



PRESENTADO POR ALFIO
MUÑOZ

NUBE PRIVADA CON MIKROTIK CLOUD HOSTED ROUTER, VIRTUALIZACION, DISASTER RECOVERY Y TELEFONIA IP



Acerca de mi

Alfio Muñoz

- MikroTik Certified Consultant.
- Director de entrenamientos y capacitaciones de Issabel PBX.
- Consultor de infraestructura y telefonía para el Ministerio de Defensa RD.

Experiencia:

- 12 años de experiencia en Networking, routing y switching desde el 2007
- Implementación de soluciones VoIP para empresas
- Virtualización de datacenters e infraestructura de servidores
- Capacitaciones de Voip, Virtualización, etc.
- Amante del software libre, pero no fanático.



AGENDA

- Que es un Cloud Hosted Router (CHR)
- Que es Proxmox
- Instalacion del CHR de Mikrotik
- Primeras configuraciones CHR
- Asignacion de Puentes virtuales Proxmox
- Creación de Nube privada
- Publicando servicios desde el CHR
- Creación de VPN L2TP IPSEC y BCP
- Plan de replicación de servidores de local a remoto por túnel VPN
- Telefonía IP mediante Tuneles BCP

CLOUD HOSTED ROUTER

- Cloud Hosted Router (CHR) es una version de RouterOS creada para ejecutarse como una maquina virtual. Soporta arquitectura x86 64-bit y puede ser utilizado por los principales hypervisores para virtualizacion como: VMWare, Hyper-V, VirtualBox, KVM y muchos mas. CHR Tiene todas las funcionalidades habilitadas por defecto pero viene con un modelo de licenciamiento diferente que las demas versions de RouterOS.
- Para mas detalles:
- <https://wiki.mikrotik.com/wiki/Manual:CHR>

PROXMOX



QUE ES PROXMOX

- Es un proyecto de código abierto, desarrollado y mantenido por Proxmox Server Solutions.
- Completa plataforma de virtualización basada en sistemas de código abierto que permite la virtualización tanto sobre LXC como KVM.
- Es una distribución bare-metal, basada en Debian con solo los servicios básicos para de esta forma obtener un mejor rendimiento.
- Permite la migración en vivo de máquinas virtuales, clustering de servidores, backups automáticos y conexión a un NAS/SAN con NFS, iSCSI, etc...

Cloud Hosted Router



	6.44.5 (Long-term)	6.45.3 (Stable)	6.46beta16 (Testing)
Images	vmdk, vhdx, vdi, ova, img		
VHDX image			
VMDK image			
VDI image			
OVA template			
Raw disk image			
Extra packages			
The Dude server			
The Dude client			
Changelog			
Checksum			

DIFERENTES MANERAS DE INSTALAR EL CHR EN PROXMOX

DESCARGANDO LA IMAGEN DIRECTAMENTE DESDE EL SITIO WEB DE MIKROTIK

TIPOS DE INSTALACIONES

- Crear la VM y verificar bien el ID de esta, en nuestro caso de ejemplo 125, crear el disco en formato qcow2
- Subir o descargar el archivo .img al servidor proxmox
- Ubicar la carpeta donde se ha creado la VM
- Correr el siguiente commando en la misma carpeta que subimos la imagen del CHR : `qemu-img convert -f raw -O qcow2 chr-6.44.5.img vm-125-disk-0.qcow2`
- Luego ir a la carpeta que contiene el disco virtual de la VM que es `/var/lib/vz/images/125` y reemplazarlo por la imagen ya convertida.
- Arrancamos nuestra VM y listo.

INSTALANDO DESDE UNA IMAGEN RAW

- <https://www.youtube.com/watch?v=MeVfZvaGDAU&feature=youtu.be>

INSTALANDO CON EL SCRIPT

- Notas a tener en cuenta:
- Crear el directorio `/home/root/temp` de forma manual con un `mkdir /home/root/temp`
- Colocarse en ese directorio y crear el archivo donde vamos a copiar el script dentro.
- Ejemplo: `touch chrinstallscript.sh`
- Darle permisos de ejecución: `chmod 755 chrinstallscript.sh`

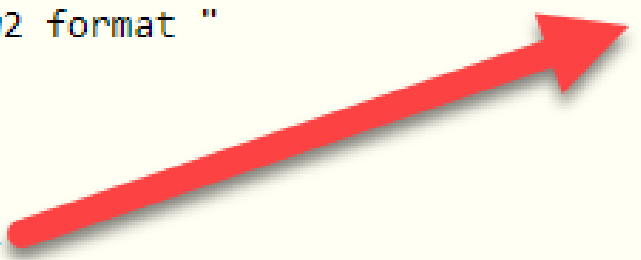
INFORMACION DE LA WIKI

- https://wiki.mikrotik.com/wiki/Manual:CHR_ProxMox_installation

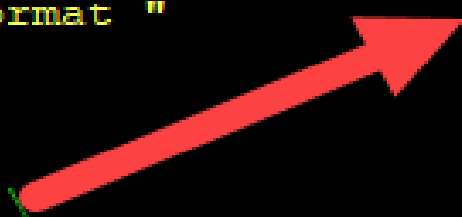
INSTALANDO CON EL SCRIPT

Modificamos la linea y le
agregamos “/home” de otra forma
no nos va a funcionar.

```
# Creating qcow2 image for CHR.  
echo "-- Converting image to qcow2 format "  
qemu-img convert \  
    -f raw \  
    -O qcow2 \  
    /root/temp/chr-$version.img \  
    /var/lib/vz/images/$vmID/vm-$vmID-disk-1.qcow2  
# Creating VM
```



```
# Creating qcow2 image for CHR.  
echo "-- Converting image to qcow2 format "  
qemu-img convert \  
    -f raw \  
    -O qcow2 \  
    /home/root/temp/chr-$version.img \  
    /var/lib/vz/images/$vmID/vm-$vmID-disk-1.qcow2  
# Creating VM  
echo "-- Creating new CHR VM"
```



- 
- 
- https://www.youtube.com/watch?v=8i_vwywNMho&feature=youtu.be

PROXMOX Virtual Environment 6.0-4

Server View

- Datacenter
 - alfiolab
 - 300 (Centos7)
 - 301 (OwnCloud)
 - 100 (CG-WIN2012-R2)
 - 125 (CHRMKT)
 - 150 (chr-6.44.5)**
 - local (alfiolab)

Virtual Machine 150 (chr-6.44.5) on node 'alfiolab'

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

Add Remove Edit Resize disk Move disk Revert

Memory	256.00 MiB
Processors	1 (1 sockets, 1 cores)
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	Default (LSI 53C895A)
Hard Disk (virtio0)	local:150/vm-150-disk-1.qcow2
Network Device (net0)	virtio=16:1D:2E:9A:8F:F6,bridge=vbr0

NUESTRO CHR
LISTO Y
EJECUTANDOSE

Escenario I

Nube Privada

Como crear la nube privada y agregar una interfaz del CHR al segmento privado, de manera que solo se tenga acceso a dicho segmento mediante el CHR.

Podemos tener la opción de aislarnos totalmente de la red pública publicar servicios mediante nuestro nuestro CHR redireccionando puertos

CREACION DE UN
SEGMENTO PUENTE
AISLADO EN
PROXMOX PARA
ASIGNARLO A
NUESTRO CHR

BRIDGE EN PROXMOX CON UN PUERTO FISICO DE RED

PROXMOX Virtual Environment 5.2-6 You are logged in as 'root@pam' [Documentation](#) [Create VM](#) [Create CT](#) [Logout](#)

Server View

Datacenter

- Proxmox2
 - 100 (JoomlaMUM)
 - 101 (mail.hospitalcentral.mil.do)
 - 102 (Corazonesunidos)
 - 104 (Moodlelssabel)
 - 111 (mail.corazonesunidos.com.do)
 - 203 (NextCloud)
 - 400 (NextCloud-Disnet)
 - 401 (NextCloud-Fonsabana)
 - 150 (MKT)
 - 200 (Elastix4)
 - 201 (Win2016SRV)
 - 300 (cPanelMaster)
 - 302 (Belltec)
 - 303 (MailStore)
 - 310 (cpanel-03)
 - 311 (cPanel-02)
 - 322 (cPanel-05)
 - 330 (cPanel-07)
 - BackupOVH5TB (Proxmox2)

