Optimix
NETWORK CONSULTING

Gestión de Redes remotas apoyado en VPNs+BGP+Dude

Ing. Jorge Daniel Filippo

info@optimix.com.ar

Objetivos Optimix NETWORK CONSULTING

- Proveer estrategias de red monitoreadas para estar siempre un paso adelante.
- Capacitar a las redes administradas, para que puedan resolver la operación diaria.
- Ser un aliado intelectual ayudando desde la vanguardia del conocimiento.
- Simplificar, resumir, aclarar, divertir.

Objetivos de esta exposición

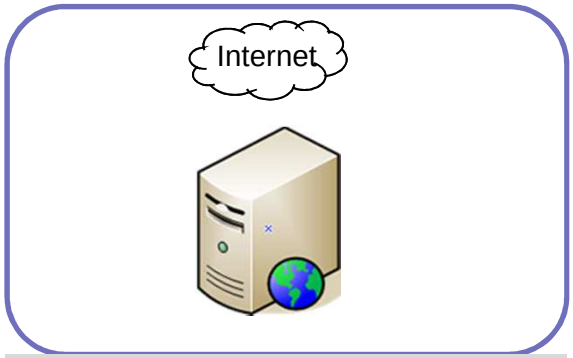
- Analizar el valor del monitoreo en la reputación del consultor MikroTik.
- Comprender el potencial de poseer redes con ruteo bidireccional, para múltiples funcionalidades.
- Brindar un panorama de los elementos que componen el operar redes remotas (VPNs).
- Analizar una configuración en producción de ruteo bidireccional con BGP interno, para acceso remoto.

Visibilidad bidireccional

- A pesar de que el tráfico IP siempre es bidireccional, no siempre lo es la visibilidad IP entre los participantes de la red.
- La visibilidad bidireccional IP entre los participantes de una red, implica que se puedan **iniciar** conexiones desde y hacia cualquier participante.
- Las configuraciones con `nat` o `masquerade`, tradicionalmente resultan funcionalmente en permitir solo conexiones que fluyen en un solo sentido.

Recursos detrás de NAT

*Domicilio**B***



Servidor con IP pública
190.1.1.172

*Domicilio**A***

LAN privada
10.210.12.0/24

*Domicilio**C***

PC con IP pública
200.7.7.14

Panorama VPN

- Las VPNs nos permiten posicionar (virtualmente) nuestra PC adentro de otra red remota. A nivel IP, es como si la PC estuviese dentro de dicha red.
- La presencia IP se logra al conectarse al router remoto, y adquirir en dicha conexión una IP de esa red.
- Cuando un router MikroTik es el que se conecta a una VPN, la situación es más compleja: la de un router conectado a otro router.
- La interconexión por VPN de routers, permite que las dos redes se vean entre si, de forma bidireccional. Así, desde una red de NOC, podremos administrar (y monitorear) todas las redes que administramos, simultáneamente.

Optimix
NETWORK CONSULTING

Ruteo e Interfaces Punto-A-Punto

Túneles bridgeados o routeados

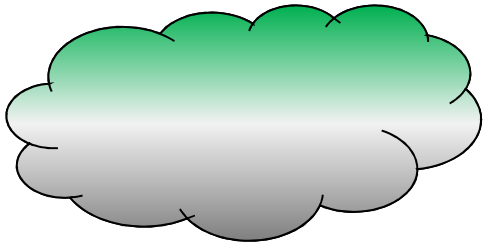
Técnicas punto a punto

- Las técnicas de túneles punto a punto para interconexión IP, incluyen los protocolos estándares PPP (PPTP, L2TP, SSTP, etc…), y los protocolos dedicados IPIP y EoIP.
- Cuando tenemos una conexión IP con otro router, podemos:
  - Mediante un túnel bridgeable, unir ambas zonas en un mismo entorno de broadcast.
  - Mediante un túnel ruteable, comunicar ambas zonas por ruteo (en capa 3), aislándolas en capa 2, segmentando en redes.

