HablaIP
Integración & Desarrollo

Tips & Tricks to connect to a Layer2 IXP

MUM Chile 2019

MikroTik

HablaIP
Integración & Desarrollo

Agenda

- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- Filtros de seguridad mínimos
- Tips para Layer2
- Q & A

HablaIP
Integración & Desarrollo

Quien les habla

- **Jaime Cruz M.** **<jaime.cruz@hablaip.com>**
  - Integrador de sistemas con más de 10 años de experiencia en Redes IP, telecomunicaciones, Sistemas Linux, Mikrotik, Asterisk y telefonía IP.

MikroTik MTCNA | MikroTik MTCTCE | MikroTik MTCUME | MikroTik MTCRE

  - Interconnection Strategy en IXP Pit Chile.

HablaIP
Integración & Desarrollo

Agenda

- **Introducción**
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- Filtros de seguridad mínimos
- Tips para Layer2
- Q & A

HablaIP
Integración & Desarrollo

Introducción

- Que es un IXP?

  Un PIT o Punto de Intercambio de Tráfico (IXP Internet eXchange Point en inglés) es una instalación donde se intercambian los datos entre diferentes redes de diferentes proveedores y consumidores de internet.

  Es decir, un PIT permite interconectar directamente (algunas de) las redes que conforman el internet.

HablaIP
Integración & Desarrollo

Introducción

- Que es un IXP?
  - Esquema tradicional

    Con un proveedor de Internet.

HablaIP
Integración & Desarrollo

Introducción

- Que es un IXP?

  - Esquema tradicional

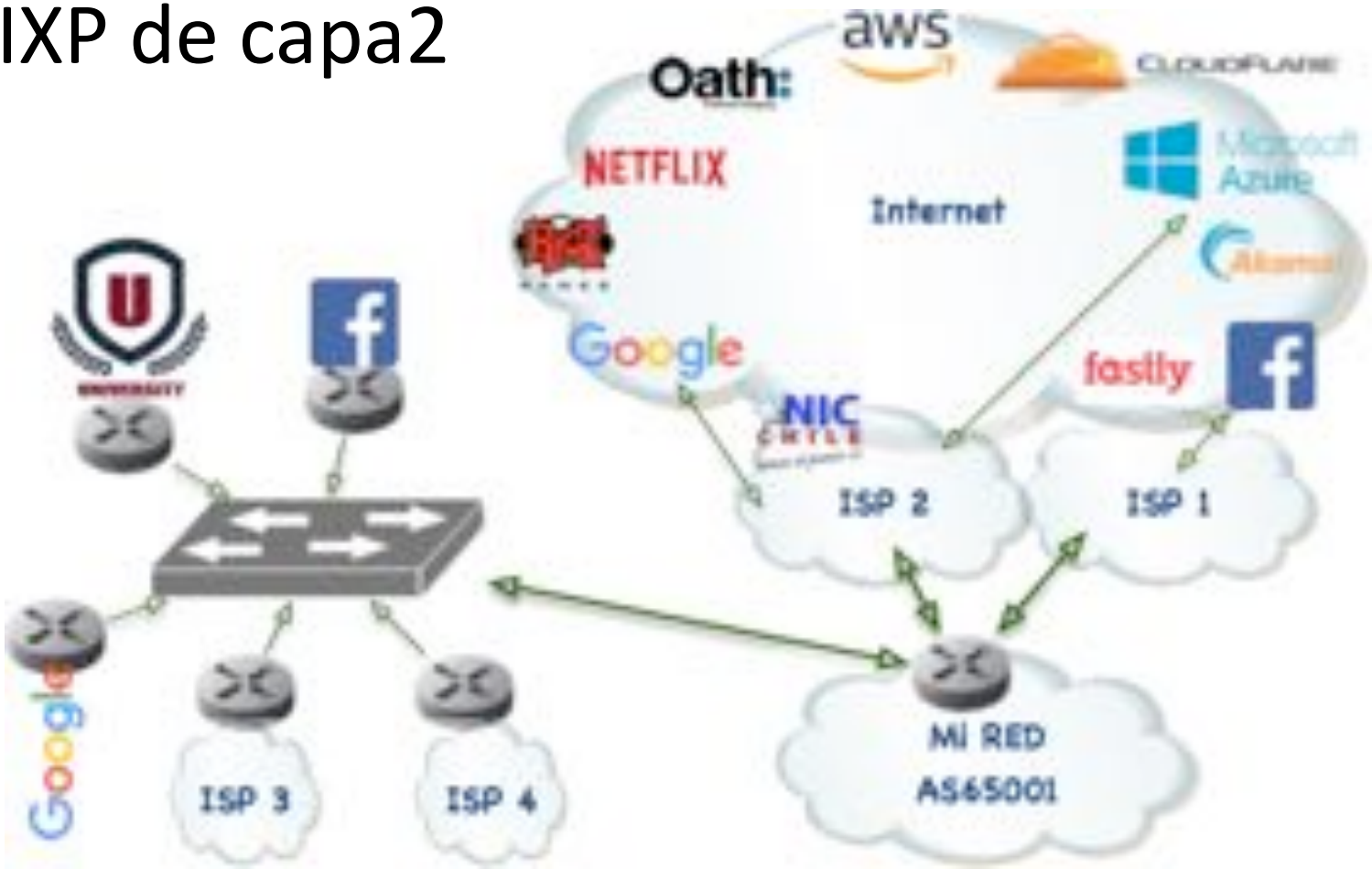
    Con /dos/ proveedores

    De Internet.

HablaIP
Integración & Desarrollo

Introducción

- Un IXP de capa2



HablaIP
Integración & Desarrollo

Introducción

- IXP/PIT's en Chile: (según Subtel)

- PIT Claro Chile
- PIT Entel
- PIT Level3
- PIT Intercity
- PIT NAP Chile
- PIT Orange
- PIT Telefónica Mundo
- PIT Chile
- PIT Tecnoera
- PIT Concepción

L2

Valparaiso

L2

L2

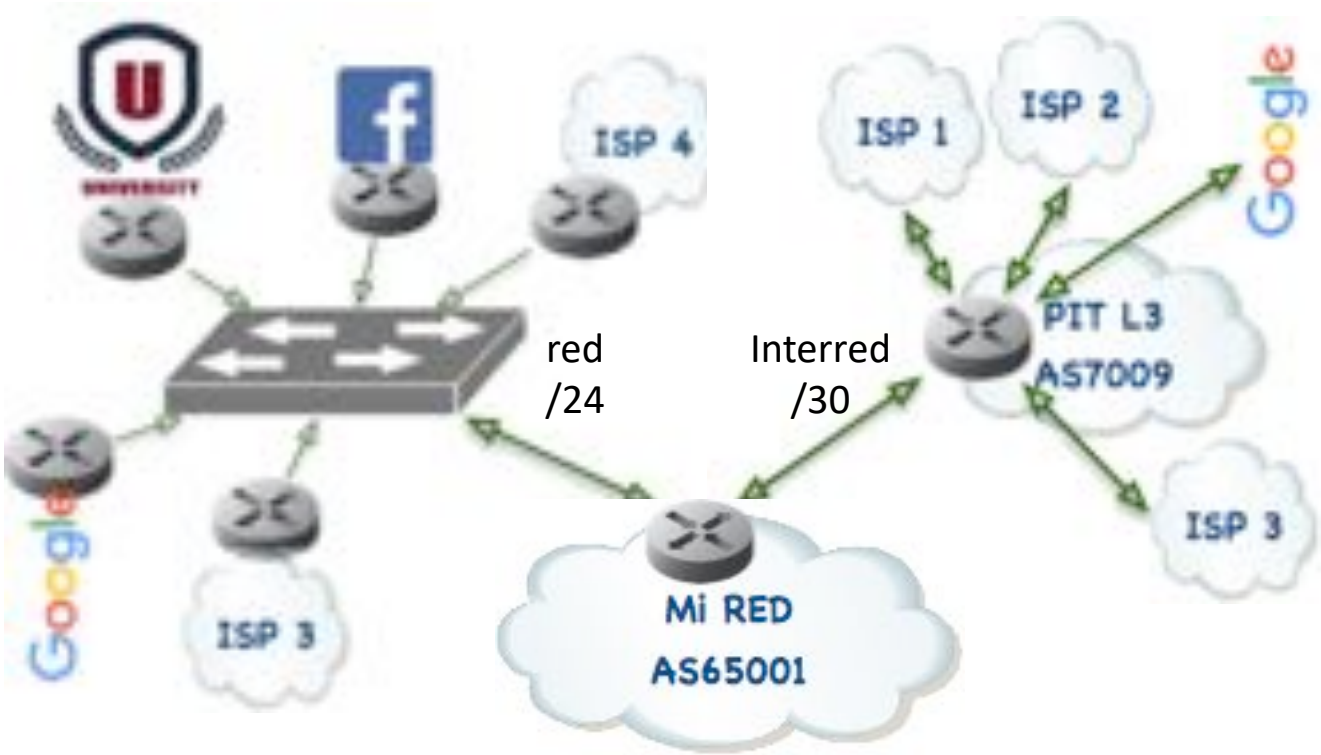
(fuente: https://www.subtel.gob.cl/normativa-tecnica-internet)

HablaIP
Integración & Desarrollo

Introducción

- Diferencia entre IXP Layer3 v/s Layer2

Los PIT en capa2 ofrecen conectividad total y libre entre sus miembros.



HablaIP
Integración & Desarrollo

Introducción

- Requisitos para conectar a un IXP.
  - Contar con recursos IPv4/IPv6
    - Minimo /24 en IPv4.
  - Contar con un ASN (número autónomo)
  - Solicitarlos en LACNIC para Latinoamerica
    - www.lacnic.net
  - Contar con equipamiento de red que soporte BGP4. ←Mikrotik ;-)

HablaIP
Integración & Desarrollo

Introducción

- Que es un ASN (Sistema Autonomo)?
  - Conjunto de redes administrado por una misma entidad, que a su vez tiene autonomía en internet.
  - Entidades de gobierno, financieras, universidades, proveedores de internet, etc.
  - Ej. SII(AS15208), Codelco(AS52226), BancoChile(AS22975), U.Chile(AS23140), GTD(AS14259), etc.

(fuente: https://bgp.he.net)

HablaIP
Integración & Desarrollo

Introducción

Que es un BGP4?

- Protocolo de enrutamiento de borde o /exterior/
- Conecta diferentes Sistemas Autónomos
- Utiliza el puerto tcp/179

- Internet es un conjunto de sistemas autónomos que hablan BGP.

HablaIP
Integración & Desarrollo

Agenda

- Introducción
- **creando peers BGP4**
- Filtros BGP (in & out)
- Usando Comunidades BGP
- Filtros de seguridad mínimos
- Tips para Layer2
- Q & A

HablaIP
Integración & Desarrollo

Mikrotik en el borde

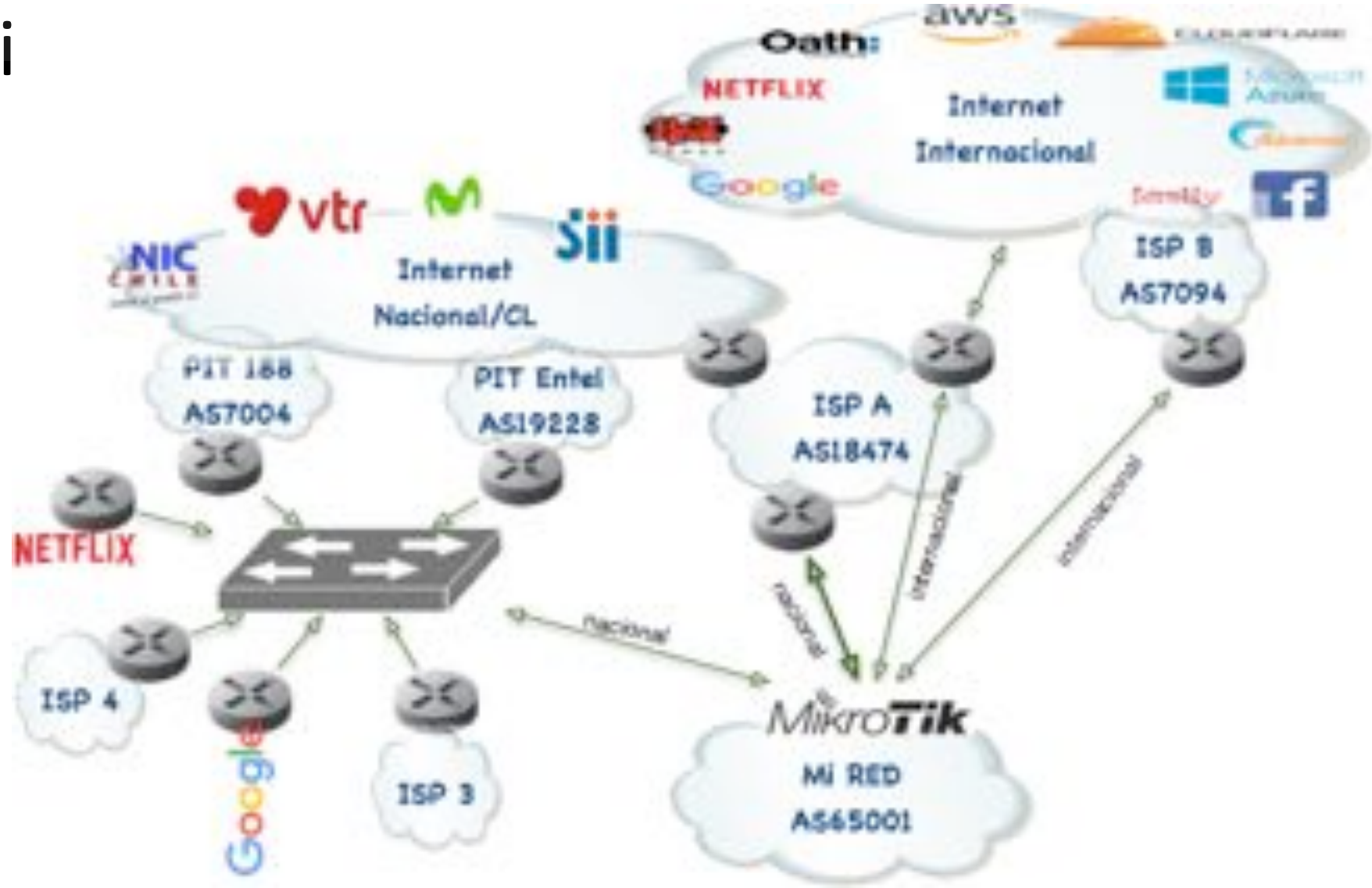
- Ejemplo de organización conectada a dos ISP's y un PIT.
  - RED a conectar: AS65001
  - ISP A: AS18474 nac. e inter.
  - ISP B: AS7094 inter.
  - PIT CL: AS61522