Node 'Proxmox2'

[Restart](#) [Shutdown](#) [Shell](#) [Bulk Actions](#) [Help](#)

[Create](#) [Revert](#) [Edit](#) [Remove](#)

Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	IP address	Subnet mask	Gateway	Comment
eth0	Network Device	Yes	No	No					
eth1	Network Device	No	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	eth0	2607:5300:020...			
vmbr1	Linux Bridge	Yes	Yes	No	dummy0				
vmbr2	Linux Bridge	Yes	Yes	No					
vmbr3	Linux Bridge	Yes	Yes	No					Bridge JC

System

- Network
- Certificates
- DNS
- Time
- Syslog
- Updates
- Firewall
- Disks
- Ceph

PUENTES EN PROXMOX PARA EL CHR

Edit: Linux Bridge

Name:	vmbr0	Autostart:	☒
IP address:	192.168.1.1	VLAN aware:	☐
Subnet mask:	255.255.255.0	Bridge ports:	eth0
Gateway:	192.168.1.254	Comment:	
IPv6 address:	2001:5000:0000:0000:0000:0000:0000:0000		
Prefix length:	64		
Gateway:			

OK Reset

Edit: Linux Bridge

Name:	vmbr2	Autostart:	☒
IP address:		VLAN aware:	☐
Subnet mask:		Bridge ports:	
Gateway:		Comment:	
IPv6 address:			
Prefix length:			
Gateway:			

OK Reset

ual Machine 150 (MKT) on node 'Proxmox2'

Summary	Add Remove Edit Resize disk Move disk Revert	
Console	Keyboard Layout	Default
Hardware	Memory	1.00 GiB
Cloud-Init	Processors	4 (1 sockets, 4 cores)
Options	Display	SPICE (qxl)
Task History	CD/DVD Drive (ide2)	none,media=cdrom
Monitor	Hard Disk (scsi0)	local:150/vm-150-disk-1.qcow2,size=32G
Backup	Network Device (net0)	virtio=02:00:00:e2:af:0b,bridge=vmbr0
Replication	Network Device (net1)	virtio=06:00:36:31:80:14,bridge=vmbr1
Snapshots	Network Device (net2)	virtio=12:86:C7:1F:21:37,bridge=vmbr3
Firewall	Network Device (net3)	virtio=CA:2F:DA:6C:2F:A1,bridge=vmbr0
Permissions	Network Device (net4)	virtio=AE:6D:E5:3D:42:7E,bridge=vmbr2

CADA
TARJETA A UN
PUENTE
DISTINTO

- 
- 
- El vmbr0 es el Puente que se comunica con el exterior y donde tendremos asignadas las IP públicas.
 - Los otros puentes son segmentos aislados independientes en donde solo se pueden comunicar los equipos en el mismo Puente.
 - En el CHR asignamos en cada interfaz de los otros puentes las IP privadas.
 - En el CHR creo reglas para publicar Servicios que apunten a la red privada interna de un segmento o puente.
 - Puedo crear tuneles VPN con BCP que se conecten directamente a cada segmento o Puente.

NAT Rule 

General Advanced Extra Action Statistics

Chain: dstnat

Src. Address:

Dst. Address: 

Protocol: ☐ 6 (tcp)

Src. Port:

Dst. Port: ☐ 443

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

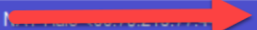
Routing Mark:

Routing Table:

Connection Type:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters



General Advanced Extra Action Statistics

Action: dst-nat

☐ Log

Log Prefix:

To Addresses: 192.168.25.50

To Ports: 443

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

PUBLICANDO
UN SERVICIO
EN EL CHR

SALIDA UNO A UNO DE UN CLIENTE

NAT Rule <192.168.25.50>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address: ☐ 192.168.25.50

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

In. Interface List:

Out. Interface List:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters

NAT Rule <192.168.25.50>

General Advanced Extra Action Statistics

Action: netmap

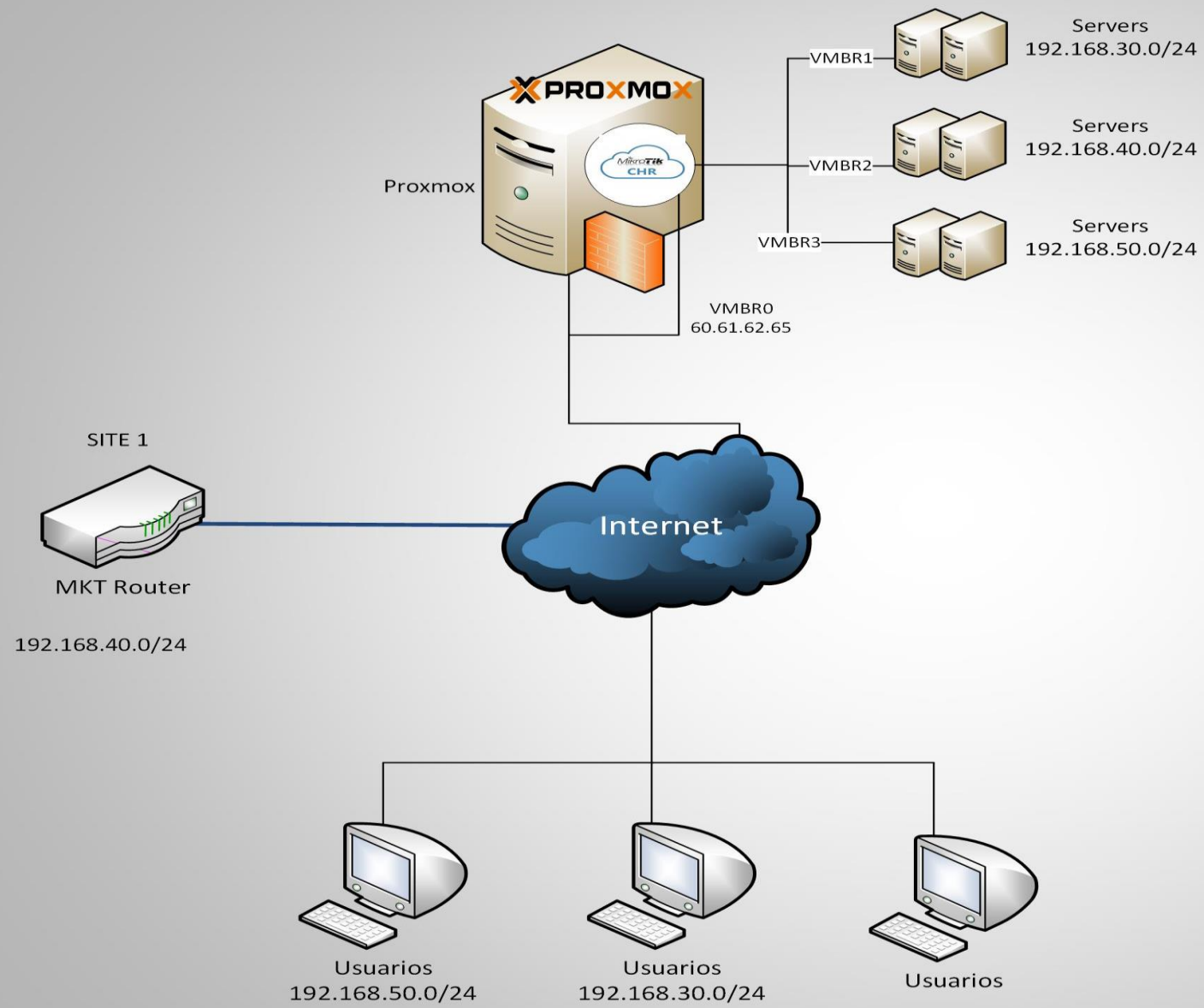
☐ Log

Log Prefix:

To Addresses: 

To Ports:

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters



ESCENARIO 2: DISASTER RECOVERY Y FAILOVER 100% AUTOMATIZADO

- Mediante el túnel BCP **conectamos tres centros** de datos iguales donde tenemos Proxmox instalado

PPP + BCP

- Trataremos con:
- Layer 2 Tunneling Protocol (L2TP), el cual lo vamos a combinar con encriptacion IPSEC
- BCP es Bridge Control Protocol, el cual permite el envio de tramas Ethernet sobre PPP.
- Multilink Maximum Received Reconstructed Unit (MRRU)

MULTI-LINK PPP

- QUE ES MULTI-LINK PPP?

