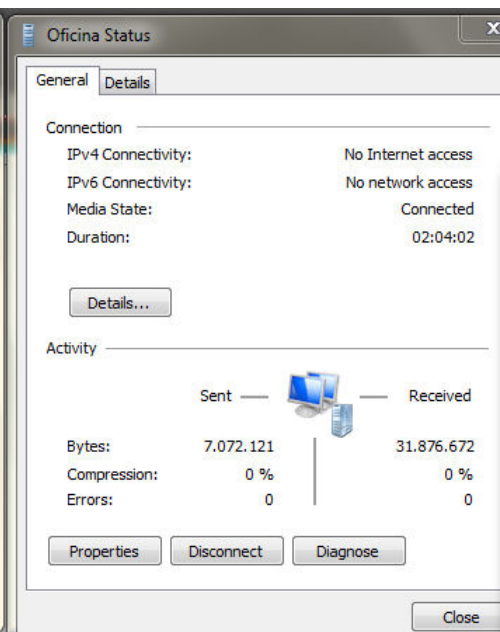
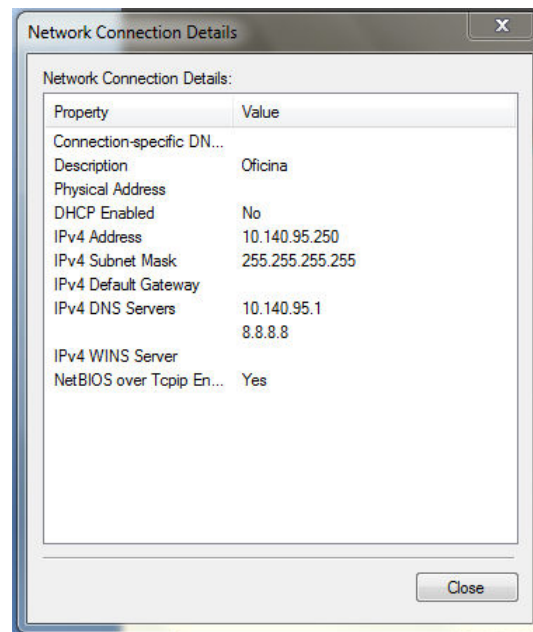
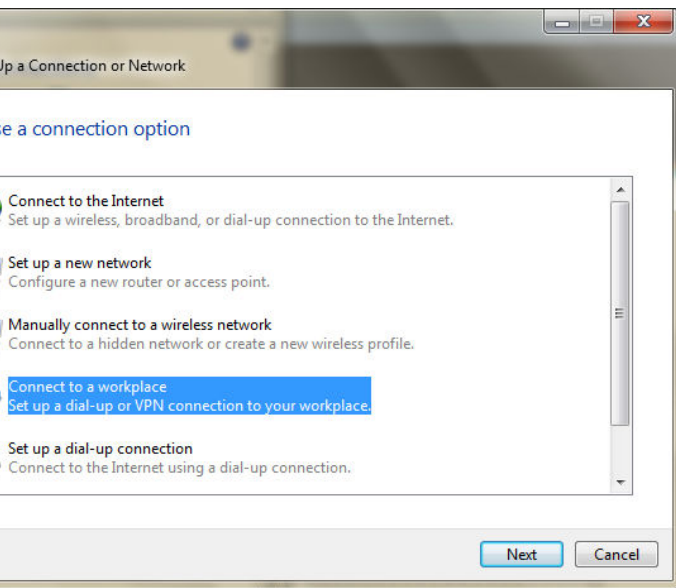
Limit Bytes In:

Limit Bytes Out:

enabled

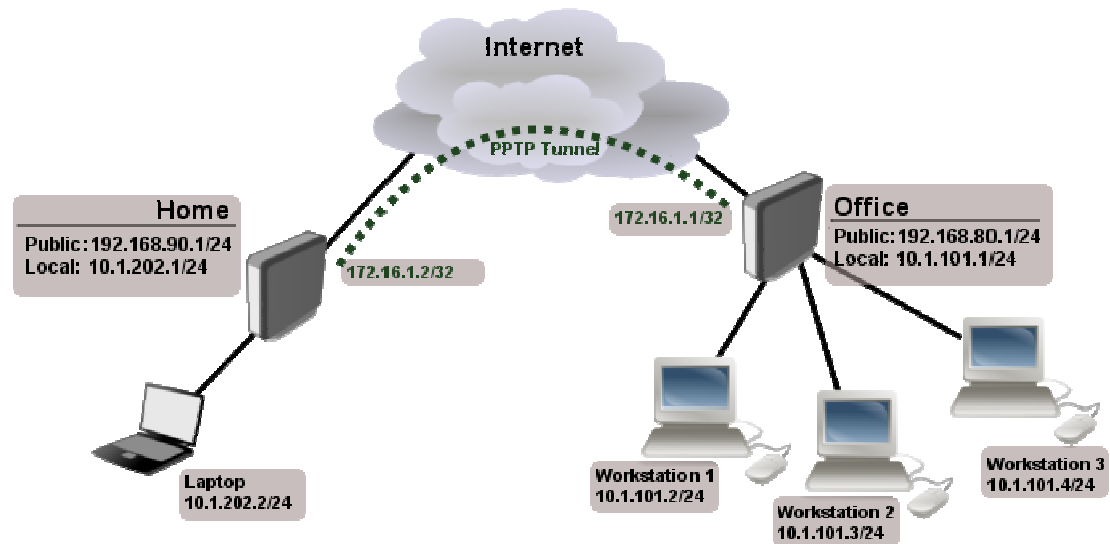
Pasos para configurar una VPN remote access

- En Windows se crea el cliente VPN con los siguientes datos:
 - IP Servidor VPN
 - Usuario y contraseña



VPN Site to Site

- Permite el establecimiento de conexión entre dos sedes remotas para permitir servicios locales a travesando una red pública.
- Tipos de VPN
 - PPTP
 - L2TP
 - SSTP
 - OpenVPN
 - IPSEC



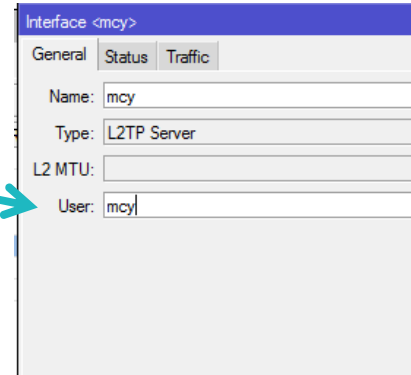
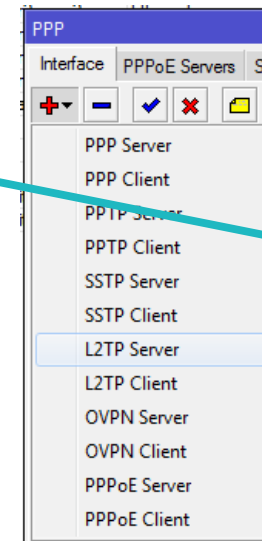
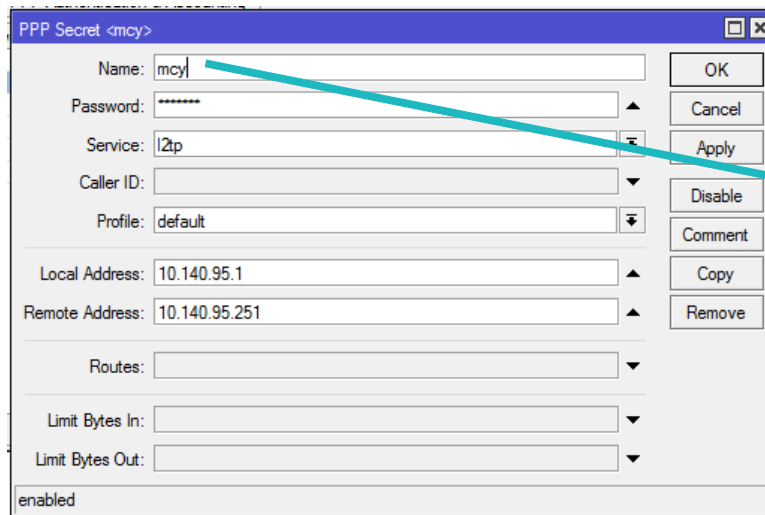
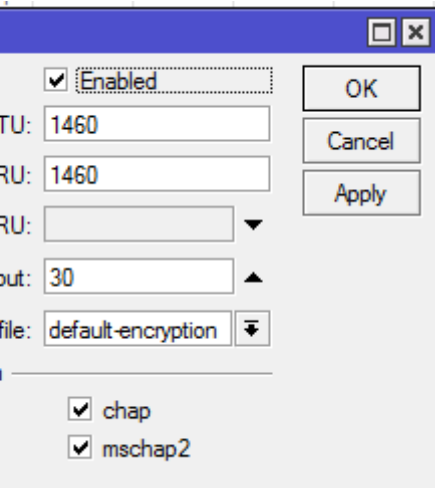
Pasos para configurar una VPN site to site