HablaIP
Integración & Desarrollo

Mikrotik en el borde

HablaIP
Integración & Desarrollo

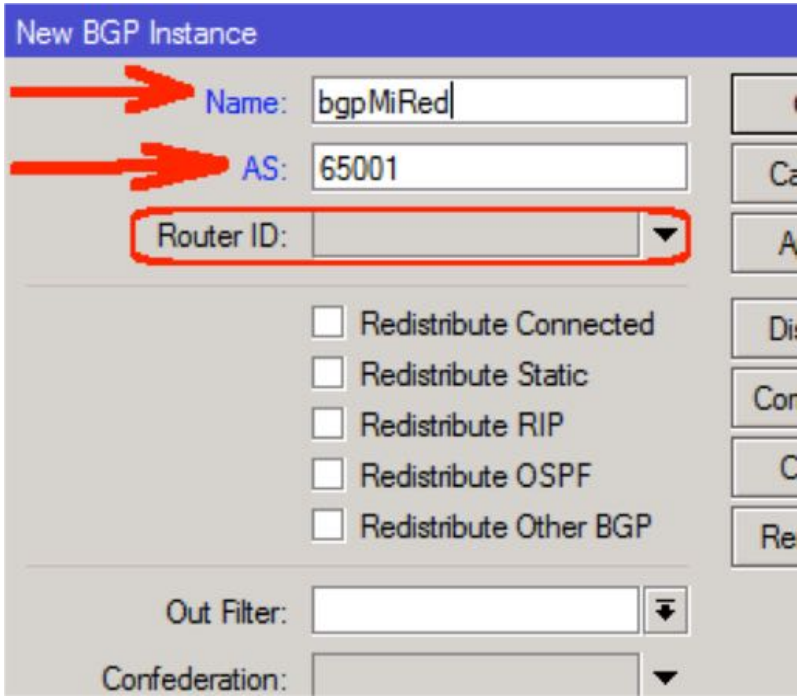
Mi



HablaIP
Integración & Desarrollo

Creando peers BGP4

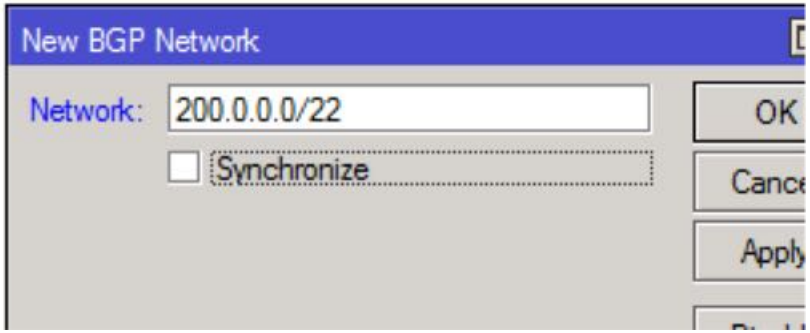
- Crear una “Instancia BGP”
- Routing->BGP->Instance-> +
  - Nombre descriptivo
  - ASN local es 65001
  - RouterID opciones
  - “redistribute XXXXX”

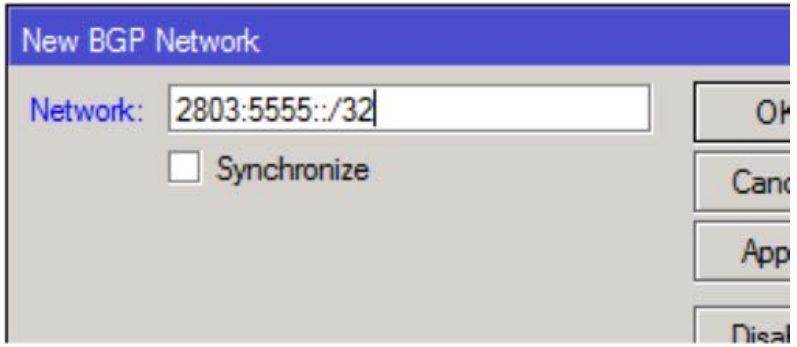


HablaIP
Integración & Desarrollo

Creando peers BGP4

- Definir la redes a anunciar
- Routing->BGP->Networks-> +
  - Requisito contar con IPv4 y/o IPv6

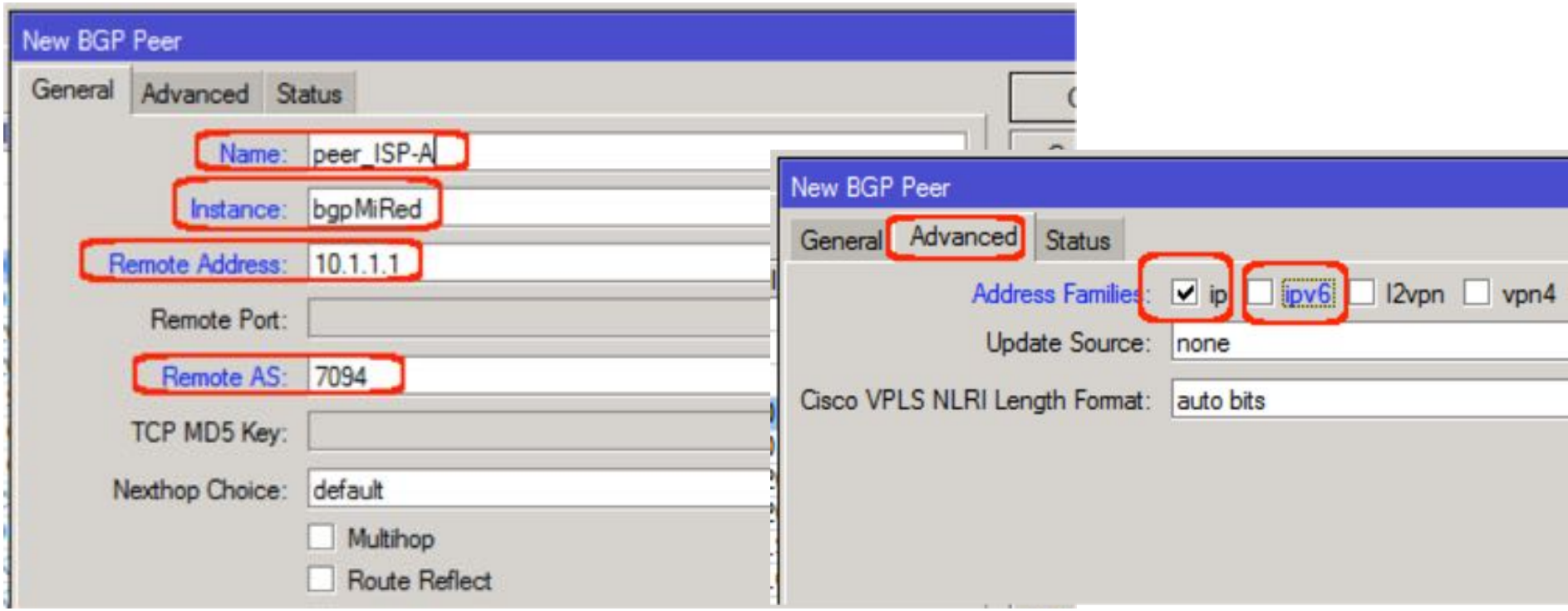




HablaIP
Integración & Desarrollo

Creando peers BGP4

- Crear un Peer BGP
- Routing->BGP->Peers -> +
  - Requisitos: ip y asn remoto (10.1.1.1/30 AS7094)



HablaIP
Integración & Desarrollo

Creando peers BGP4

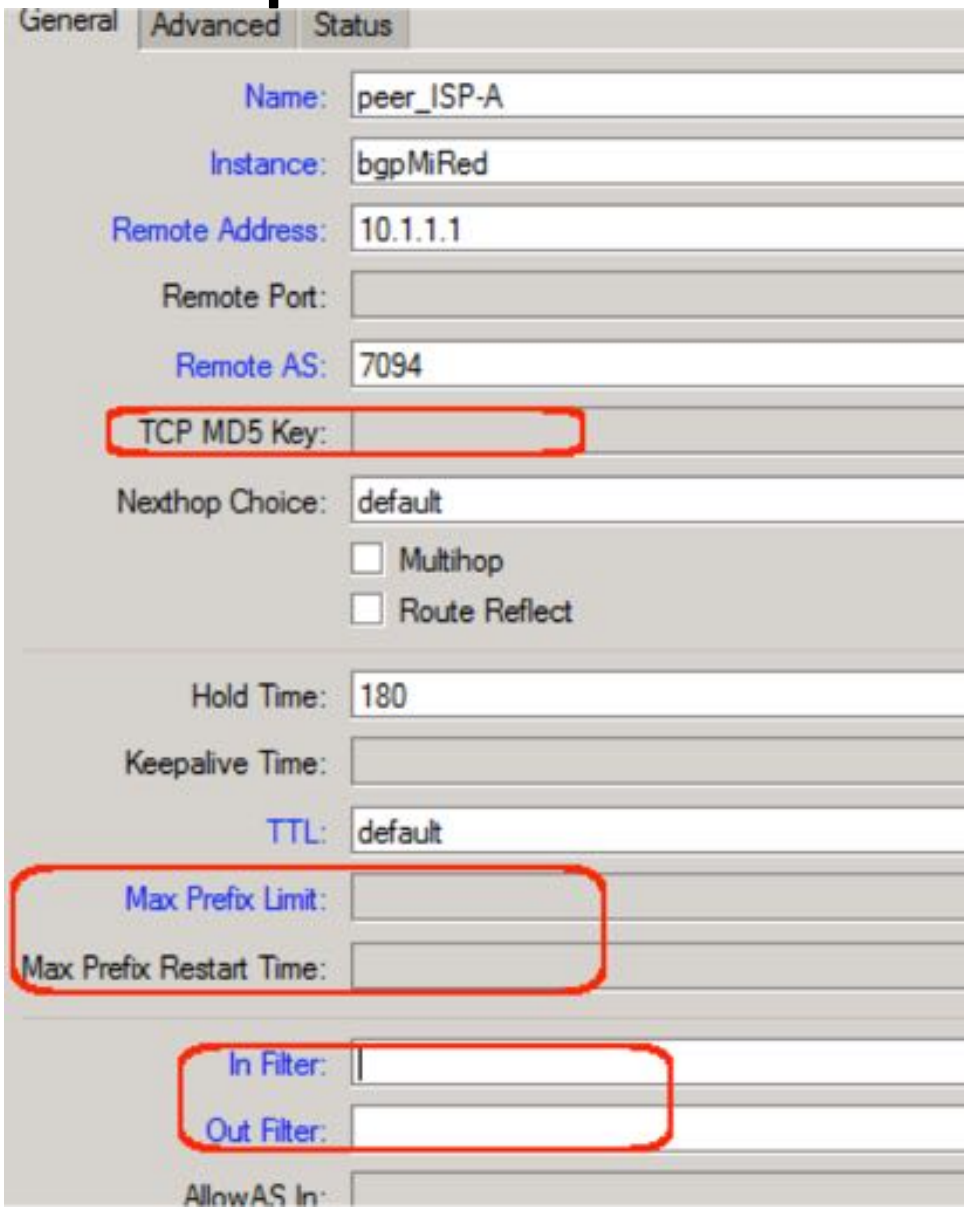
- Ejemplo de visualización de Peers BGP

Nombre	Remotos IP	Remotos ASN		Uptime	Prefix Count	Estado
Pit_PCH-42	200.23.206.220	42	200.23.206.220	8d 11:36:53	127	established
Pit_Microsoft2	200.23.206.211	8075	207.46.32.82	23d 06:58:36	212	established
Pit_Microsoft1	200.23.206.210	8075	207.46.32.81	23d 06:58:33	212	established
Pit_V6_Chile1	2801:14:9000::1	61522	200.23.206.1	88d 05:11:48	235	established
Pit_V6_Chile2	2801:14:9000::2	61522	200.23.206.2	88d 05:11:41	235	established
Pit_Google	200.23.206.225	15169	74.125.251.16	23d 06:57:47	579	established
PitChile1	200.23.206.1	61522	200.23.206.1	18d 22:14:07	5180	established

HablaIP
Integración & Desarrollo

Creando peers BGP4

- Opciones “Peer BGP”
  - Opcion clave MD5
  - Max prefix limit
  - Max Pref. Restart T.
  - In & Out Filter