RFC 1990

<https://tools.ietf.org/html/rfc1990>

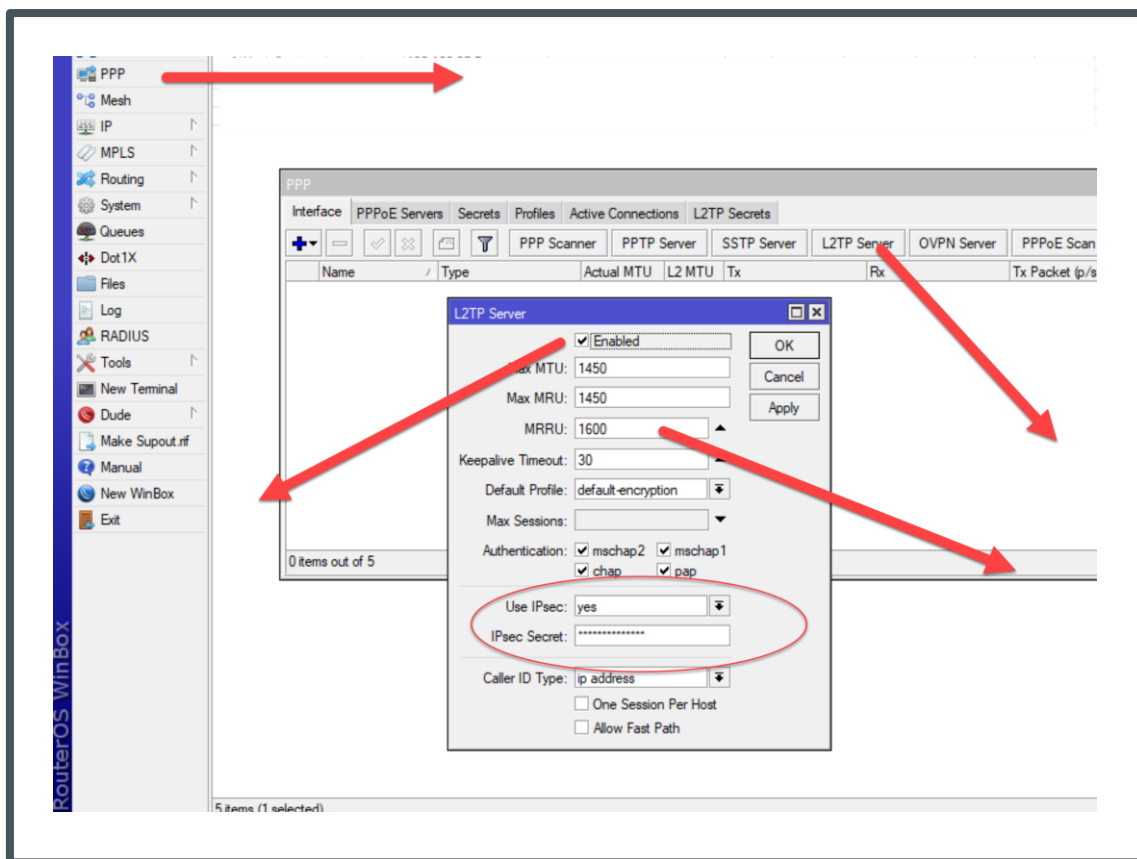
Multi-Link Point to Point Protocol (MP, Multi-Link PPP, MultiPPP or MLPPP) es un metodo de dividir, recombinar and secuenciar datos a traves de multiples enlaces logicos de datos.

Fuente:

https://wiki.mikrotik.com/wiki/Manual:MLPPP_over_single_and_multiple_links

Para que una VPN capa 2 funcione las tramas ETHERNET tienen que viajar através del tunel VPN, pero generalmente el MTU de la VPN es mas pequeño que el tamaño de la trama ETHERNET. En ese orden para poder tener o manejar un MTU mayor debemos establecer multiples tuneles PPP y los combinamos todos juntos, esto se llama Multi-Link PPP

L2TP SERVER CON IPSEC



- En el servidor principal habilitamos el L2TP server con IPSEC Es muy importante cambiar el MRRU a 1600 por el tema del multilink anteriormente explicado.

EN EL SERVIDOR PRINCIPAL

- Creamos un Bridge y seleccionamos SRTP para el STP
- **Bridge** menu → **[+]**
- Luego agregamos el Puerto del CHR, aqui Podemos elegir un Puerto ethernet, en nuestro caso el eth5

Interface <bridge1>

General STP VLAN Status Traffic

Name: bridge1

Type: Bridge

MTU: [dropdown]

Actual MTU: 1500

L2 MTU: 65535

MAC Address: 62:D4:6F:64:53:67

ARP: enabled [dropdown]

ARP Timeout: [dropdown]

Admin. MAC Address: [dropdown]

Ageing Time: 00:05:00

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

New Bridge Port

General STP VLAN Status

Interface: ether5 [dropdown]

Bridge: bridge1 [dropdown]

Horizon: [dropdown]

Learn: auto [dropdown]

☒ Unknown Unicast Flood

☒ Unknown Multicast Flood

☒ Broadcast Flood

☐ Trusted

☒ Hardware Offload

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

Interface <bridge1>

General STP VLAN Status Traffic

Protocol Mode: ☐ none ☐ STP ☒ RSTP ☐ MSTP

Priority: 8000 hex

Region Name: [text box]

Region Revision: 0

Max Message Age: 00:00:20

Forward Delay: 00:00:15

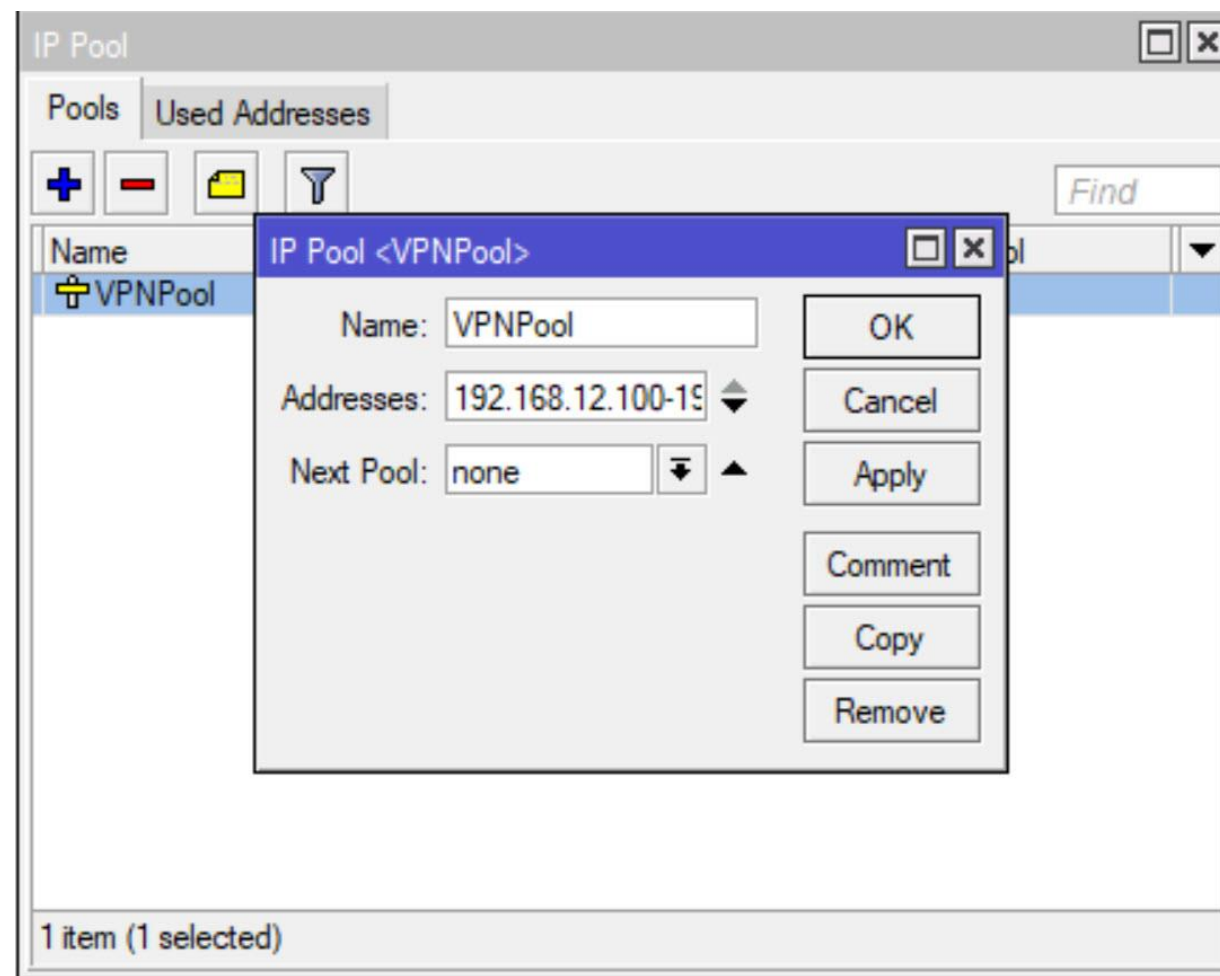
Transmit Hold Count: 6

Max Hops: 20

Status: running slave

POOL PARA VPN

- Creamos un IP Pool para las VPN point-to-point IP:
- IP → Pools → [+]