- Configuración del servidor

1. Habilitación del servicio
2. Creación de Secret con credenciales de acceso , dirección local y remota.
3. Creación de interfaz VPN Server (El usuario debe coincidir con el creado en el Secret)

2

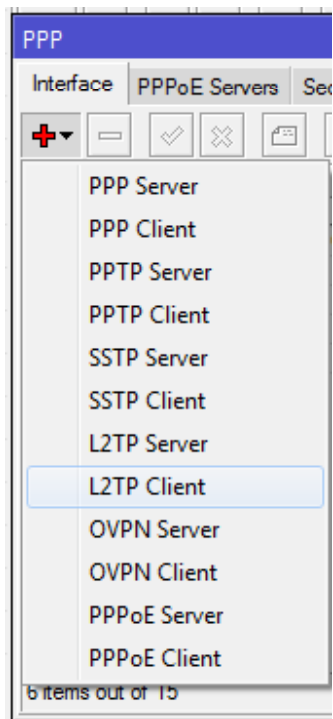
3



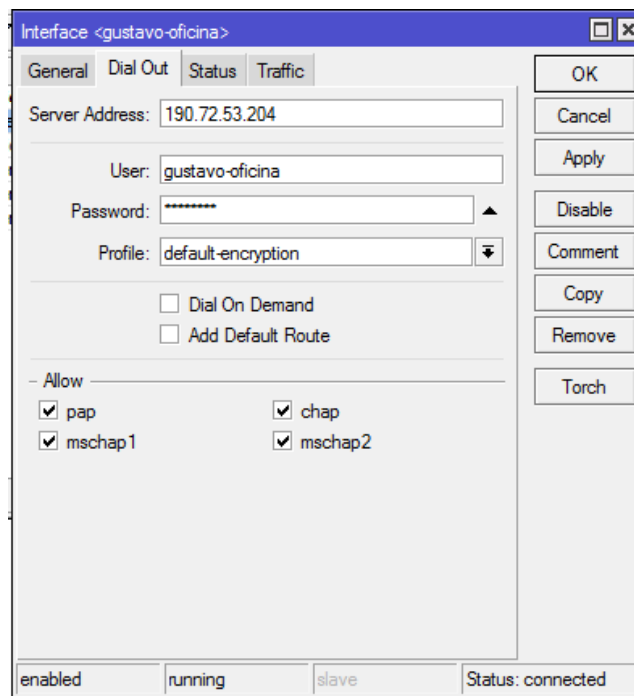
Pasos para configurar una VPN site to site

- Configuración del cliente

1. Creación de interfaz cliente en el MikroTik
2. Se colocan las credenciales de acceso (Usuario y contraseña) junto con la IP del servidor