Interconexión bridgeada

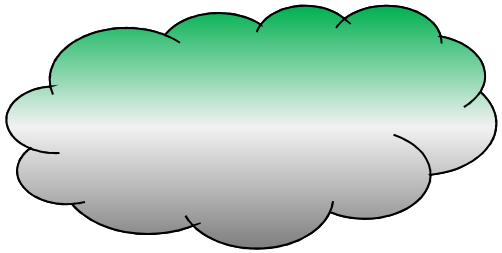
- *Domicilio**A***

  192.168.**0**.1/24 - 192.168.**0**.128/24



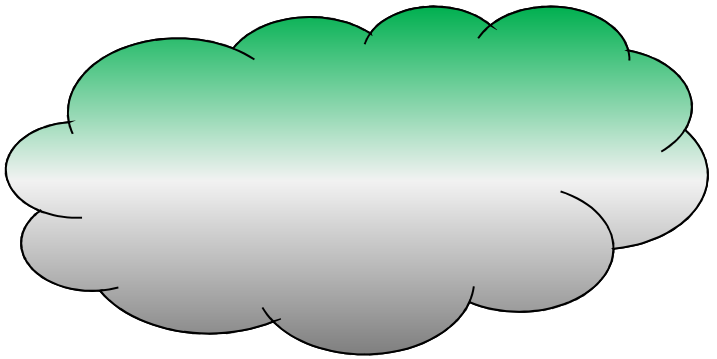
- *Domicilio**B***

  192.168.**0**.129/24 - 192.168.**0**.254/24



- *Red resultante **A**+**B***

  192.168.**0**.1/24 - 192.168.**0**.254/24



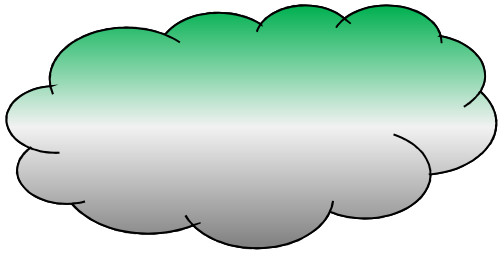
Interconexión bridgeada

- Se suele implementar mediante túneles EoIP, que se bridgean con el ethernet.
- La topología general se simplifica. Todo se visualiza como una única LAN.
- Es inviable si las redes pertenecen a distintos dueños, dado que existe visibilidad promiscua entre ambas (ej: carpetas compartidas de Windows).

Interconexión ruteada

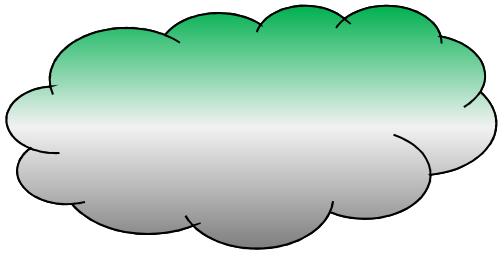
- *Domicilio**A***

  192.168.**0**.1/24 - 192.168.**0**.254/24



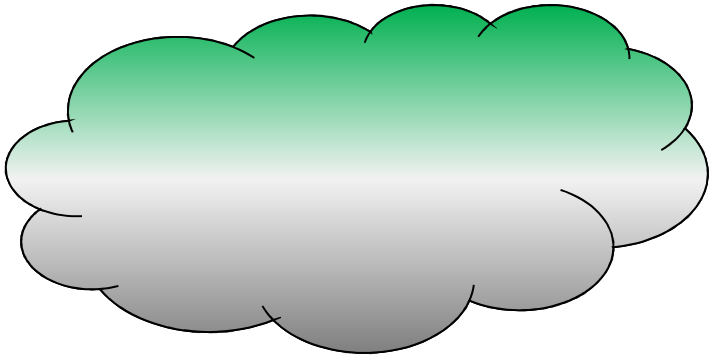
- *Domicilio**B***

  192.168.**1**.1/24 - 192.168.**1**.254/24



- *Red resultante **A**+**B***

192.168.**0**.1/24 -192.168.**0**.254/24
192.168.**1**.1/24 -192.168.**1**.254/24