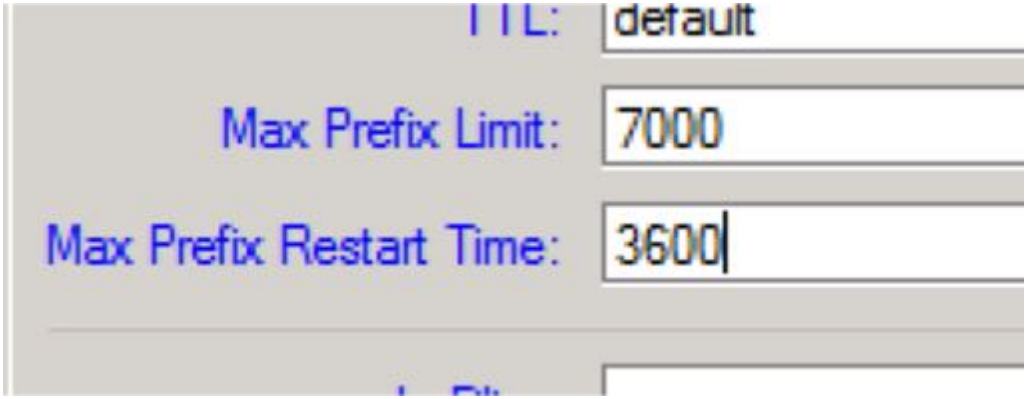


HablaIP
Integración & Desarrollo

Creando peers BGP4

- Opciones “Peer BGP”
  - Max prefix limit ~ por sobre un 20%
  - Max Pref. Restart T. (en segundos)

    0 -> (infinito)



(evitar recibir “escapes” de rutas)

HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

- Diferencias filtro IN v/s OUT
  - Son diferentes a filtros de firewall
  - OUT: Que prefijos publico
  - IN: Que prefijos acepto/filtro

HablaIP
Integración & Desarrollo

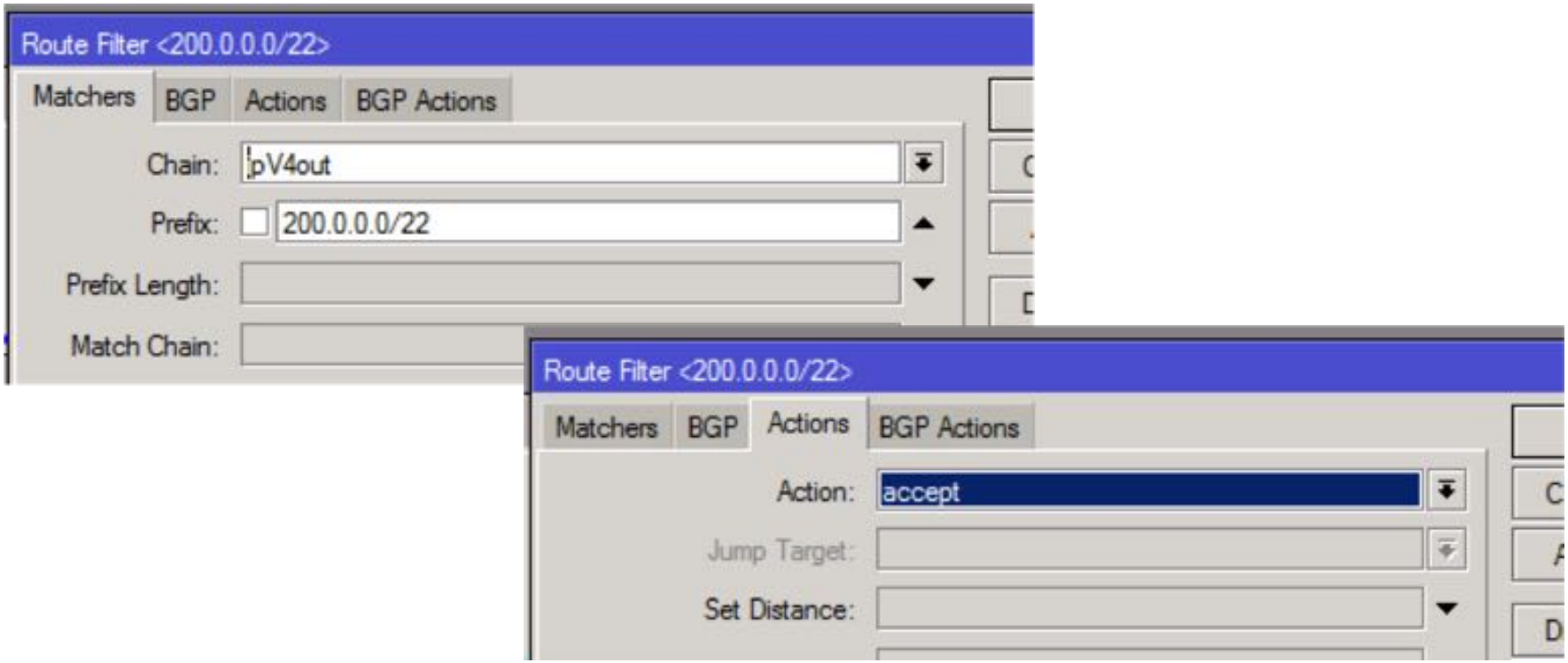
Filtros BGP: IN & OUT

- Filtros OUT:
  - Solo publicar mis prefijos!!!
  - Publicar lo mas sumarizado posible

HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

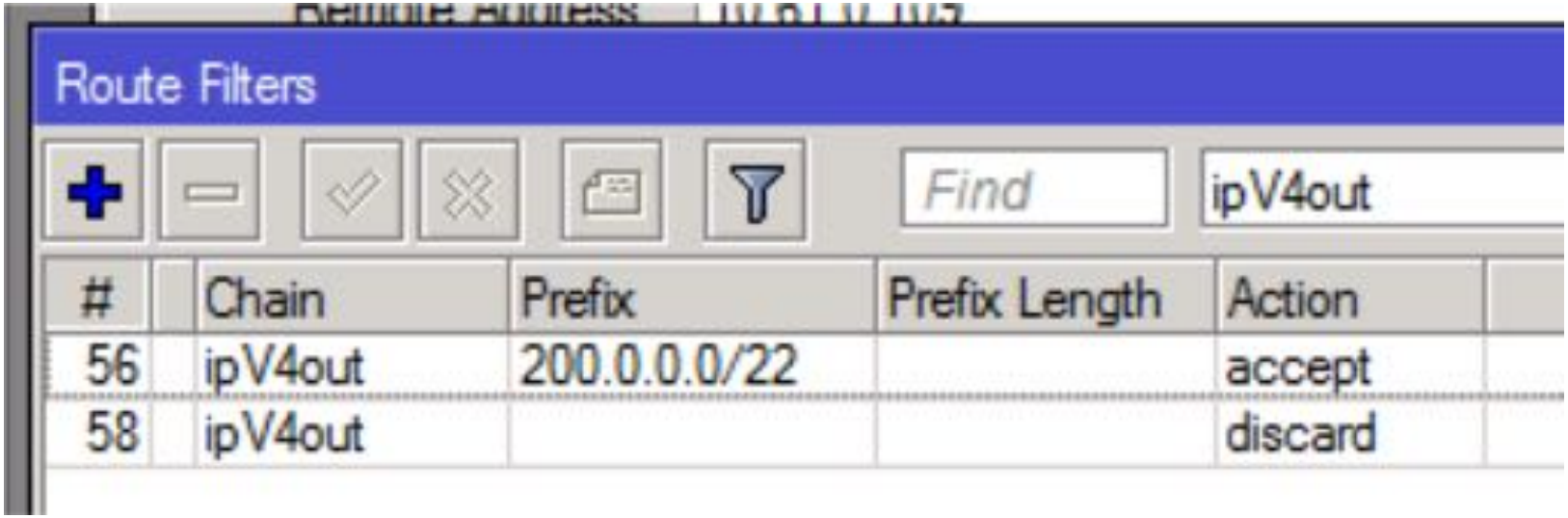
- Filtros OUT: (solo mis prefijos)
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

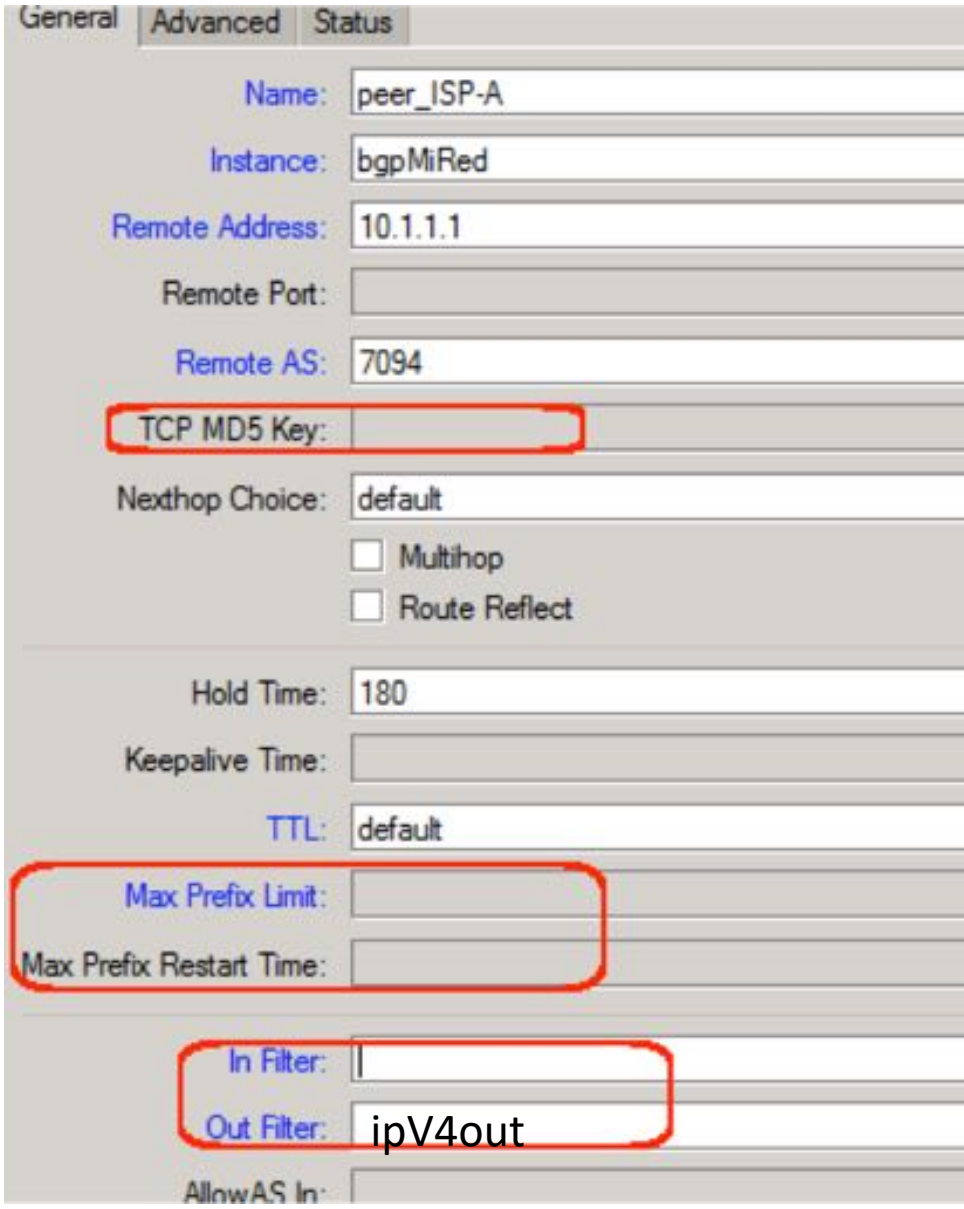
- Filtros OUT: (solo mis prefijos)
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

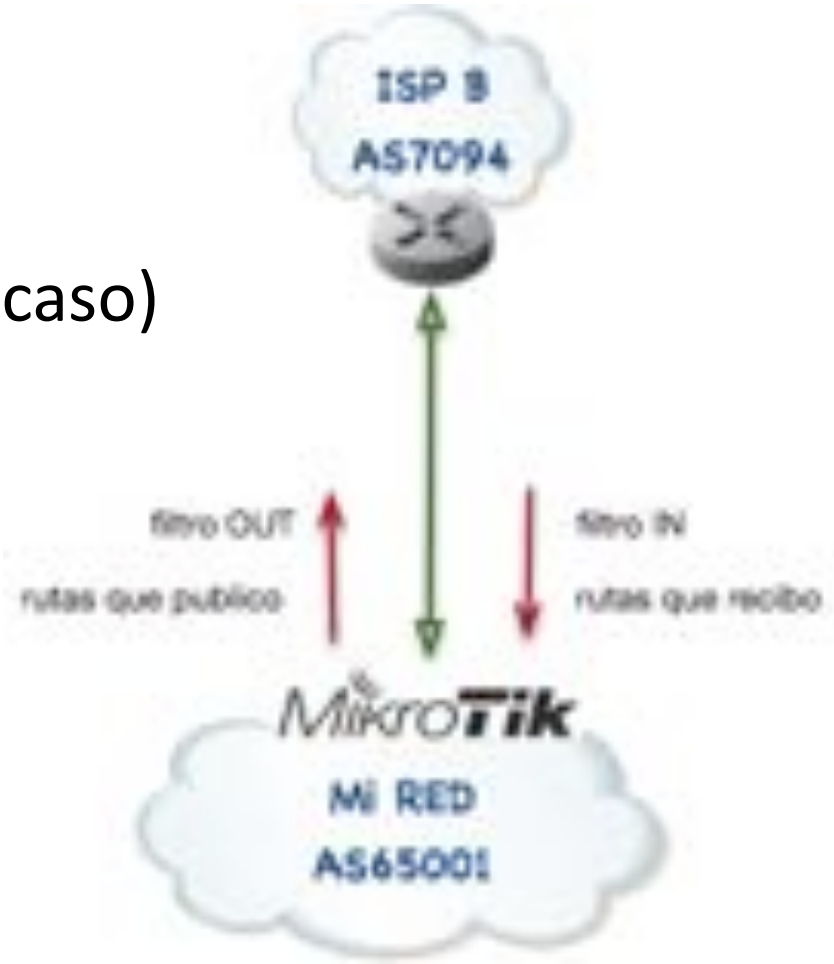
- Filtros OUT: Aplicado al peer BGP.
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