SERVIDOR PRINCIPAL

- Creamos un profile ppp y habilitamos el BCP cuando asignamos el bridge ya creado anteriormente al profile.

The screenshot shows the 'PPP Profile <MumBog>' configuration window. The 'General' tab is selected. The 'Name' field is 'MumBog'. The 'Local Address' is '192.168.12.1'. The 'Remote Address' is 'VPNPool'. The 'Bridge' is 'bridge1'. The 'Bridge Port Priority' is empty. The 'Bridge Path Cost' is empty. The 'Bridge Horizon' is empty. The 'Incoming Filter' is empty. The 'Outgoing Filter' is empty. The 'Address List' is empty. The 'Interface List' is empty. The 'DNS Server' is empty. The 'WINS Server' is empty. The 'Change TCP MSS' section has 'no' selected. The 'Use UPnP' section has 'default' selected. A red arrow points from the 'Bridge' field to the 'Bridge Path Cost' field. Another red arrow points from the 'Bridge Path Cost' field to the 'Bridge Horizon' field. A third red arrow points from the 'Bridge Horizon' field to the 'Incoming Filter' field. A fourth red arrow points from the 'Incoming Filter' field to the 'Outgoing Filter' field. A fifth red arrow points from the 'Outgoing Filter' field to the 'Address List' field. A sixth red arrow points from the 'Address List' field to the 'Interface List' field. A seventh red arrow points from the 'Interface List' field to the 'DNS Server' field. An eighth red arrow points from the 'DNS Server' field to the 'WINS Server' field. A ninth red arrow points from the 'WINS Server' field to the 'Change TCP MSS' section. A tenth red arrow points from the 'Change TCP MSS' section to the 'Use UPnP' section. A red line is drawn across the 'Local Address' and 'Remote Address' fields.

PPP Profile <MumBog>

General Protocols Limits Queue Scripts

Name: MumBog

Local Address: 192.168.12.1

Remote Address: VPNPool

Bridge: bridge1

Bridge Port Priority:

Bridge Path Cost:

Bridge Horizon:

Incoming Filter:

Outgoing Filter:

Address List:

Interface List:

DNS Server:

WINS Server:

Change TCP MSS

no yes default

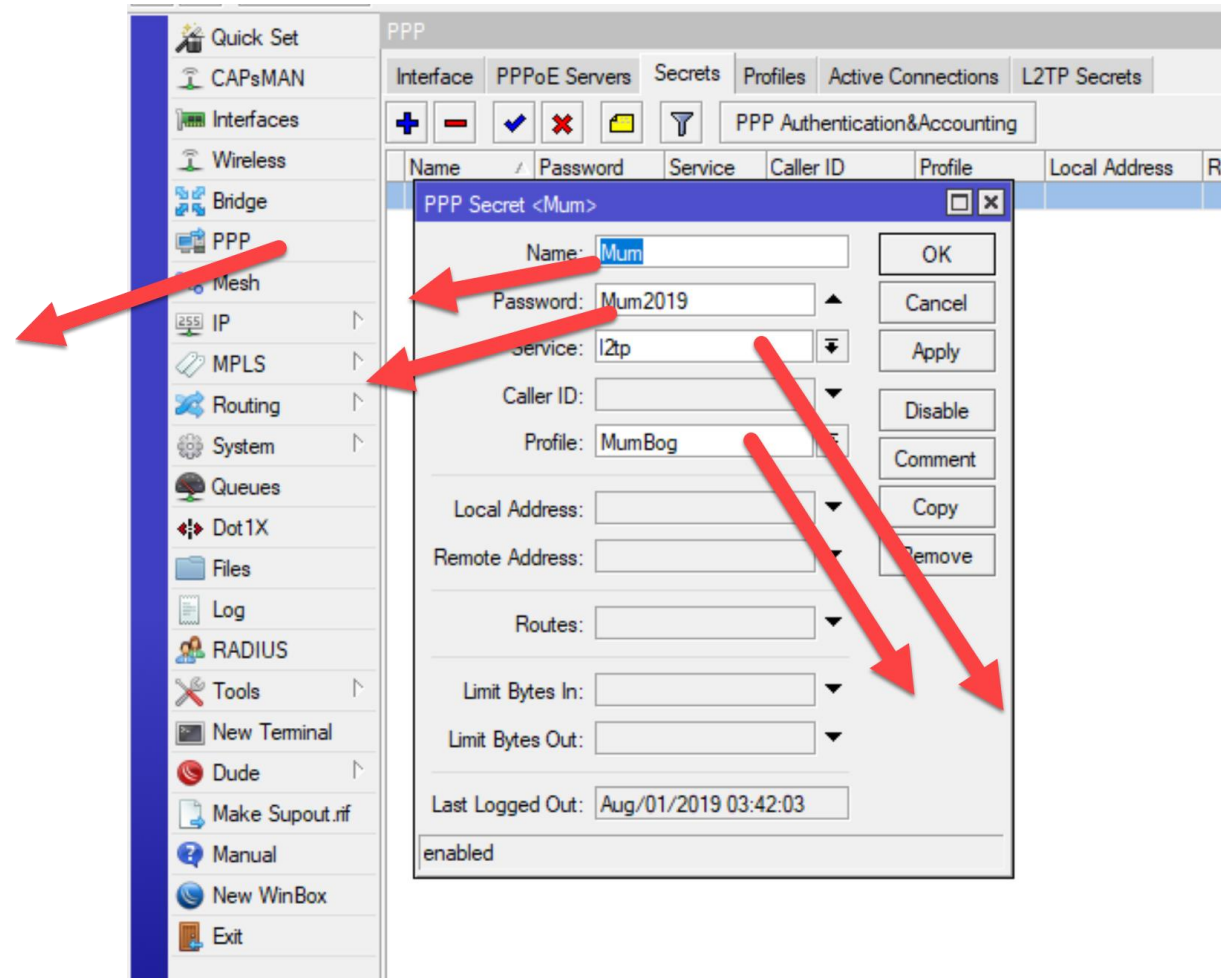
Use UPnP

no yes default

OK Cancel Apply Comment Copy Remove

CREAMOS EL PPP SECRET PARA LAS OFICINAS REMOTAS

- Podemos si deseamos utilizar el mismo secret para todas las oficinas remotas

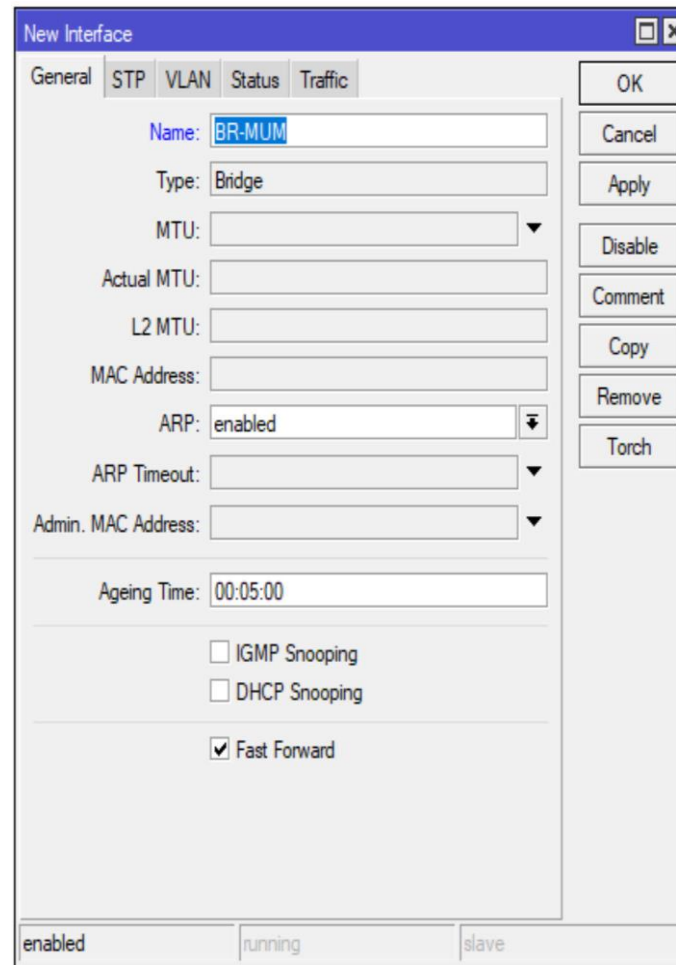




EN LAS OFICINAS
REMOTAS AHORA

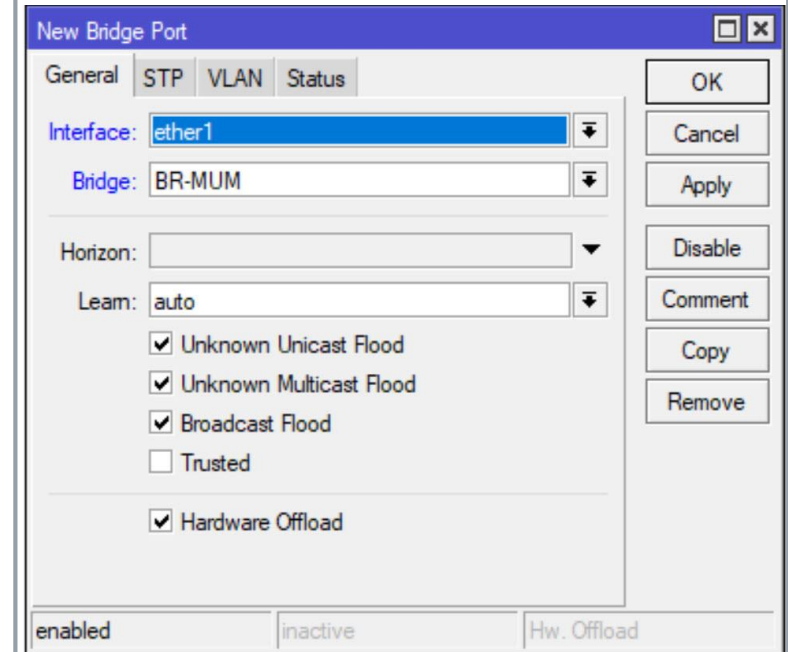
EN LAS OFICINAS REMOTAS

- Creamos el bridge “BR-MUM” y asignamos el Puerto que será miembro de el.



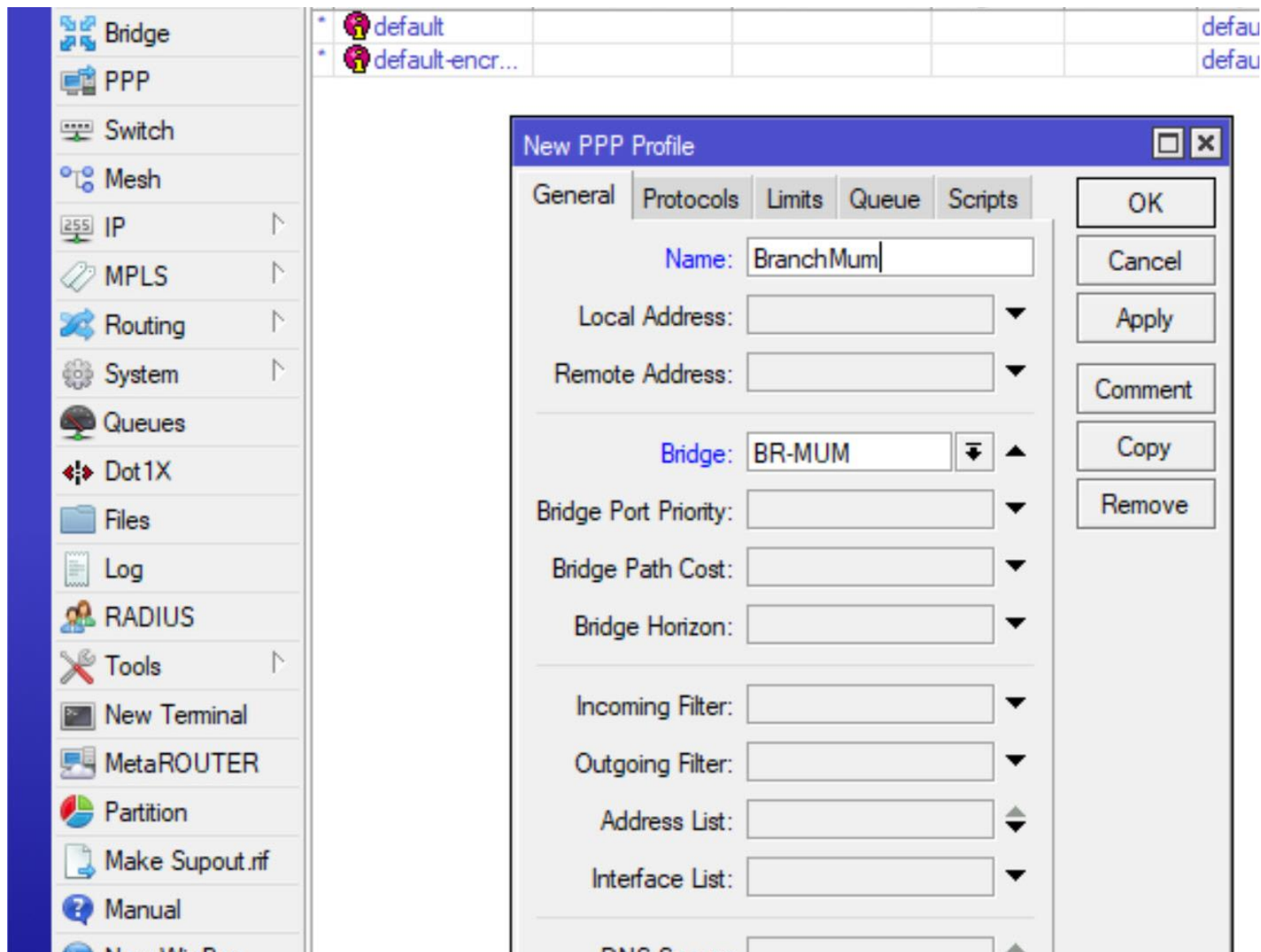
The 'New Interface' window shows the configuration for a new bridge interface. The 'General' tab is active. The 'Name' field is set to 'BR-MUM'. The 'Type' is set to 'Bridge'. The 'MTU' is set to the default value. The 'Actual MTU' and 'L2 MTU' are empty. The 'MAC Address' is empty. The 'ARP' is set to 'enabled'. The 'ARP Timeout' is set to the default value. The 'Admin. MAC Address' is empty. The 'Ageing Time' is set to '00:05:00'. The 'IGMP Snooping' and 'DHCP Snooping' checkboxes are unchecked. The 'Fast Forward' checkbox is checked. The 'Status' bar at the bottom shows 'enabled', 'running', and 'slave'.