Interconexión ruteada

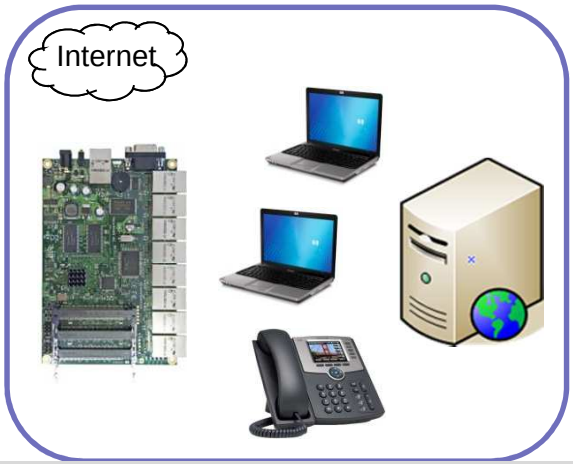
- Tradicionalmente requiere rutas estáticas, que crecen exponencialmente a cada nueva red que se agrega.
- La contrapartida es conectarse una vez a cada VPN, y desconectarse para conectarse a la siguiente.
- La alternativa simplista de iniciar múltiples VPNs desde una PC, carece de control, solidez, y estabilidad.

Interconexión ruteada con BGP

- La interconexión de domicilios por VPNs ruteadas, ofrece escalabilidad ilimitada porque no se intercambia tráfico broadcast.
- La utilización de BGP permite difundir toda nueva zona planteada en la comunidad, automáticamente.
- Incluso, si no se quiere que algunas zona puedan iniciar conexiones a otras (o para priorizar el uso de un vínculo a otro), se pueden definir más controles mediante filtros de ruteo.

Concepto de uso

*Domicilio**B***

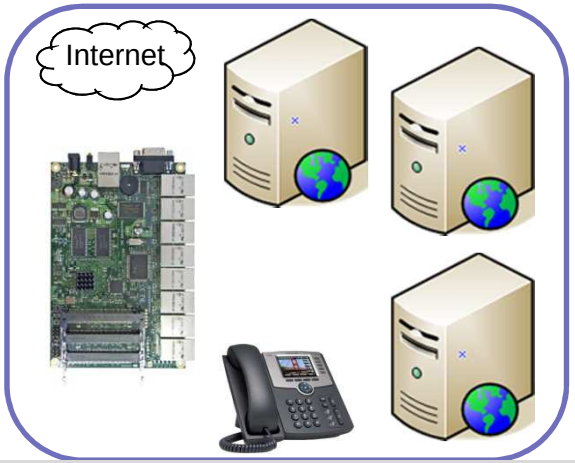


LAN **10.210.16.0/24**

*Domicilio**A***

LAN **10.210.12.0/24**

*Domicilio**C***



LAN **10.210.20.0/24**

Nueva gestión – Ahora podemos:

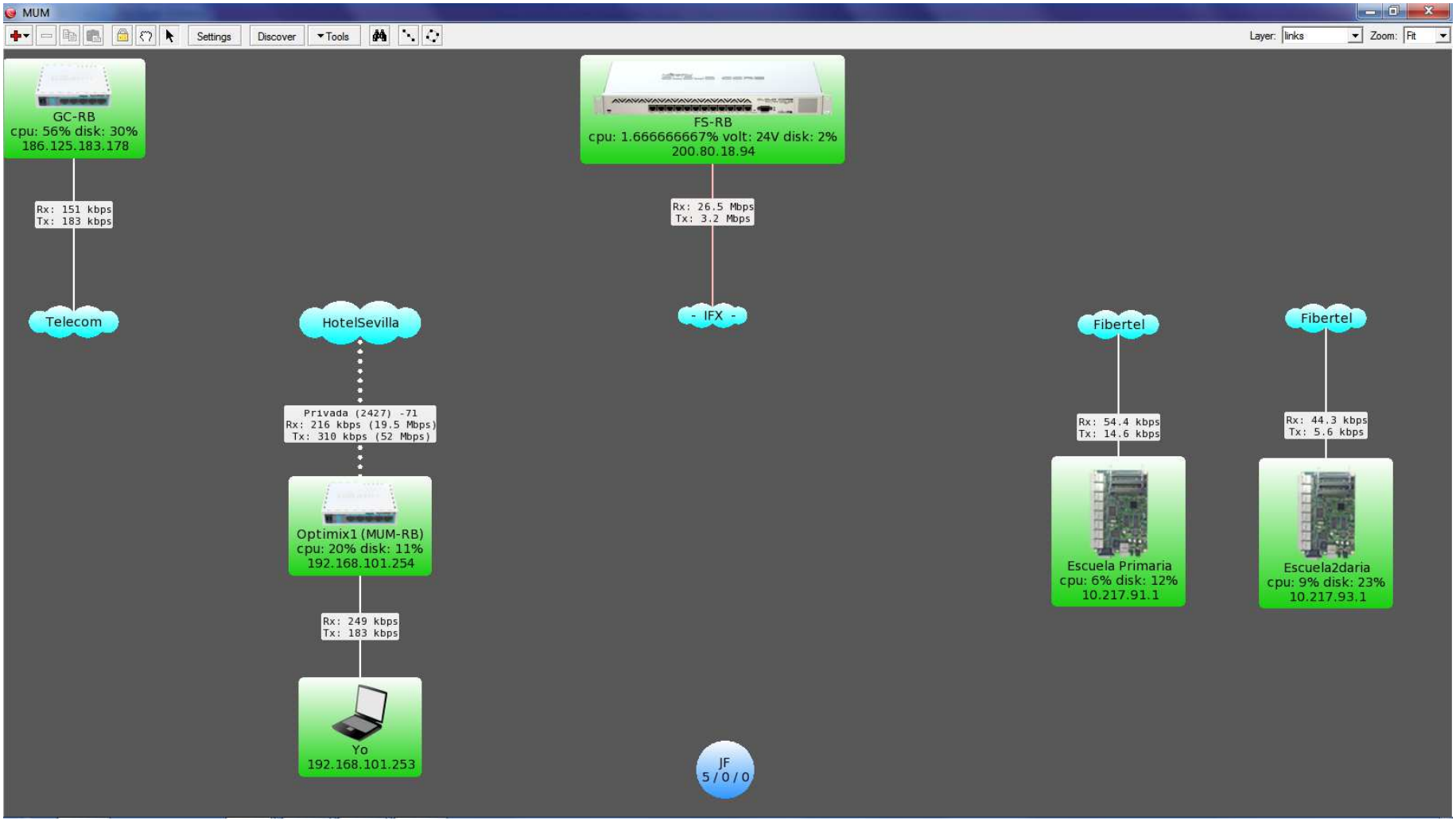
- Auditar quién se conecta a qué recurso, porque podemos conocer la IP origen de cada recurso de red.
- Regular quién puede conectarse a dónde, según su IP origen (usuarios MikroTik).
- Implementar telefonía IP sin necesidad de asignarle una IP pública a nuestra central telefónica.
- Implementar un servidor de emails interno, para backups MikroTik, Voicemails Asterisk, alarmas de red, o Intranet.
- Monitorear todas nuestras redes sin esfuerzo. Incluso, si el Dude está en nuestra notebook, cuando visitamos una red, seguimos viendo todas las demás!
- No tenemos que conectar nuestra notebook explícitamente a VPNs, evitando interrupciones (y demoras) en nuestra gestión.