2

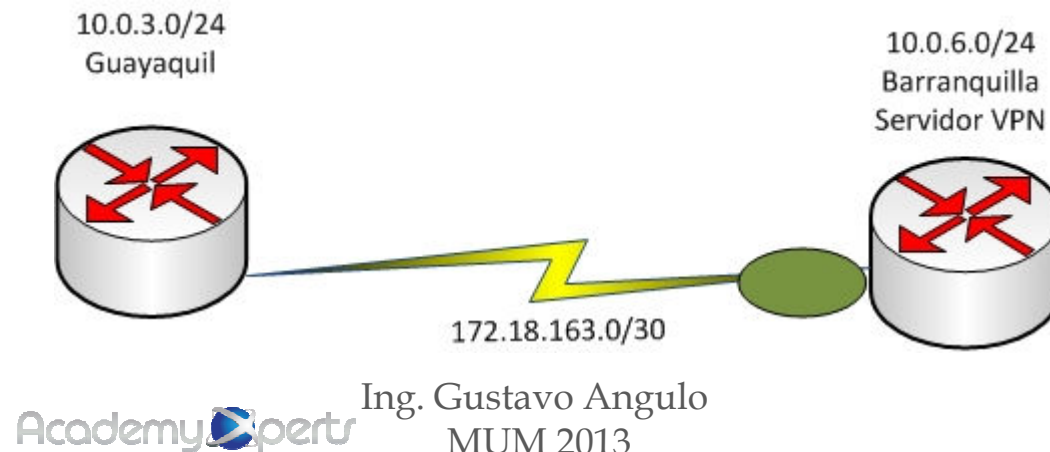


Recomendaciones en implementación de VPN

- Se evaluaron varias alternativas SSTP/PPTP/L2TP y se escogió L2TP porque era el tipo de VPN que incorporaba menos jitter y menos recursos de procesamiento.
- Implementar SSTP/PPTP significan más recursos de procesamiento e introducen un jitter que hace que la voz se degrade de forma importante.
- Uso de interfaces VPN estáticas para VPN site to site
- Ubicar servidores VPN en sedes con IP pública Fija con un buen enlace
- En el caso de ser sedes con Ip dinámica habilitar scripts.

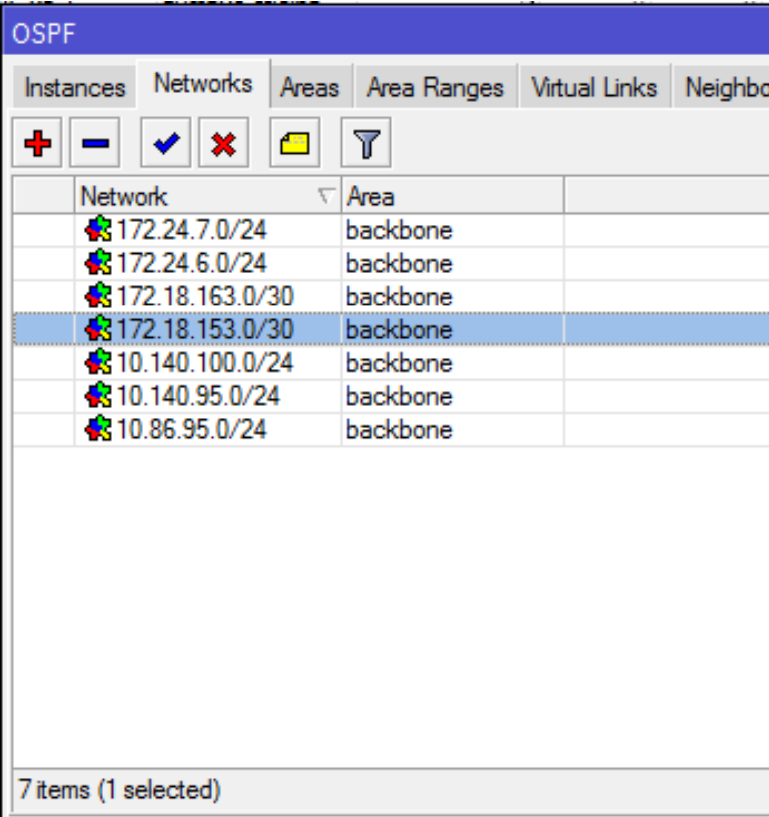
Enrutamiento estático

- Iniciamos enrutando entre los segmentos LAN mediante rutas estáticas.
- Con el crecimiento de la red y lo complejo de mantener las rutas claras y actualizadas fue necesario migrar a un protocolo avanzado.
- Se reestructuró el direccionamiento de redes punto a punto para conexión entre sedes de la siguiente manera:



Recomendaciones en OSPF

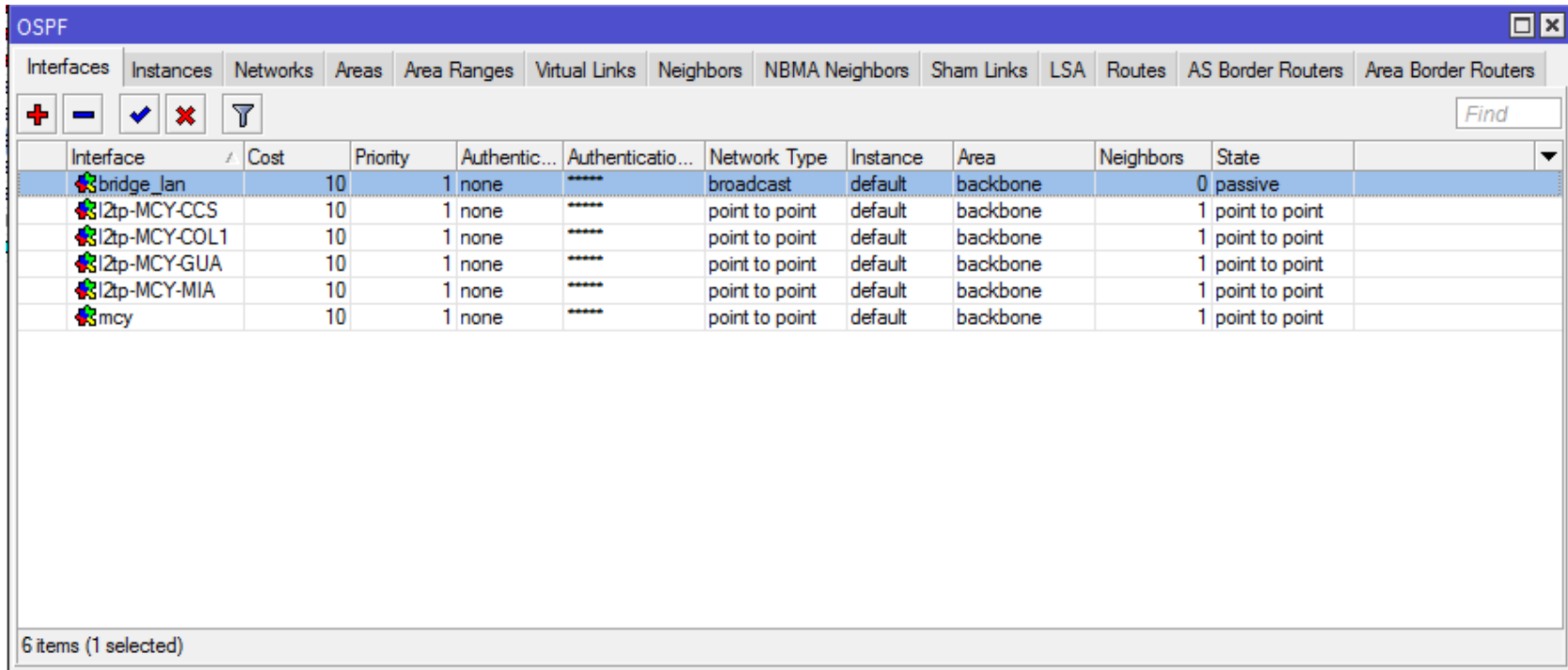
- Añadir las redes específicas que participaran en OSPF (LAN e interfaces VPN)
- A penas se coloca la primera red es suficiente para que la instancia OSPF se encuentre en modo running.



Instances	Networks	Areas	Area Ranges	Virtual Links	Neighbors
+	-	✓	✗	📁	🔍
Network	Area				
172.24.7.0/24	backbone				
172.24.6.0/24	backbone				
172.18.163.0/30	backbone				
172.18.153.0/30	backbone				
10.140.100.0/24	backbone				
10.140.95.0/24	backbone				
10.86.95.0/24	backbone				
7 items (1 selected)					

Recomendaciones en OSPF

- Añadir las interfaces que participarán en forma manual
 - Las interfaces VPN configurarlas como tipo punto a punto
 - Es altamente recomendable colocar la interfaz LAN en modo pasivo por seguridad y desempeño.



Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area	Neighbors	State
bridge_lan	10	1	none	*****	broadcast	default	backbone	0	passive
I2tp-MCY-CCS	10	1	none	*****	point to point	default	backbone	1	point to point
I2tp-MCY-COL1	10	1	none	*****	point to point	default	backbone	1	point to point
I2tp-MCY-GUA	10	1	none	*****	point to point	default	backbone	1	point to point
I2tp-MCY-MIA	10	1	none	*****	point to point	default	backbone	1	point to point
mcy	10	1	none	*****	point to point	default	backbone	1	point to point

6 items (1 selected)

Rutas dinámicas aprendidas mediante OSPF

RouterOS WinBox

Quick Set

Interfaces

Wireless

Bridge

PPP

Switch

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Make Supout.tif

Manual

Exit

Route List

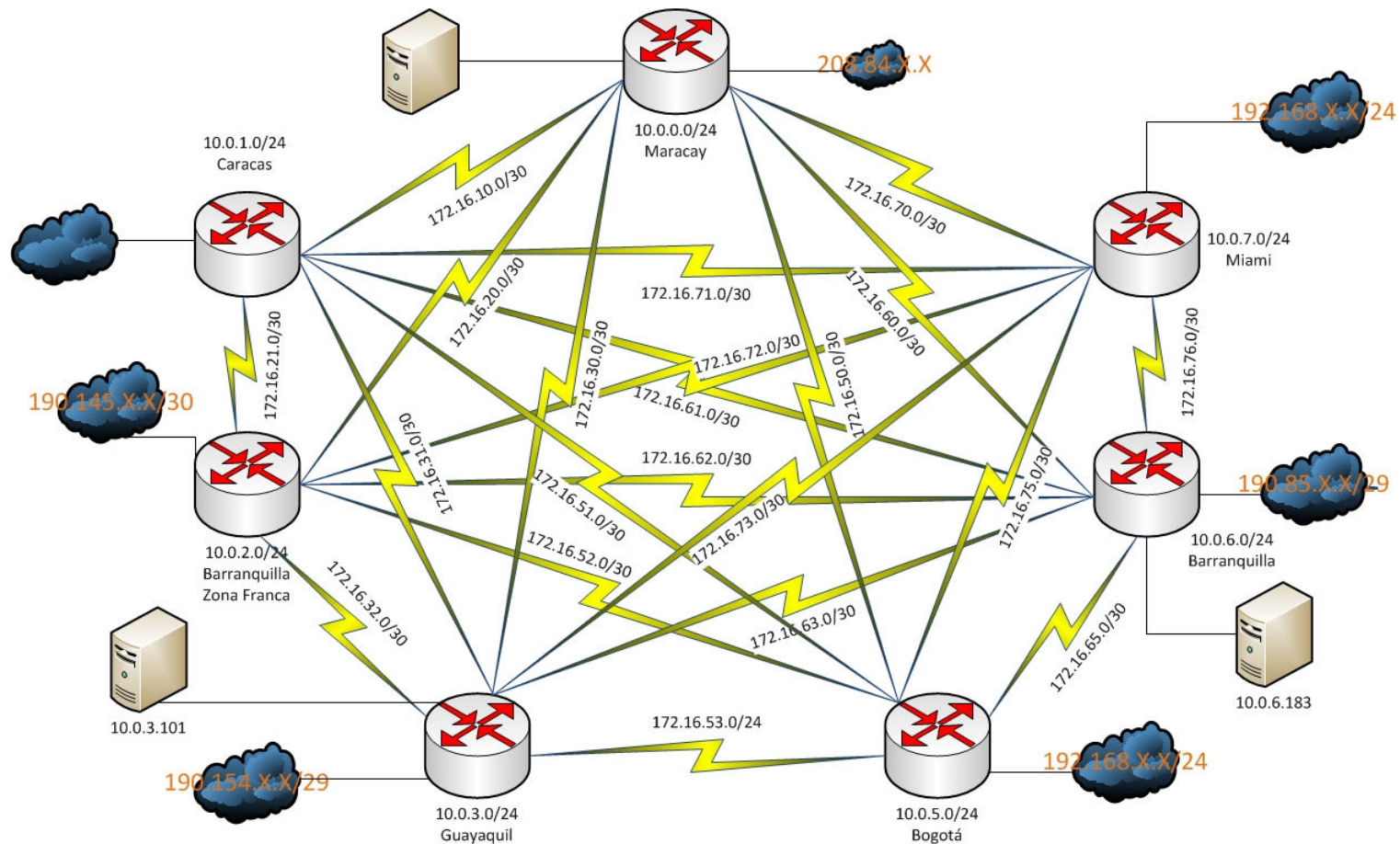
RoutesNexthopsRulesVRF

Findall

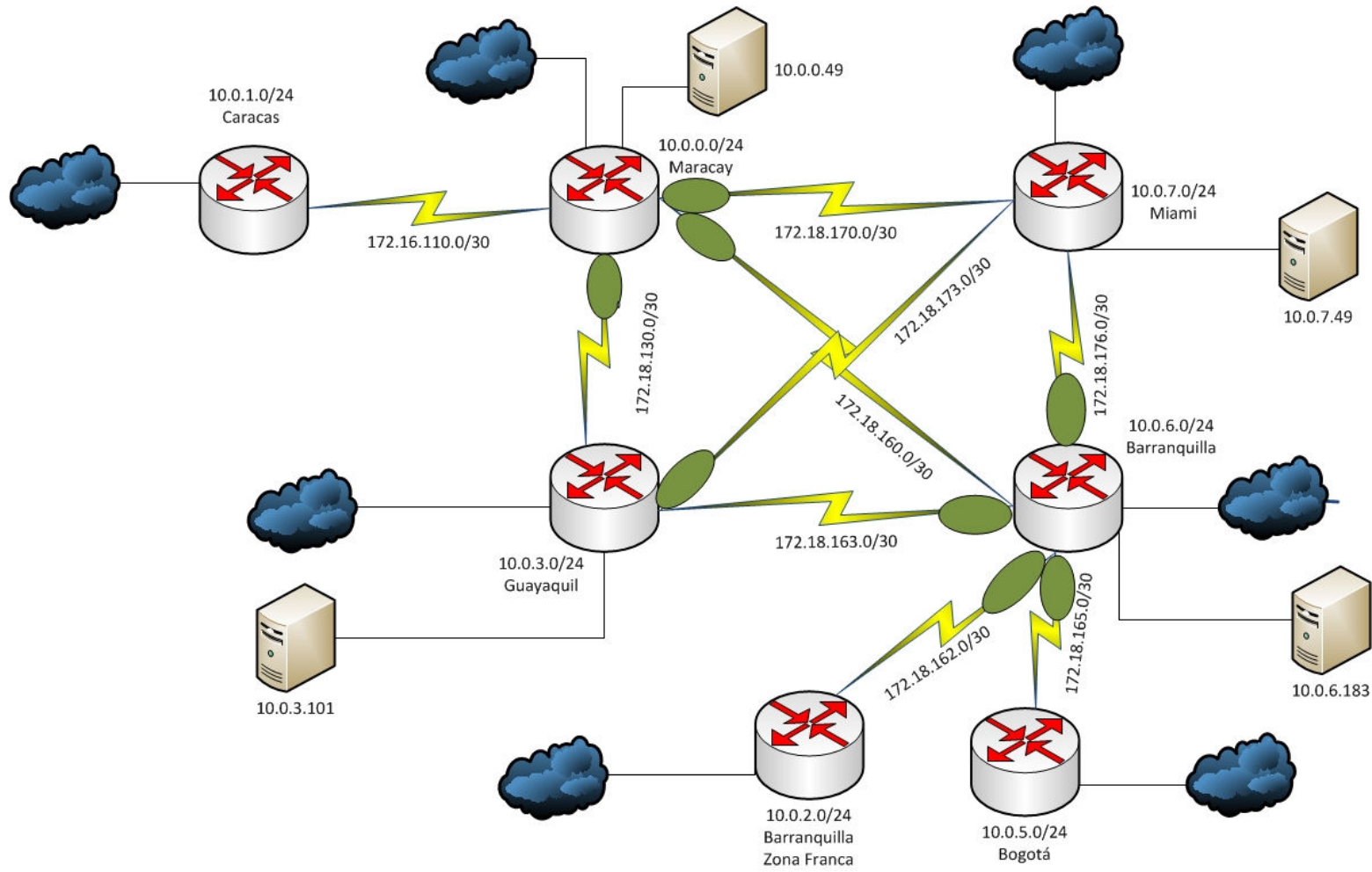
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	172.18.103.2	<2p-MCY-GUA> reachable	0		172.18.103.1
DAC	172.18.101.2	<2p-MCY-CCS> reachable	0		172.18.101.1
DAC	10.140.95.1	mcy reachable	0		10.140.95.251
DAC	10.0.0.0/24	bridge_1an reachable	0		10.0.0.1
AS	208.67.222.222	8.8.8.8 recursive via 208.84.81.97 ether1_wan	1		