General	STP	VLAN	Status	Traffic
Name: BR-MUM				
Type: Bridge				
MTU: [default]				
Actual MTU: [empty]				
L2 MTU: [empty]				
MAC Address: [empty]				
ARP: enabled				
ARP Timeout: [default]				
Admin. MAC Address: [empty]				
Ageing Time: 00:05:00				
☐ IGMP Snooping				
☐ DHCP Snooping				
☒ Fast Forward				
enabled running slave				



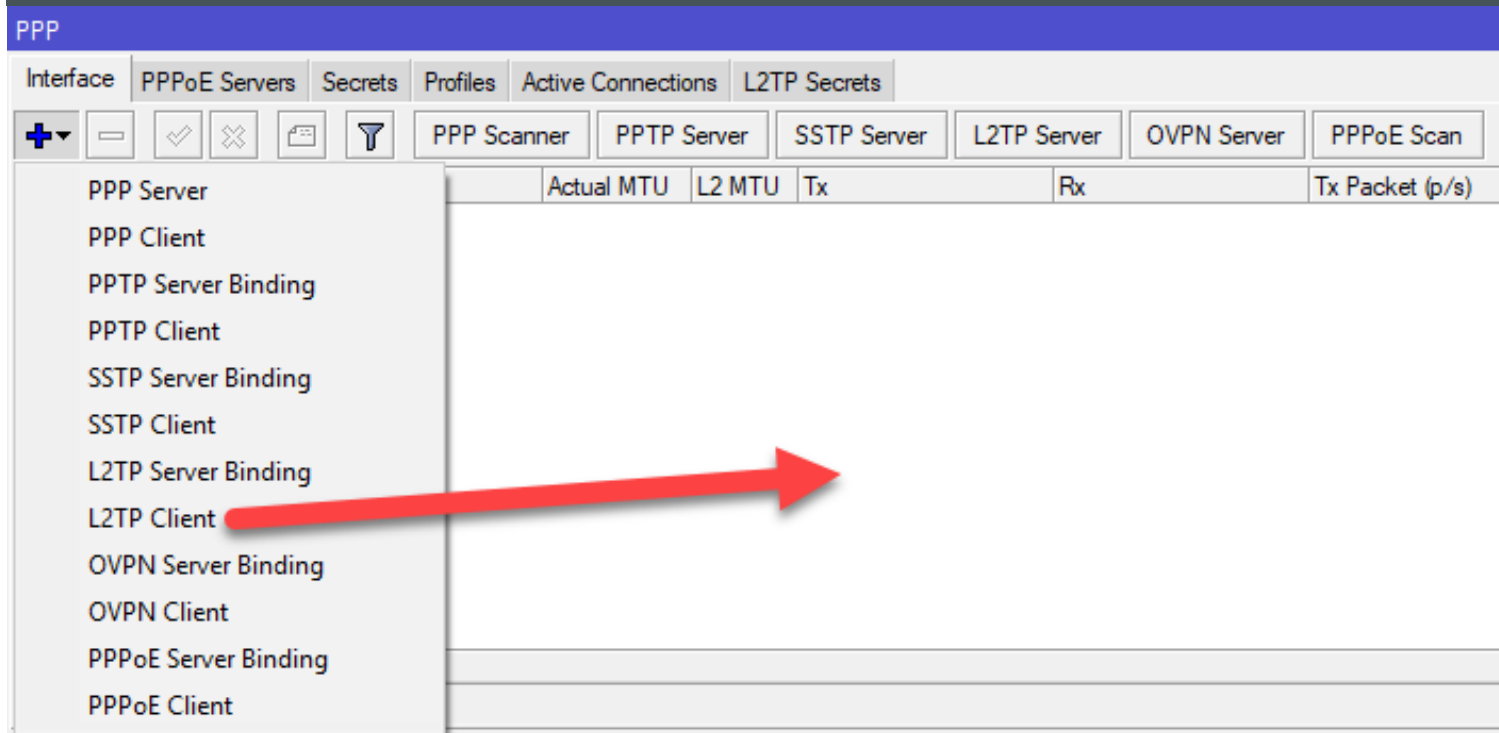
The 'New Bridge Port' window shows the configuration for a new bridge port. The 'General' tab is active. The 'Interface' is set to 'ether1'. The 'Bridge' is set to 'BR-MUM'. The 'Horizon' is set to the default value. The 'Learn' is set to 'auto'. The 'Unknown Unicast Flood', 'Unknown Multicast Flood', and 'Broadcast Flood' checkboxes are checked. The 'Trusted' checkbox is unchecked. The 'Hardware Offload' checkbox is checked. The 'Status' bar at the bottom shows 'enabled', 'inactive', and 'Hw. Offload'.

General	STP	VLAN	Status
Interface: ether1			
Bridge: BR-MUM			
Horizon: [default]			
Learn: auto			
☒ Unknown Unicast Flood			
☒ Unknown Multicast Flood			
☒ Broadcast Flood			
☐ Trusted			
☒ Hardware Offload			
enabled inactive Hw. Offload			



EN LAS OFICINAS REMOTAS

CREAMOS EL PROFILE PPP PARA
CONEXION Y LE ASIGNAMOS
TAMBIEN EL NUEVO BRIDGE
CREADO.



Creamos la interface cliente L2TP con Multi-Link PPP, para conectarnos a la oficina principal

EN LAS OFICINAS REMOTAS

New Interface

General Dial Out Status Traffic

Name: BCPVPN

Type: L2TP Client

Actual MTU:

Max MTU: 1450

Max MRU: 1450

MRRU: 1600

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status:

New Interface

General Dial Out Status Traffic

Connect To: vpn.alfiomunoz.com

User: Mum

Password: Mum2019

Profile: MumBog

Keepalive Timeout: 60

☒ Use IPsec

IPsec Secret: ClaveBienSegura

☐ Allow Fast Path

☐ Dial On Demand

☐ Add Default Route

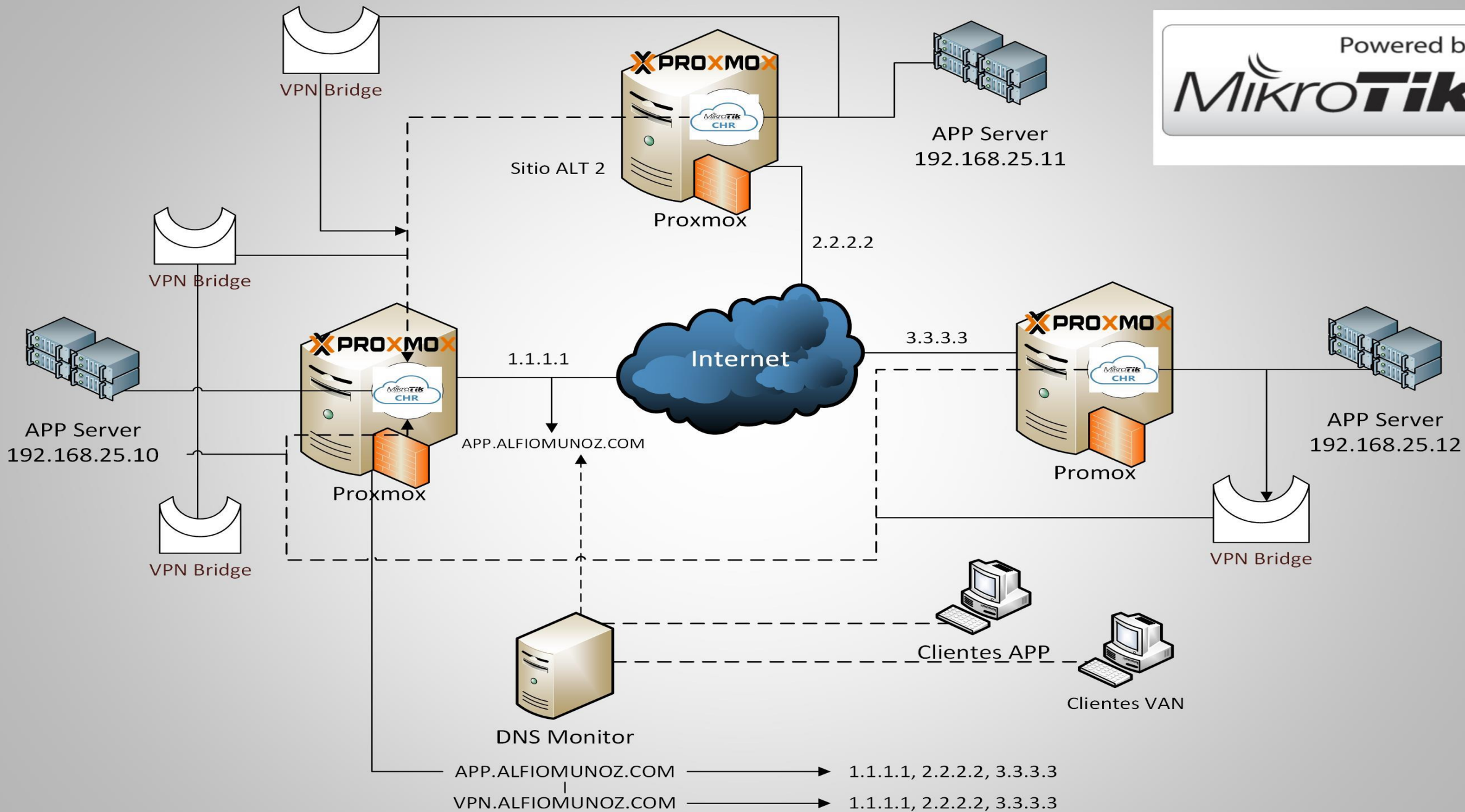
Default Route Distance: 1

Allow: ☒ mschap2 ☒ mschap1 ☒ chap ☒ pap

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave Status:

EN LAS
OFICINAS
REMOTAS



EXPLICACIÓN ESCENARIO FAILOVER AUTOMATICO

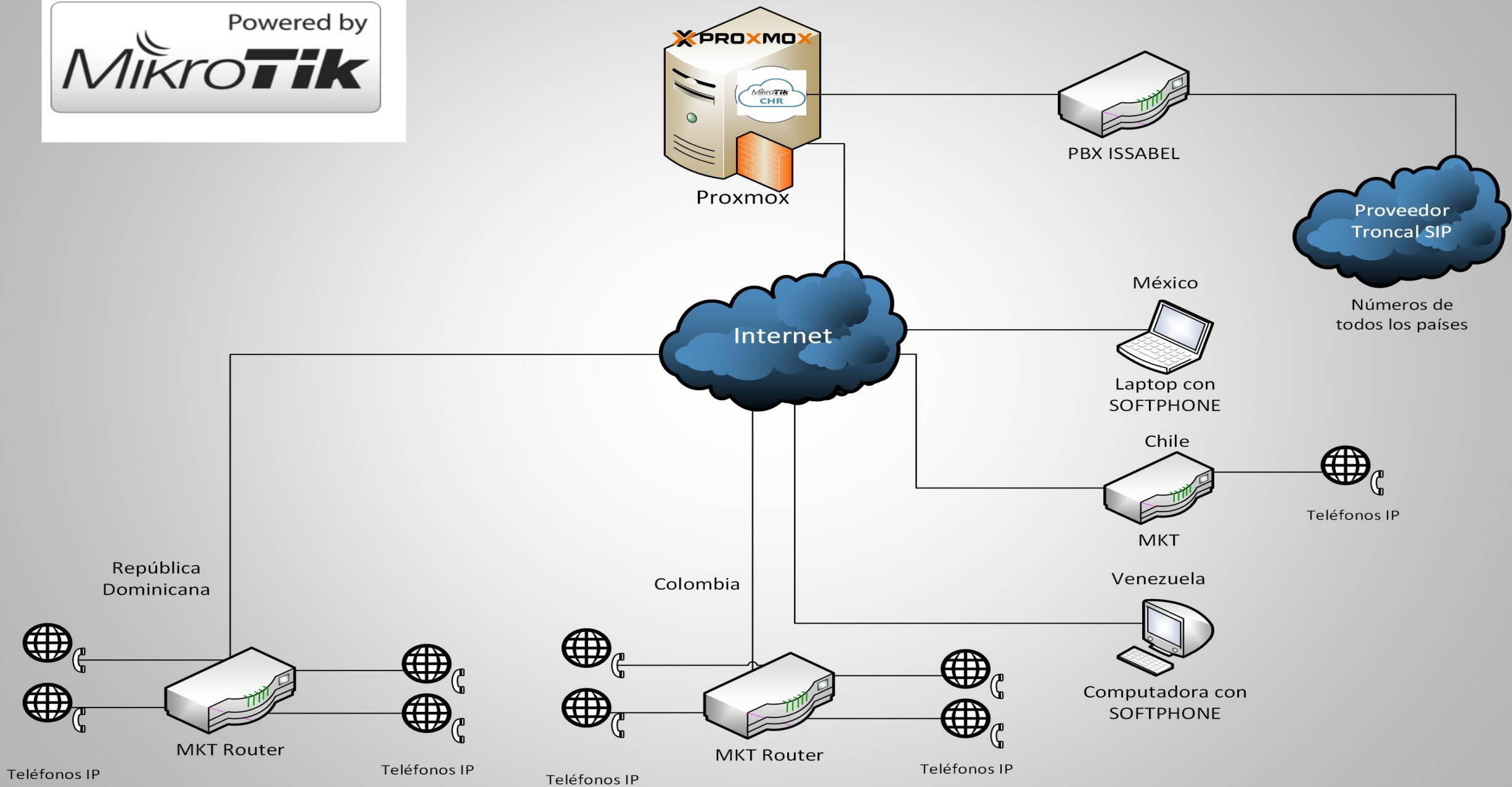
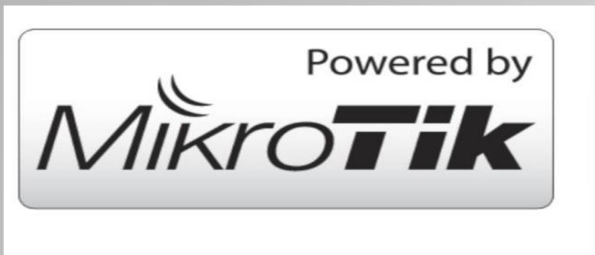
- Mediante el túnel BCP conectamos tres centros de datos iguales donde tenemos Proxmox instalado y hacemos lo siguiente:
- Tenemos una red exclusiva para servidores en el ambiente virtualizado, esa red la tenemos conectada a dos centros de datos alternos mediante los túneles con BCP, las máquinas virtuales replican entre ellas por medio de aplicaciones en tiempo real, es decir bases de datos, etc, entre cada uno de los puntos remotos, todo esto monitoreado por una aplicación de terceros en donde tenemos para cada una de los servidores un IP publico contratado y configurados en el CHR, adicional a esto les tenemos reglas de NAT, port Forwarding, etc para que sean accesibles desde el exterior.
- Site 1 : 1.1.1.1 -----→ 192.168.25.10
- Site 2 : 2.2.2.2 -----→ 192.168.25.11
- Site 3 : 3.3.3.3 -----→ 192.168.25.12
- La aplicación de terceros de monitoreo DNS permite monitorear hasta 4 IP diferentes en donde puede hacer los cambios de IP en caso de que nuestro IP primario sufra una caída. La aplicación automáticamente va a hacer el cambio al site 2 o al site 3 dependiendo las reglas que tengamos configuradas. Ahí entonces el CHR ya tiene el control de acceso de ese sitio y si tenemos VPNs y sitios remotos también van a subir y conectarse al centro alternativo.
- Los sitios remotos y los usuarios VPN estarán conectados al servicio al igual que las aplicaciones antes mencionadas a un nombre de dominio, el cual como habíamos comentado estará asociado a varias IP, es decir todos apuntarán sus servicios a:
- vpn.alfiomunoz.com

TELEFONIA IP SIN PROBLEMAS

- Cluster de centrales, una local y otra en la nube.
- Protocolo SIP muy susceptible a problemas de NAT
- Con esta solución de túnel L2TP/BCP se soluciona el problema del NAT.
- Pueden estar geográficamente separados y siempre se van a comunicar sin problemas.
- Las personas pudieran estar viajando con un mAP lite y ya con eso, su teléfono IP o Softphone se registran sin problemas.
- Soluciona el problema de ataques y vulnerabilidades ya que la PBX no está publicada al mundo exterior