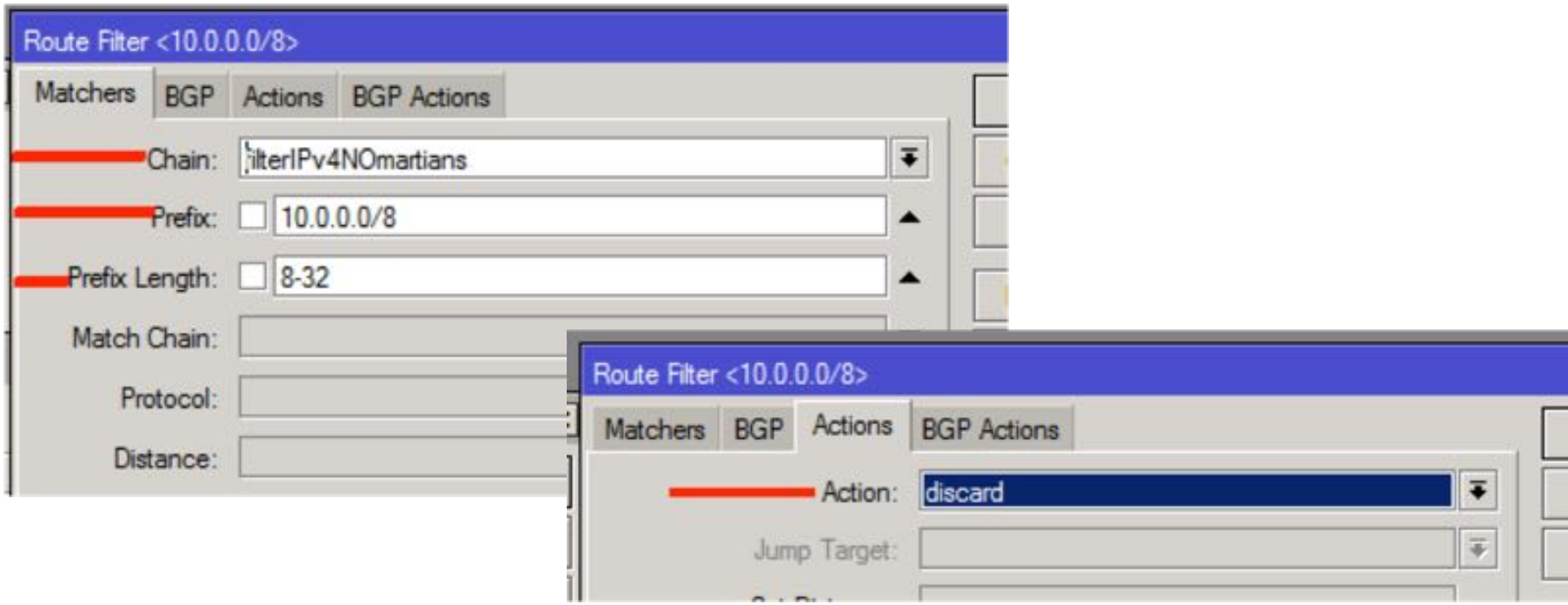
- Filtros IN:
  - Filtrar redes Marcianas!
  - Filtrar la red local
  - Filtrar ruta default (según caso)
  - Filtrar prefijos > /24



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

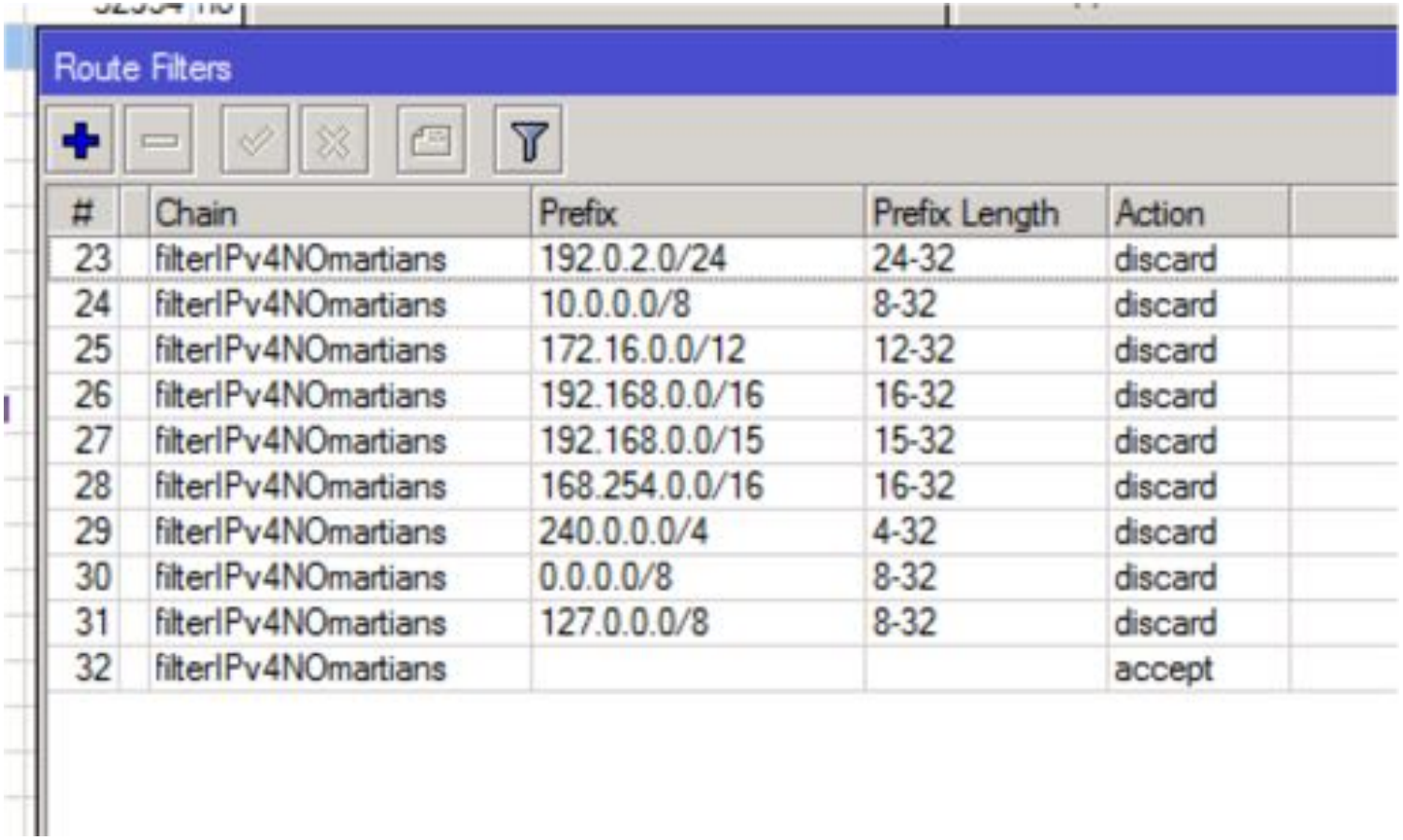
- Filtros IN:
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

- Filtros IN: (Martian Routes)

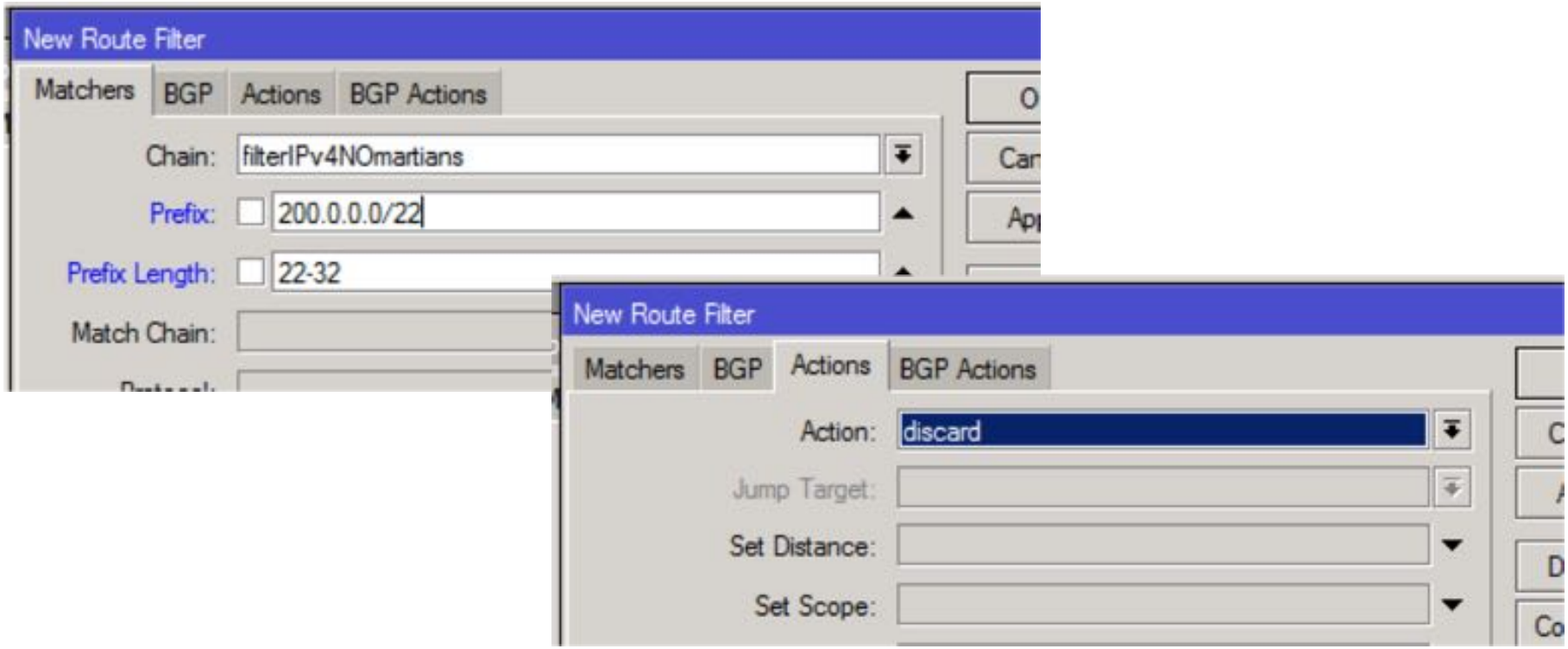


#	Chain	Prefix	Prefix Length	Action
23	filterIPv4NOmartians	192.0.2.0/24	24-32	discard
24	filterIPv4NOmartians	10.0.0.0/8	8-32	discard
25	filterIPv4NOmartians	172.16.0.0/12	12-32	discard
26	filterIPv4NOmartians	192.168.0.0/16	16-32	discard
27	filterIPv4NOmartians	192.168.0.0/15	15-32	discard
28	filterIPv4NOmartians	168.254.0.0/16	16-32	discard
29	filterIPv4NOmartians	240.0.0.0/4	4-32	discard
30	filterIPv4NOmartians	0.0.0.0/8	8-32	discard
31	filterIPv4NOmartians	127.0.0.0/8	8-32	discard
32	filterIPv4NOmartians			accept

HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

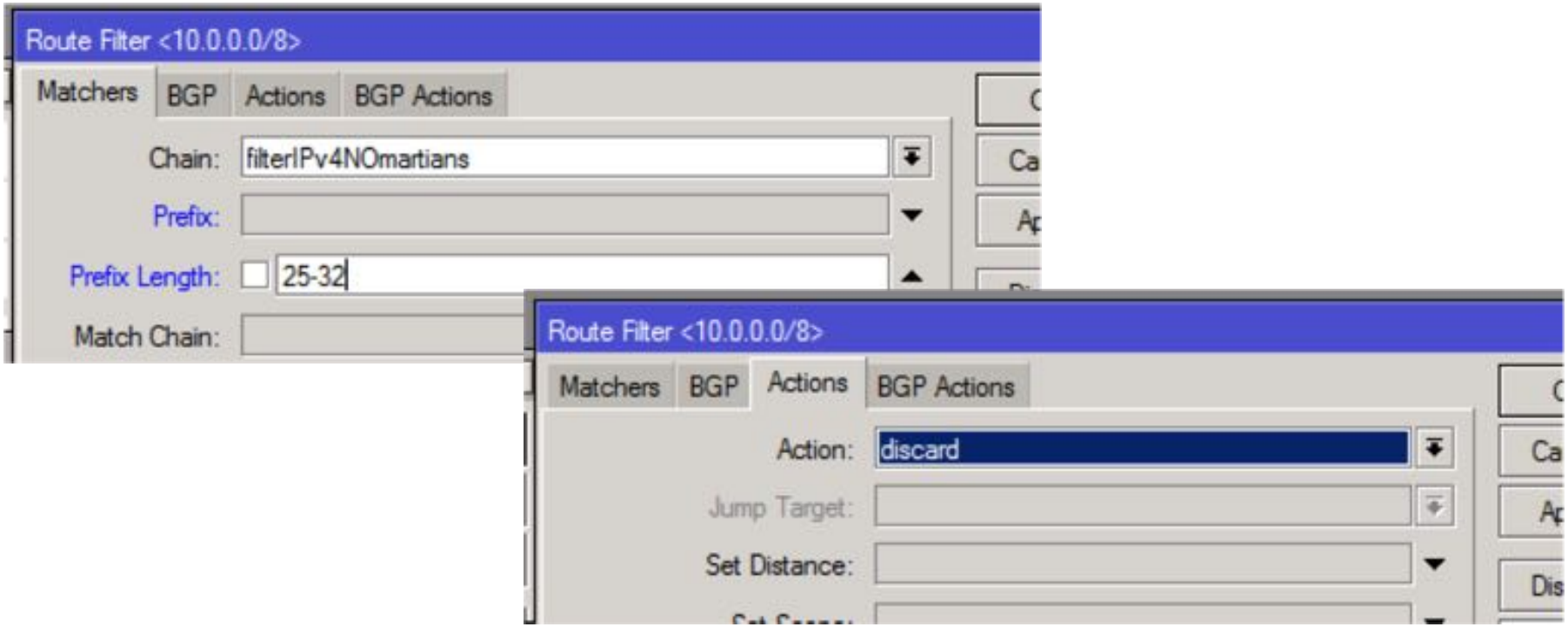
- Filtros IN: (filtrar la red local)
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