AS	208.67.220.220	8.8.8.8 recursive via 208.84.81.97 ether1_wan	1		
AS	10.140.95.0/24	10.140.95.1 reachable mcy	1		
AS	8.8.8.8	208.84.81.97 reachable ether1_wan	1		
AS	0.0.0.0/0	186.92.64.1 reachable ether2_wan	1	to_wan2	
AS	0.0.0.0/0	8.8.8.8 recursive via 208.84.81.97 ether1_wan	1	to_wan1	
DAS	0.0.0.0/0	186.92.64.1 reachable ether2_wan	1		
S	0.0.0.0/0	8.8.8.8 recursive via 208.84.81.97 ether1_wan	2		
DAo	172.24.6.1	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	172.18.167.2	172.18.106.2 reachable <2p-MCY-COL1>	110		
DAo	172.18.167.1	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	172.18.163.2	172.18.106.2 reachable <2p-MCY-COL1>	110		
DAo	172.18.163.1	172.18.103.2 reachable <2p-MCY-GUA>	110		
DAo	172.18.137.2	172.18.103.2 reachable <2p-MCY-GUA>	110		
DAo	172.18.137.1	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	172.18.107.1	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	172.18.106.1	172.18.106.2 reachable <2p-MCY-COL1>	110		
DAo	172.18.103.1	172.18.103.2 reachable <2p-MCY-GUA>	110		
DAo	172.18.101.1	172.18.101.2 reachable <2p-MCY-CCS>	110		
DAo	10.140.95.252	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.140.95.250	172.18.107.2 reachable <2p-MCY-MIA>	110		
Do	10.140.95.0/24	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.140.86.0/24	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.86.95.2	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.86.95.1	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.0.7.0/24	172.18.107.2 reachable <2p-MCY-MIA>	110		
DAo	10.0.6.0/24	172.18.106.2 reachable <2p-MCY-COL1>	110		
DAo	10.0.3.0/24	172.18.103.2 reachable <2p-MCY-GUA>	110		
DAo	10.0.1.0/24	172.18.101.2 reachable <2p-MCY-CCS>	110		

37 items (21 selected)

Planteamiento con topología mallada



Topología definitiva – malla parcial



Resultados

- Clientes satisfechos con buena calidad de voz para sus llamadas
- Interconexión de centrales IP bajo Asterisk con troncales SIP e IAX
- Desde Maracay el personal de IT puede hacerle soporte remoto a los equipos de todas las sedes que no cuentan con personal de IT
- Procesamiento de queries de base de datos accediendo a servidores en Barranquilla y Maracay
- Enlaces VPN de respaldo en caso de falla de alguna conexión a internet.

¡Gracias por su atención!

¿ Preguntas?

Academy xperts

Ing. Gustavo Angulo – Venezuela
gangulo@mikrotikxperts.cl