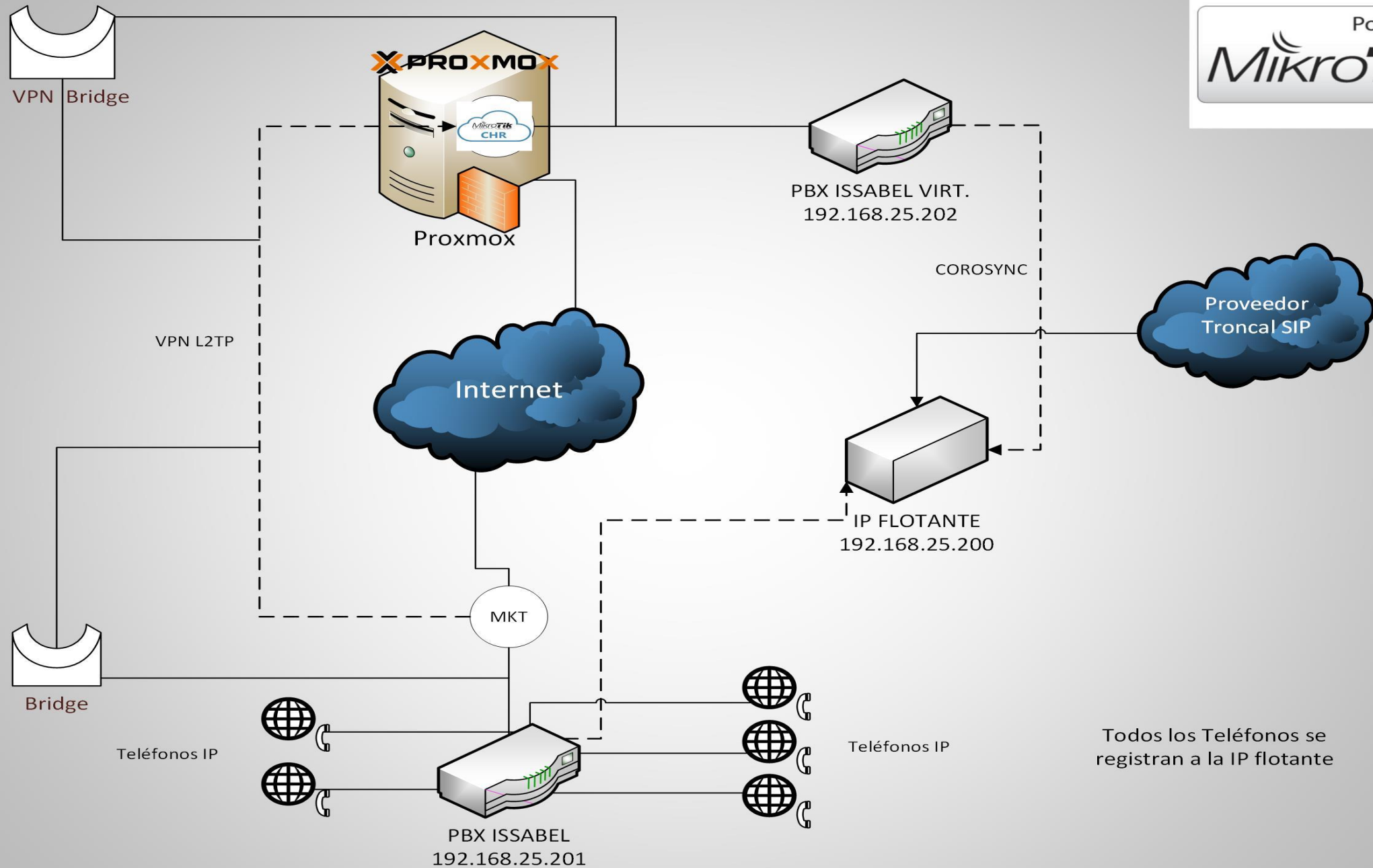
ESCENARIO I DE TELEFONIA IP

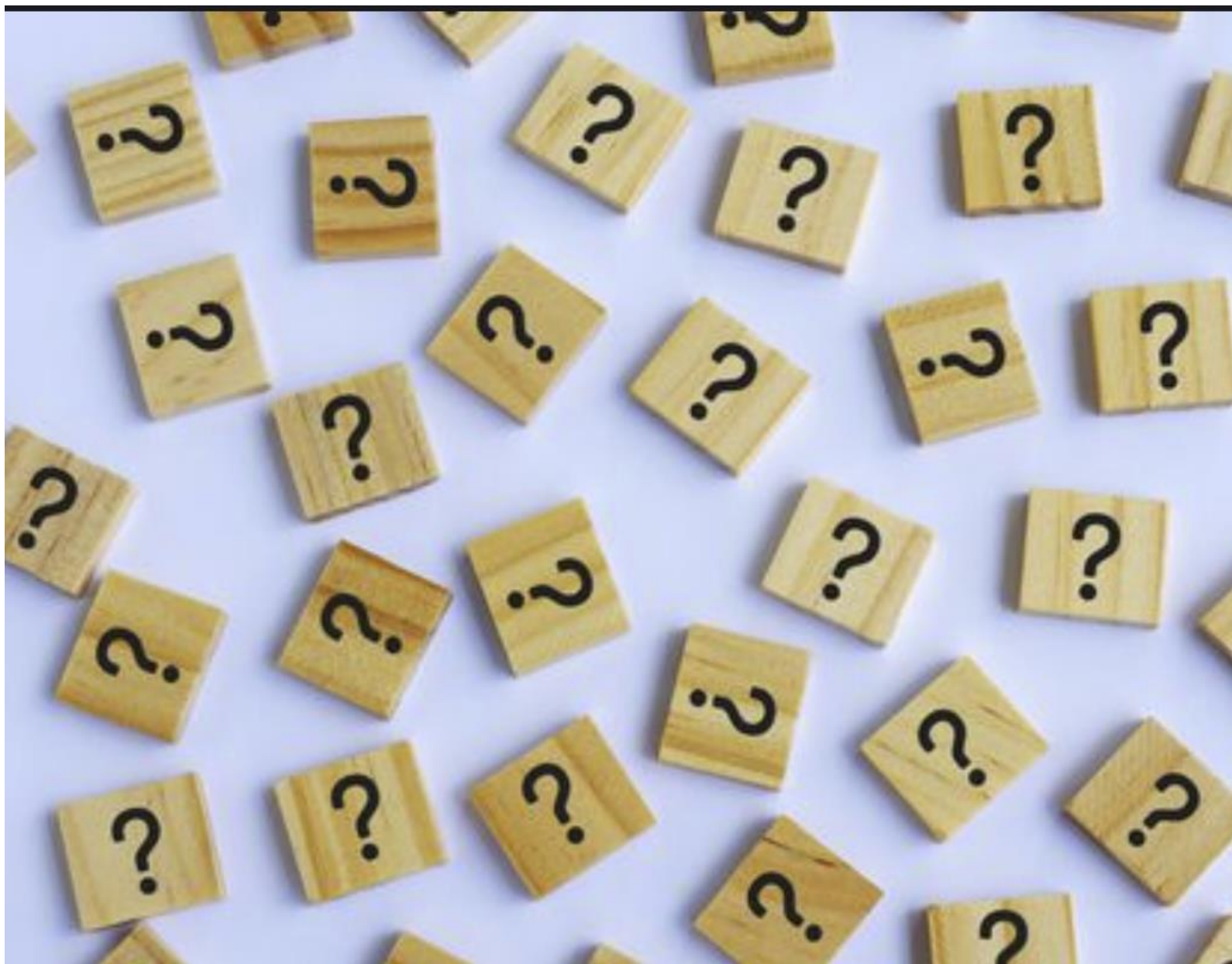
- La Central IP esta en la nube y todos los clientes se conectan remotos



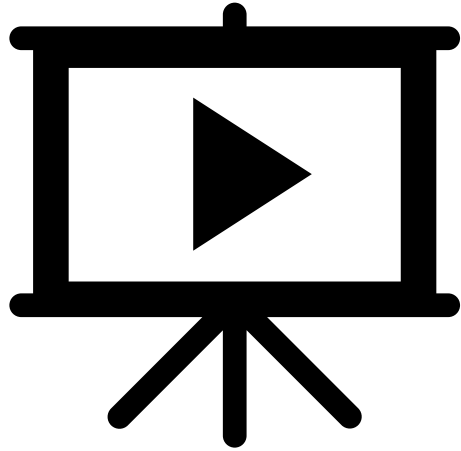
ESCENARIO 2 DE TELEFONIA IP

- Una empresa tiene su Central IP de forma Local y en la Nube tiene un respaldo en caso de desastres





PREGUNTAS?



Gracias por su atención



Alfio Muñoz

alfiomunoz@gmail.com

alfio@issabel.com

Twitter. alfiomunoz

Facebook. Alfio Muñoz

Skype. alfiomunoz

<https://t.me/IssabelPBXip>