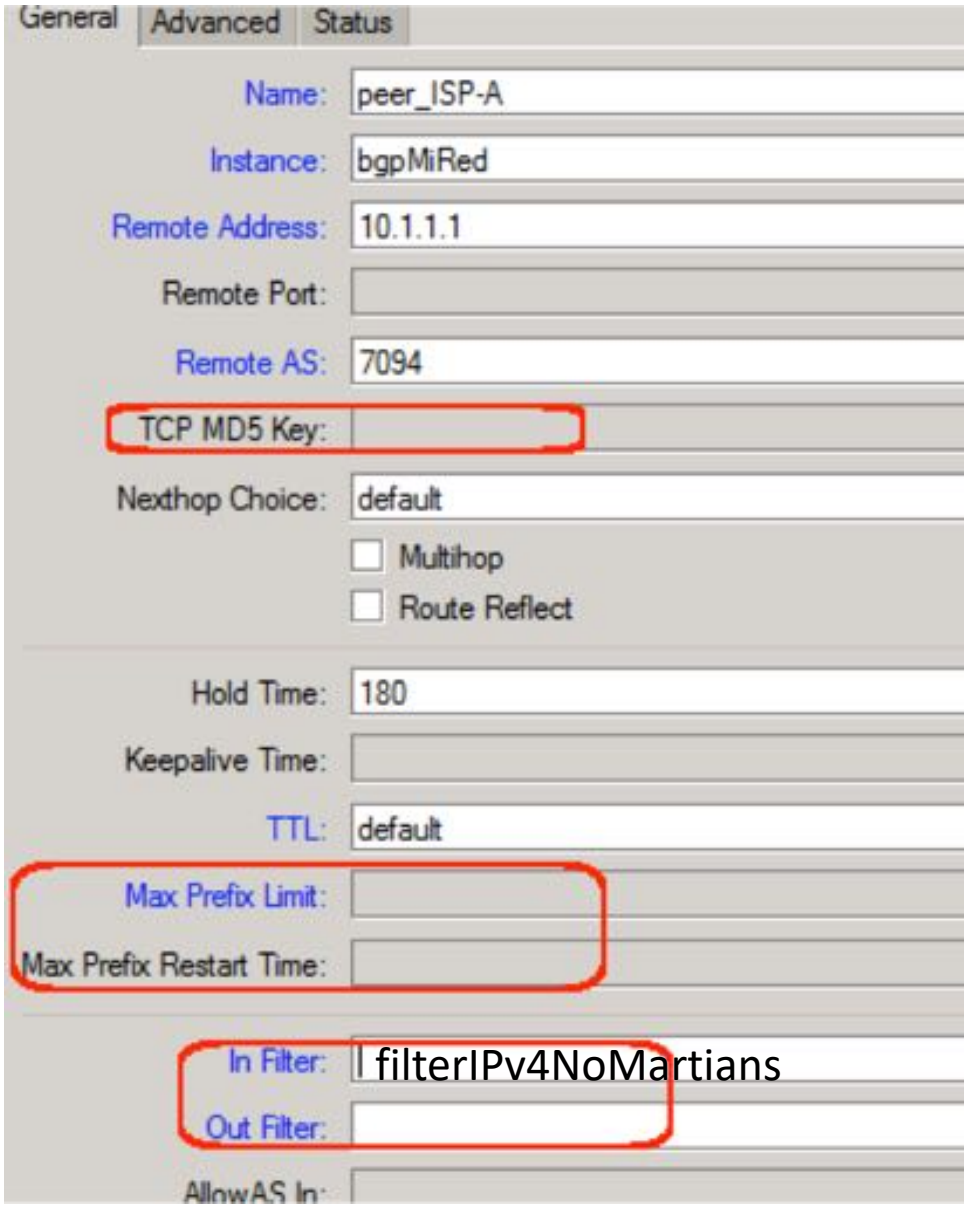
- Filtros IN: (filtrar prefijos > /24)
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Filtros BGP: IN & OUT

- Filtros IN: Aplicado al peer BGP.
- Routing->Filters -> +



HablaIP
Integración & Desarrollo

Agenda

- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- **Usando Comunidades BGP**
- Filtros de seguridad mínimos
- Tips para Layer2
- Q & A

HablaIP
Integración & Desarrollo

Comunidades BGP

- Que son las comunidades BGP
  - Son un atributo BGP y es un atributo transitivo opcional de longitud variable.
  - Las Comunidades se traspasan de Router a Router, aunque el Router no las “entienda”.
  - A cada prefijo anunciado se le pueden incorporar comunidades.

HablaIP
Integración & Desarrollo

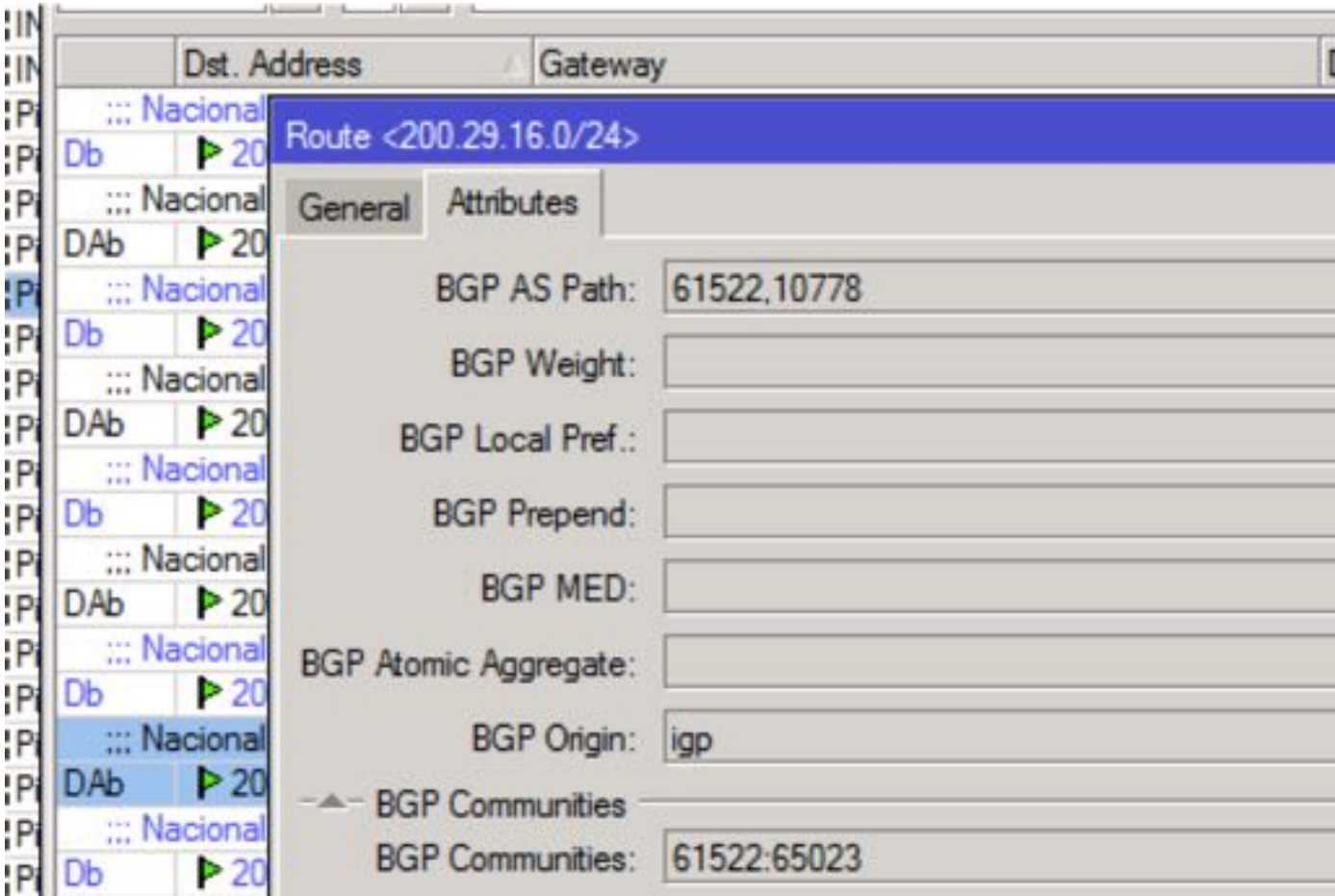
Comunidades BGP

- Para que sirven las comunidades BGP?
  - Para realizar Ingeniería de trafico (o TE)
  - Para identificar un grupo de prefijos con una o mas propiedades en común
  - El o los router upstream pueden ser influidos en su proceso de decisión de rutas.

HablaIP
Integración & Desarrollo

Comunidades BGP

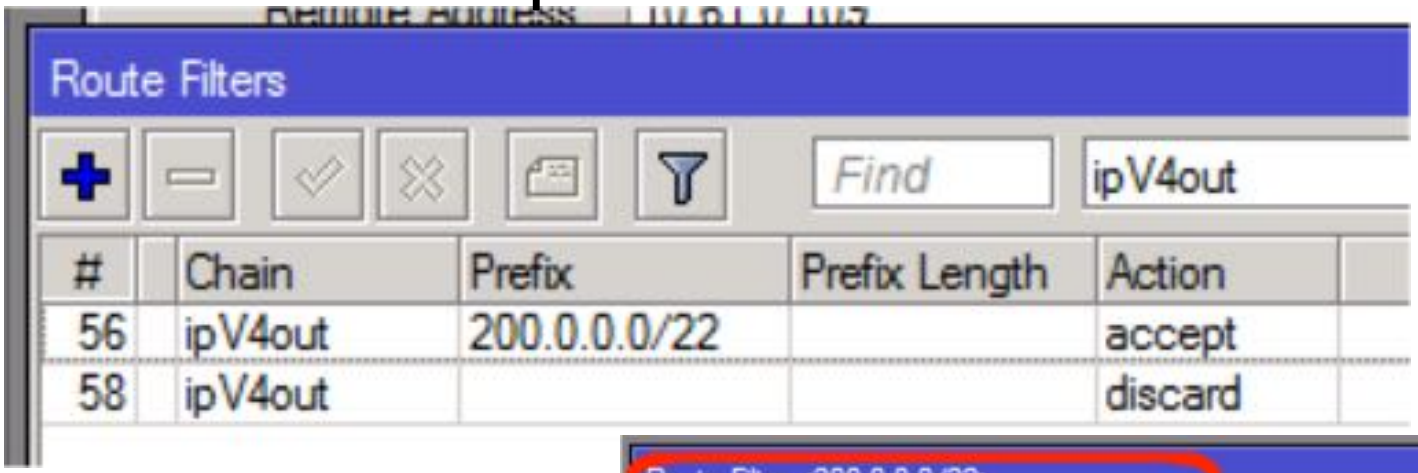
- Como ver las comunidades BGP en Mikrotik
  - IP->Routes->Detail Ejemplo: 61522:65023