Optimix
NETWORK CONSULTING

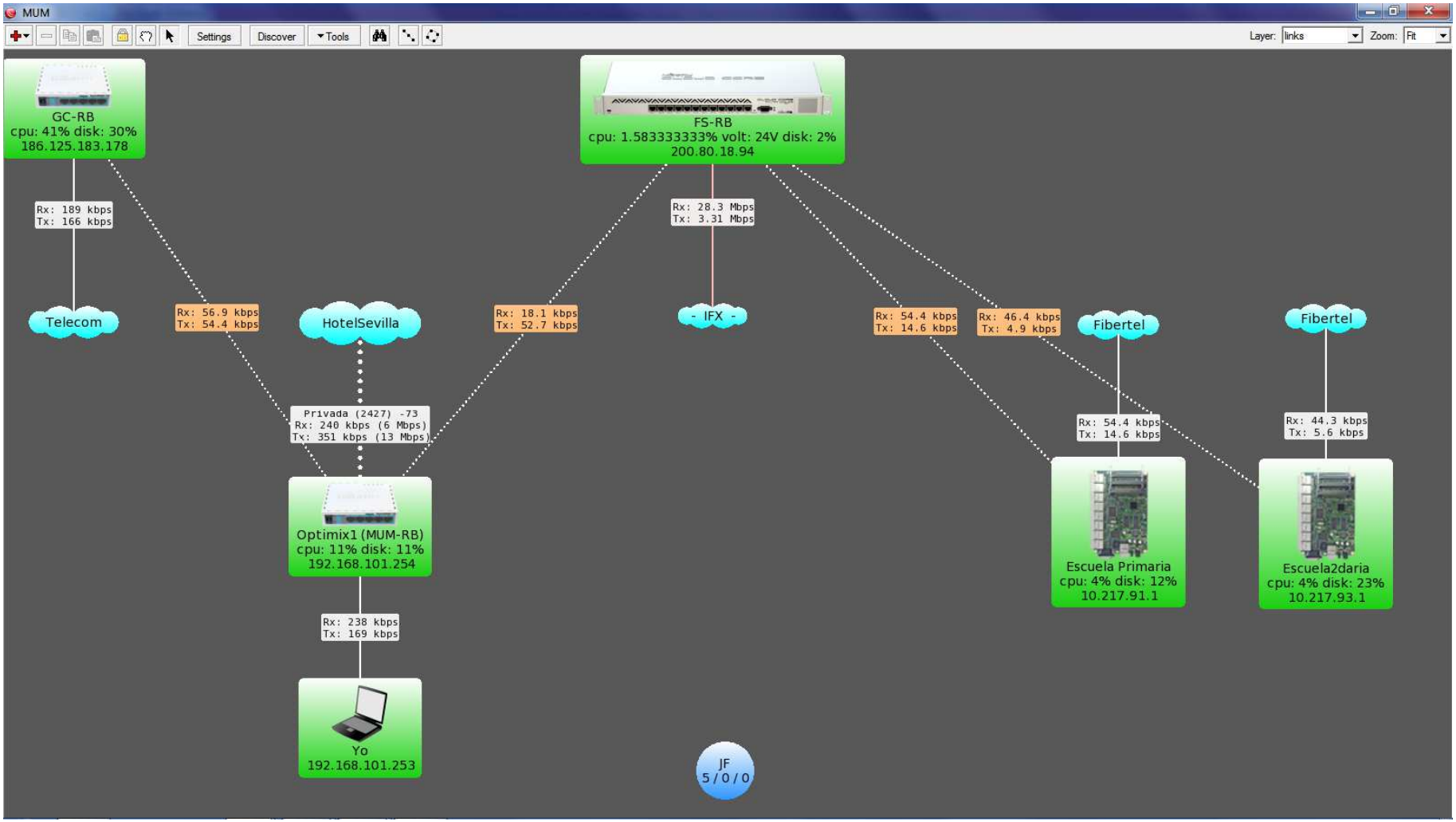
Online!

En este instante…

Recursos conectados a Internet



Interconectados por SSTP y PPTP



Análisis

- Con qué IP origen vemos la conexión al Router Escuela?
- Y si necesitamos/queremos conocer desde dónde se nos conectan?
- La ausencia de Masquerade evita adulteraciones de la IP origen, pero podemos conectarnos?
- Cómo logramos que el tráfico pueda ir y volver por los túneles?: publicando redes!

Optimix
NETWORK CONSULTING

Gracias!

Ing. Jorge Daniel Filippo