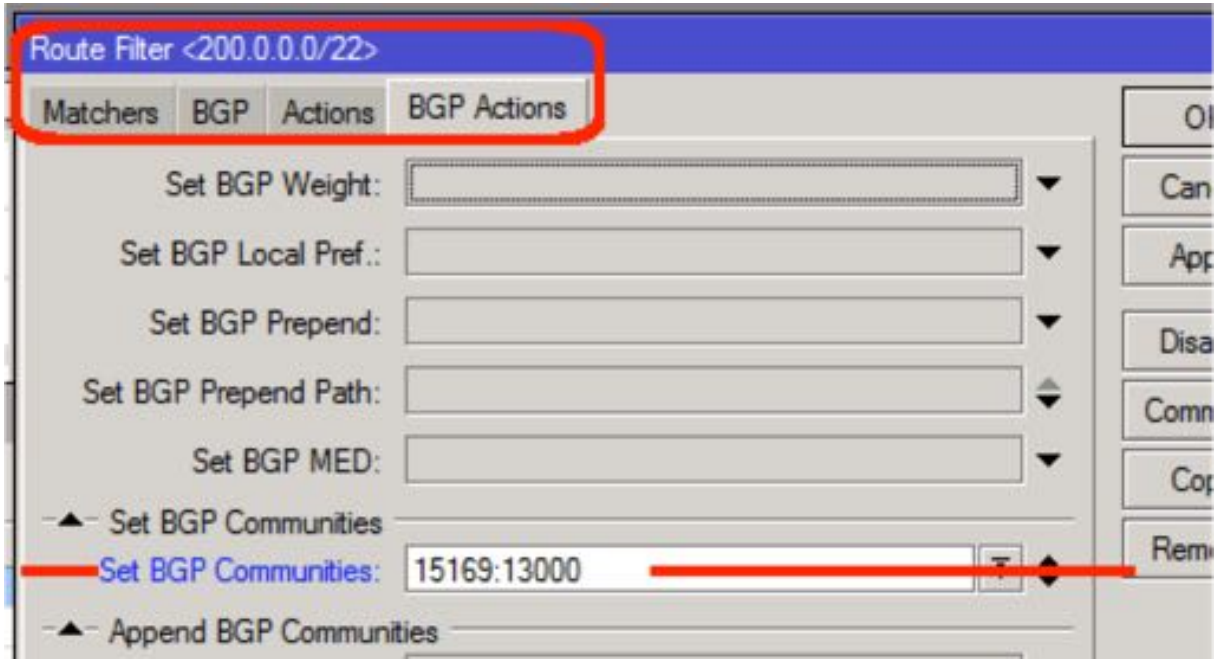


HablaIP
Integración & Desarrollo

Comunidades BGP

- Como se aplican las Comunidades en Mikrotik





HablaIP
Integración & Desarrollo

Comunidades BGP

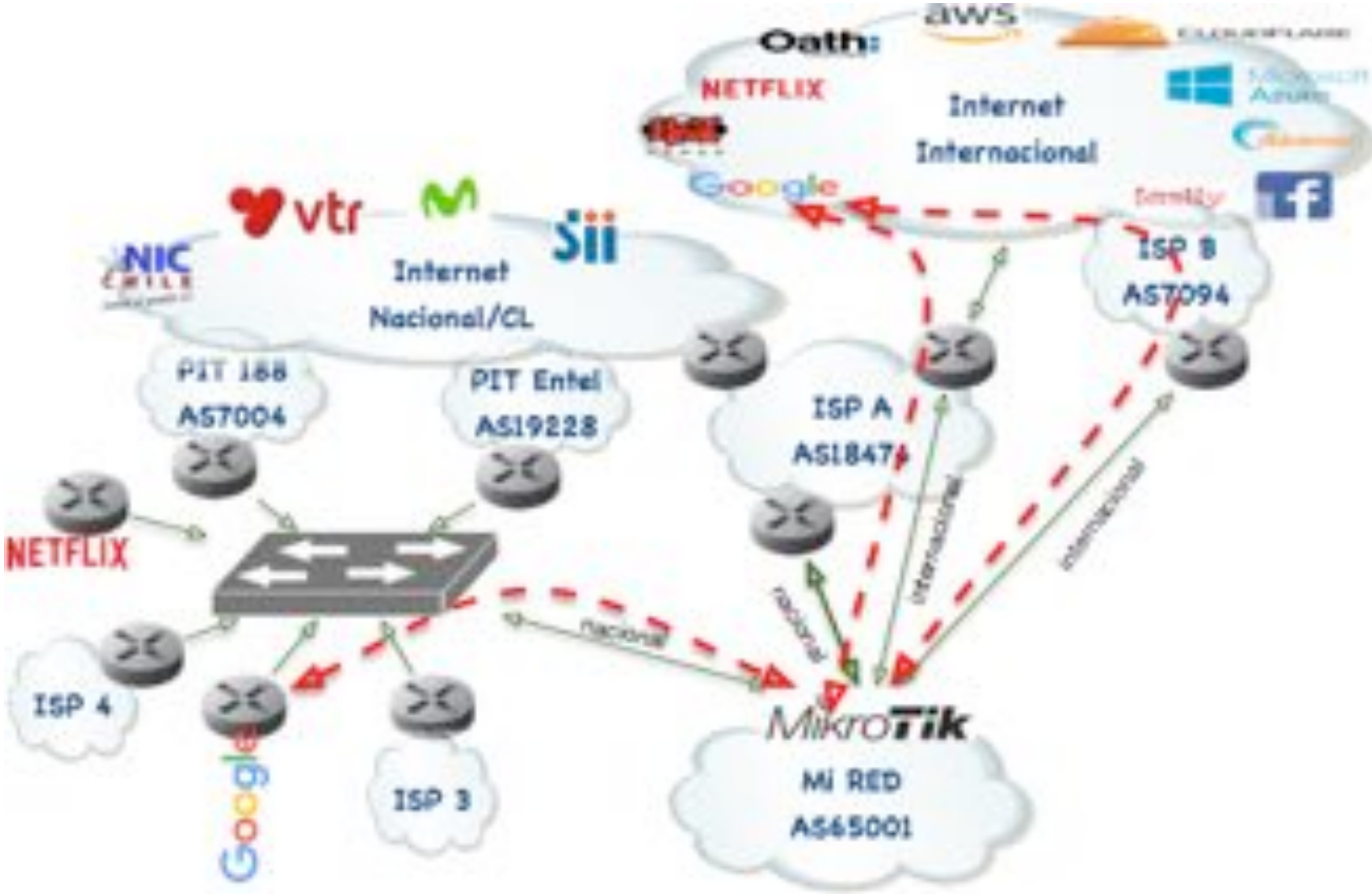
- Ejemplo Peering con Google (AS15169):

Community	Preferred Ingress Signalling Range
15169:13000	Lowest preference to receive traffic for this prefix at this interconnection point (try to not serve traffic here). Attempt to serve traffic on an indirect path (through other upstreams or peers) before using this prefix.
15169:13100	Default priority of traffic on an indirect path. Tagging with this community indicates that the preference is equal to receiving traffic over an indirect path.
15169:13200	Default priority to receive traffic for this prefix at this interconnection point (the same as if the prefix is untagged).
15169:13300	Highest preference to receive traffic for this prefix at this interconnection point (try to serve traffic here).

Fuente: (https://www.gstatic.com/isp/docs/BGPCommunitySupport.pdf)

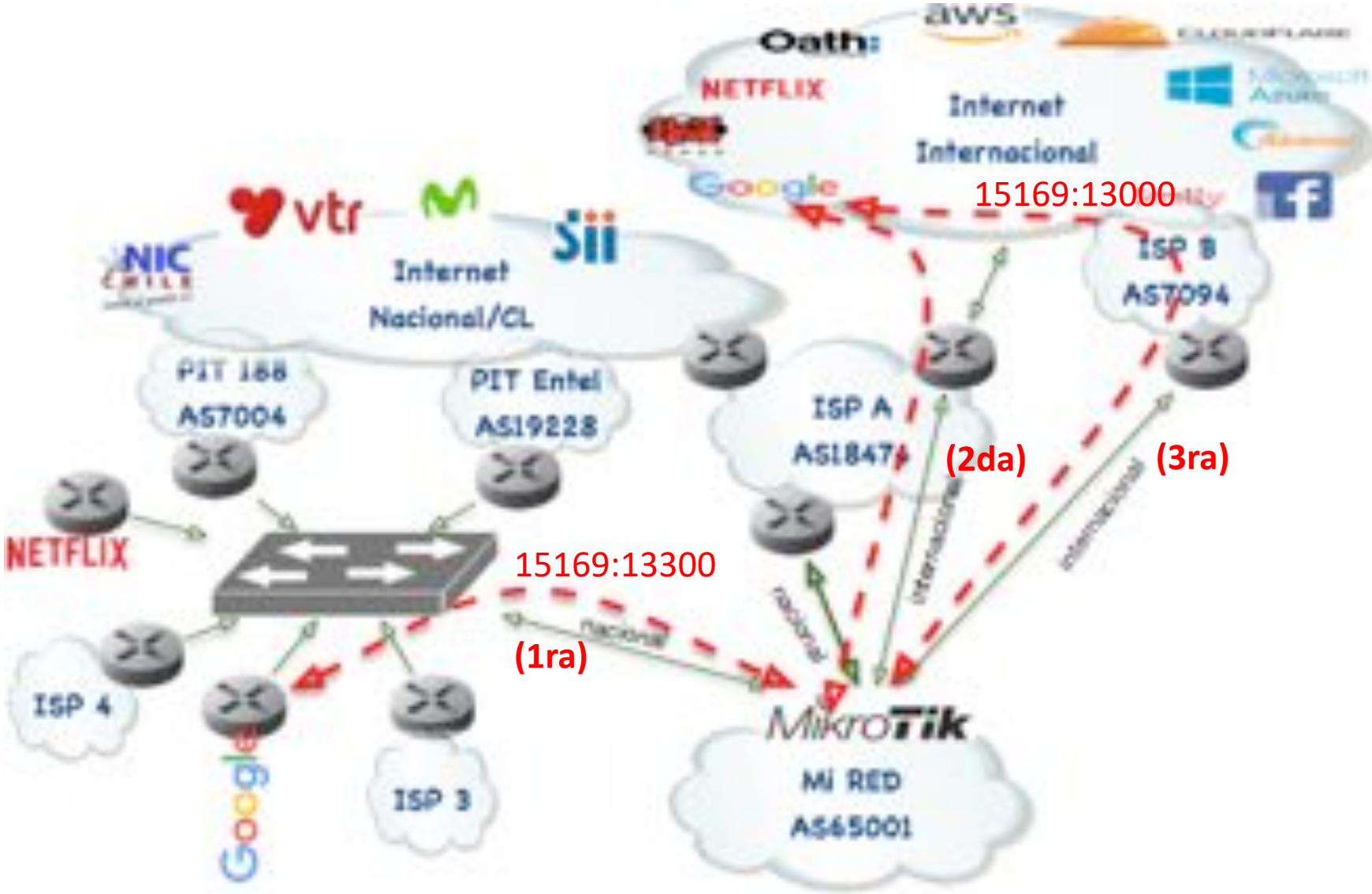
HablaIP
Integración & Desarrollo

Comunidades BGP



HablaIP
Integración & Desarrollo

Comunidades BGP



HablaIP
Integración & Desarrollo

Comunidades BGP

- Ejemplo Peering con Netflix (AS2906):

https://www.netflix.com

  - AWS

- Streaming
  - OCA

HablaIP
Integración & Desarrollo

Comunidades BGP

- Algoritmo de selección de OCA mas cercano
  - (1) Prefix (preferencia prefijo mas especifico)

    Un prefijo /24 será preferido sobre un /22

  - (2) AS Path (contabiliza AS Path diferentes)

    A prefijos iguales prefiere menor AS Path

  - (3) MED (prefiere el menor MED)

    Multi-exit Discriminator

HablaIP
Integración & Desarrollo

Comunidades BGP

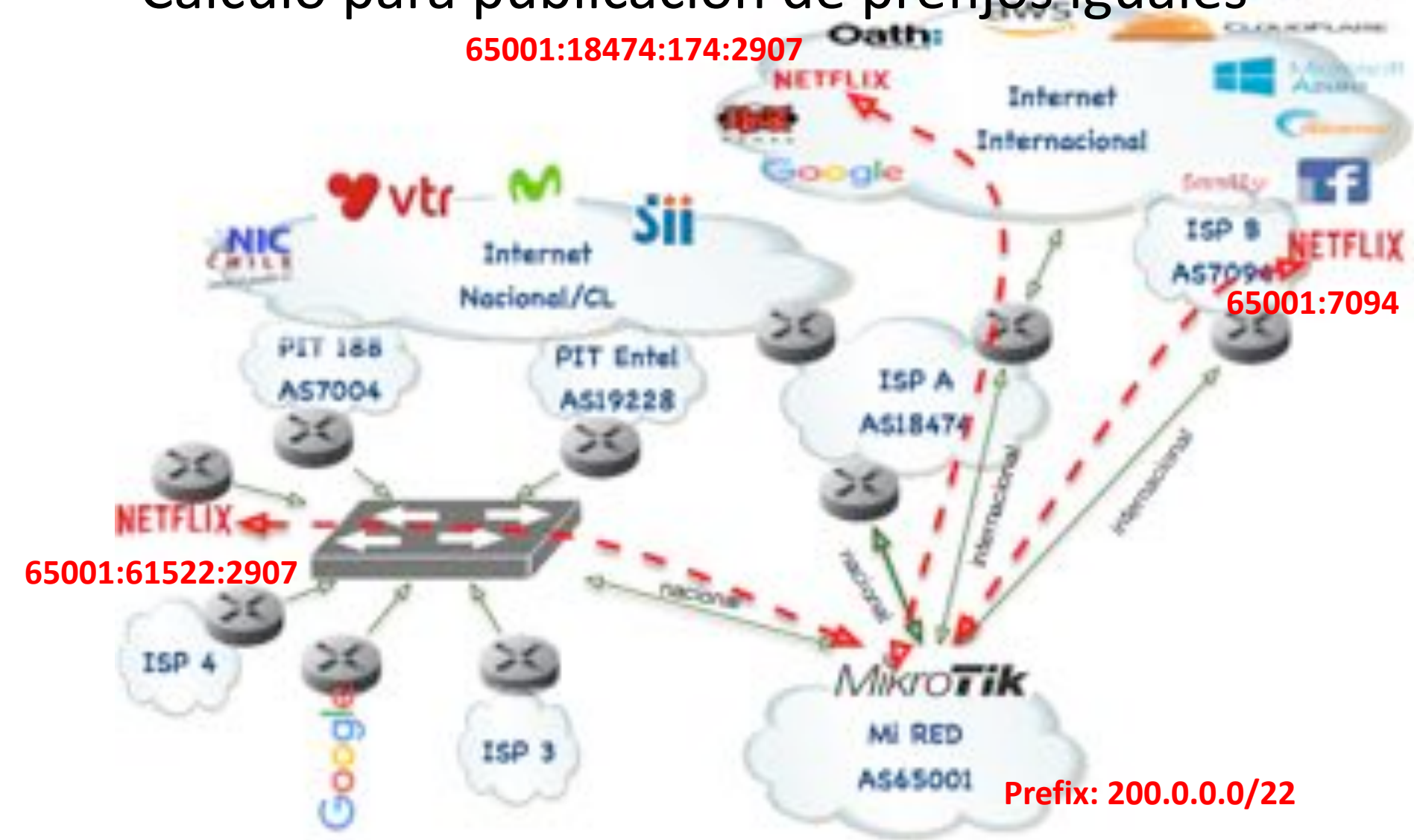
- Como verificar desde cual OCA recibo una pelicula?

Shift + Ctrl + Alt + Cmd + D

HablaIP
Integración & Desarrollo

Comunidades BGP

- Calculo para publicación de prefijos iguales



HablaIP
Integración & Desarrollo

Comunidades BGP

- Como preferir el OCA en PIT Chile?
  - Utilizaremos las Comunidades disponibles en PIT Chile:
  - 0:61522 -> No anunciar este prefijo a ningún miembro del IXP.
  - 61522:{ASN} -> Anunciar este prefijo solo al peer ASN: {ASN}

HablaIP
Integración & Desarrollo

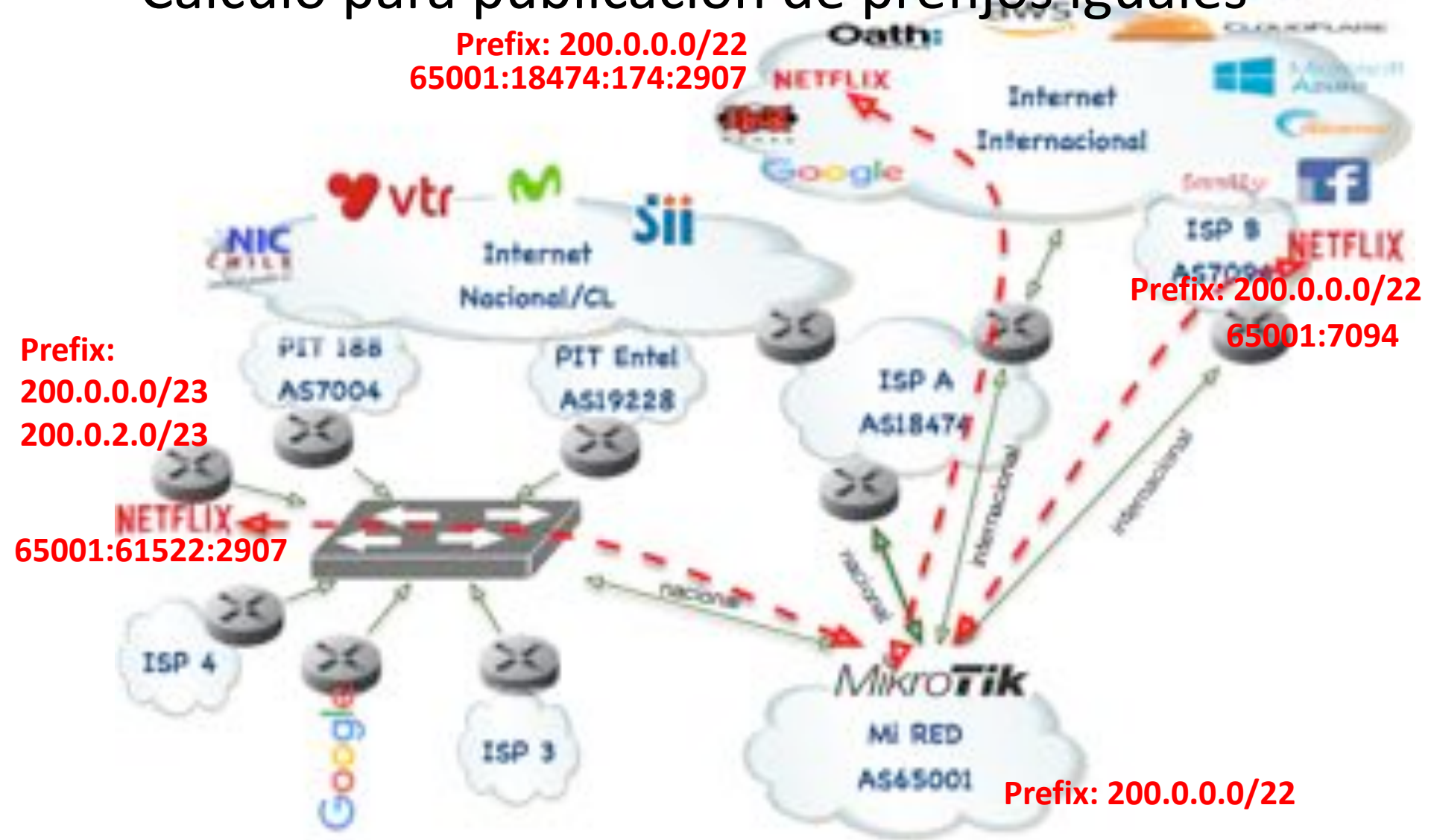
Comunidades BGP

- Como preferir el OCA en PIT Chile?
  - Publicar 200.0.0.0/22 a todos los Peer.
  - Publicar 200.0.0.0/22 a PitChile con la comunidad:
    - 0:2906 (No anunciar al peer AS2906 (Netflix))
  - Publicar solo a PitChile 200.0.0.0/23 y 200.0.2.0/23 con las comunidades:
    - 0:61522 (No anunciar a ningún miembro de PitChile)
    - 61522:2906 (SI anunciar al peer 2906 (Netflix))

HablaIP
Integración & Desarrollo

Comunidades BGP

- Calculo para publicación de prefijos iguales

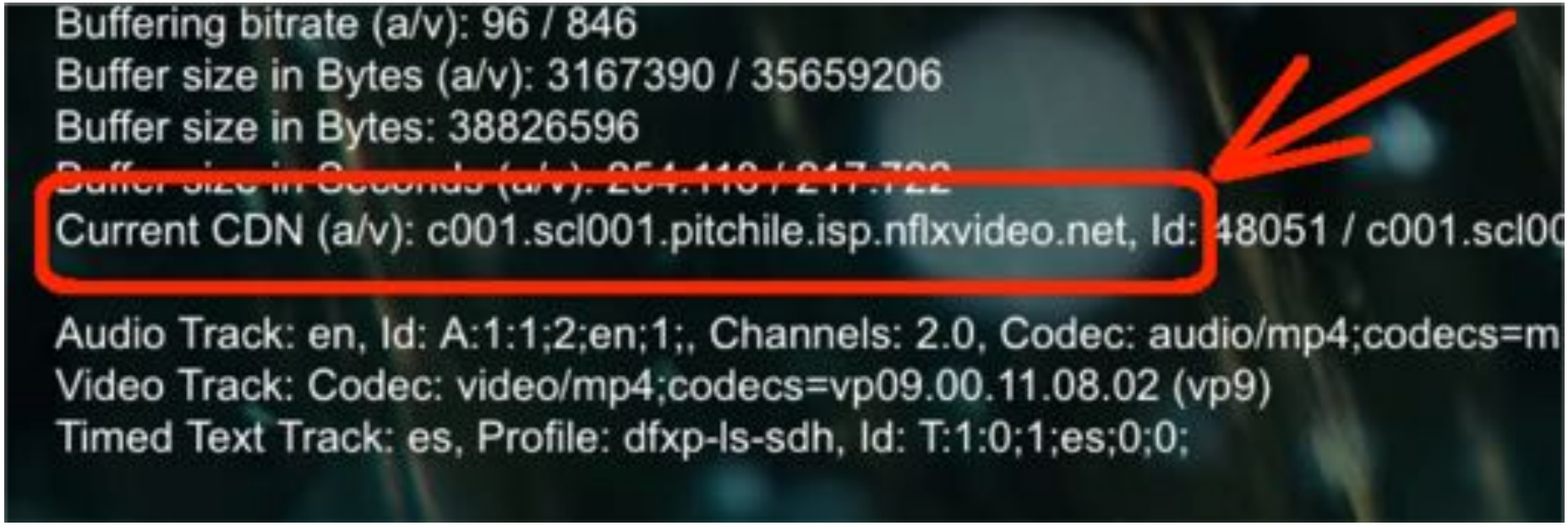


HablaIP
Integración & Desarrollo

Comunidades BGP

- Como verificar desde cual OCA recibo una pelicula?

Shift + Ctrl + Alt + Cmd + D



HablaIP
Integración & Desarrollo

Agenda

- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- **Filtros de seguridad mínimos**
- Tips para Layer2
- Q & A

HablaIP
Integración & Desarrollo

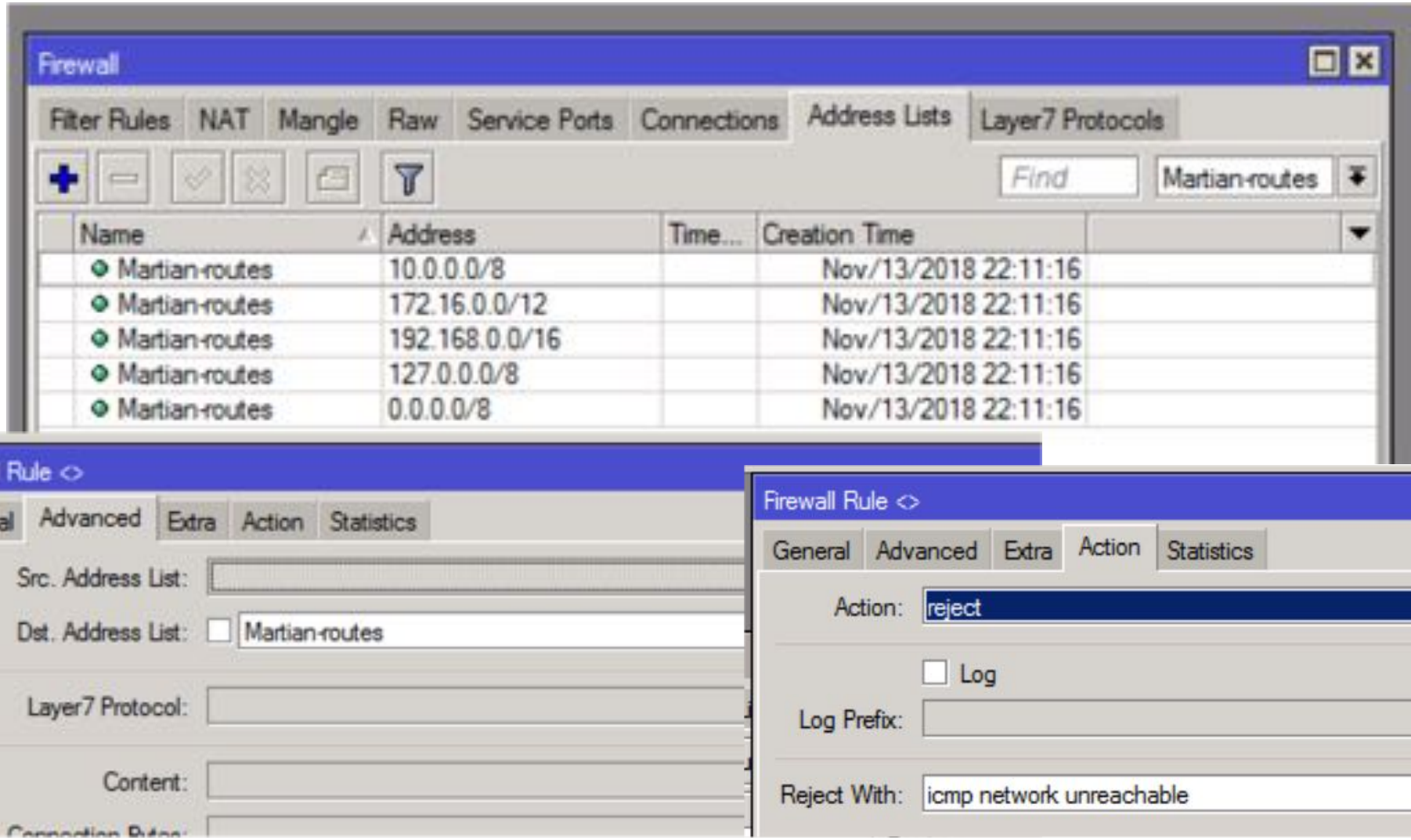
Minimo Security Filters

- Filtros de paquetes mínimos de seguridad:
  - Martian Routes filter
    - Using Address List
  - Spoofing IP Filter (IN & OUT)
    - (https://www.caida.org/projects/spoofer)
  - Transit IP Filters
  - Permitir puerto BGP tcp/179 Solo desde Peers

HablaIP
Integración & Desarrollo

Minimo Security Filters

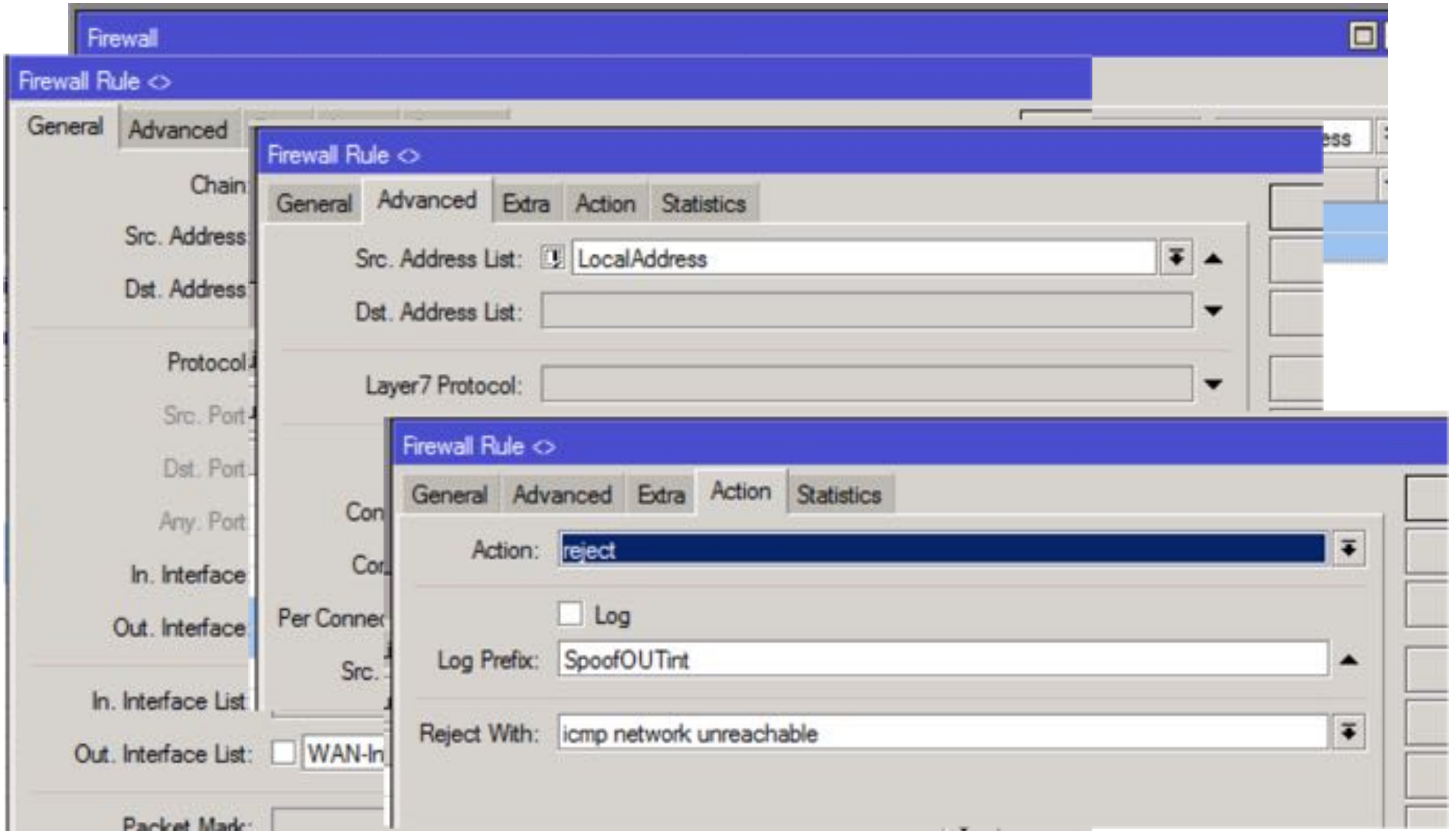
- Martian Routes Filter:



HablaIP
Integración & Desarrollo

Minimo Security Filters

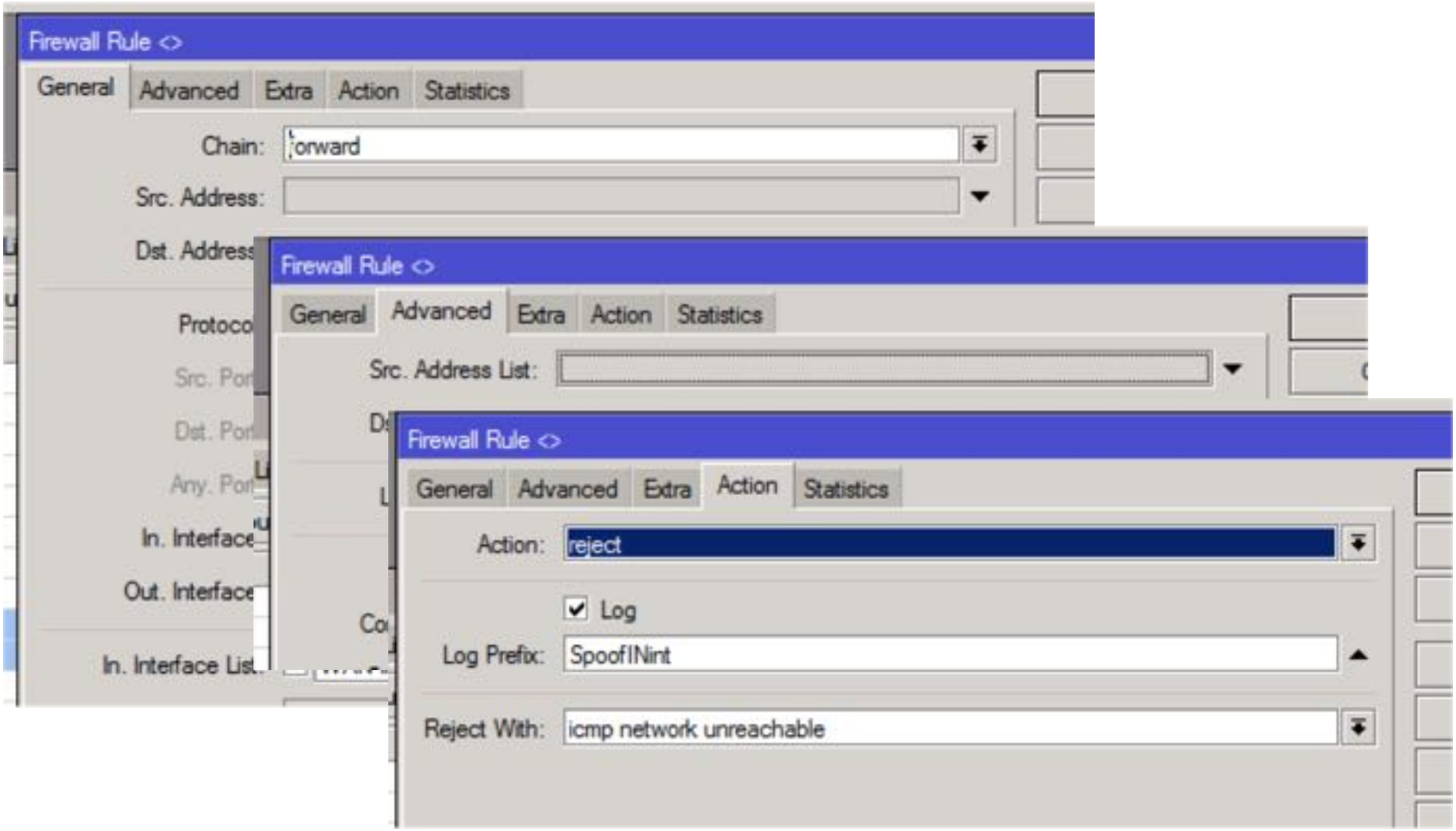
- Spoofing IP Filter (IN & OUT)



HablaIP
Integración & Desarrollo

Minimo Security Filters

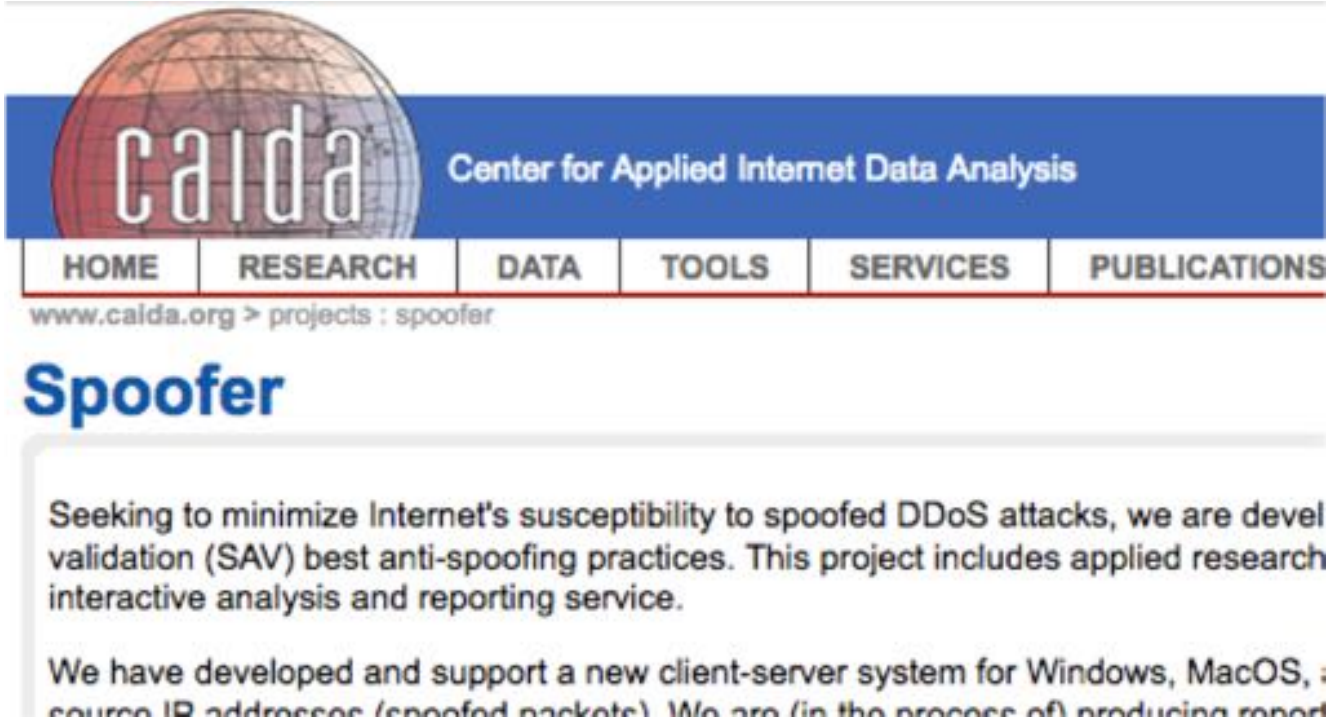
- Spoofing IP Filter (IN & OUT)



HablaIP
Integración & Desarrollo

Minimo Security Filters

- Spoofing IP Filter (IN & OUT)
  - Como verificar mi red?



  - https://www.caida.org/projects/spoofer

HablaIP
Integración & Desarrollo

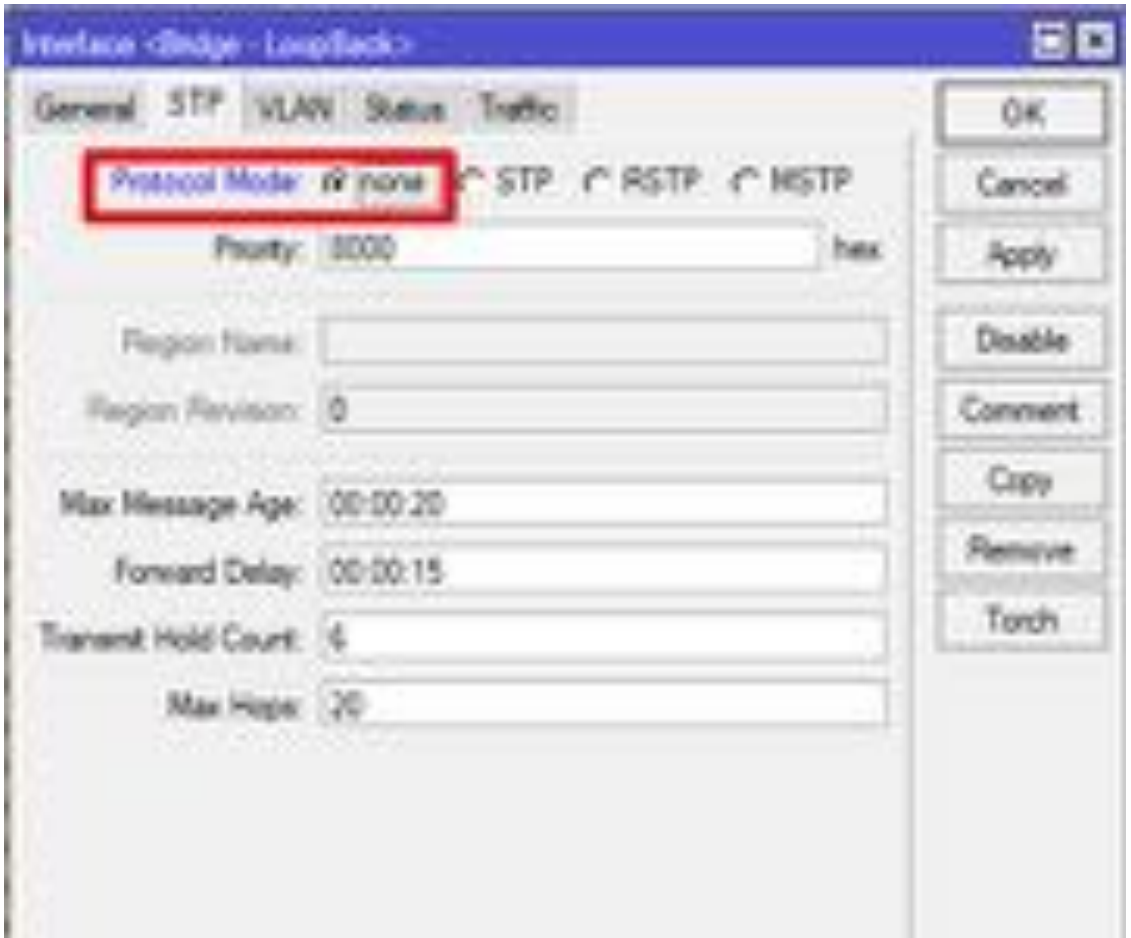
Agenda

- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- Filtros de seguridad mínimos
- **Tips para Layer2**
- Q & A

HablaIP
Integración & Desarrollo

Tips Layer2 IXP

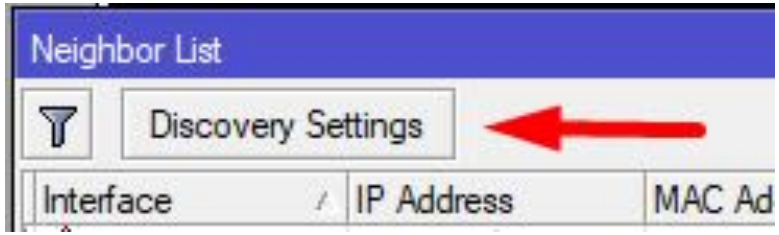
- Mejorando la seguridad de MKT en el borde:
  - Desactivando STP (Spanning tree protocol) si usas bridge



HablaIP
Integración & Desarrollo

Tips Layer2 IXP

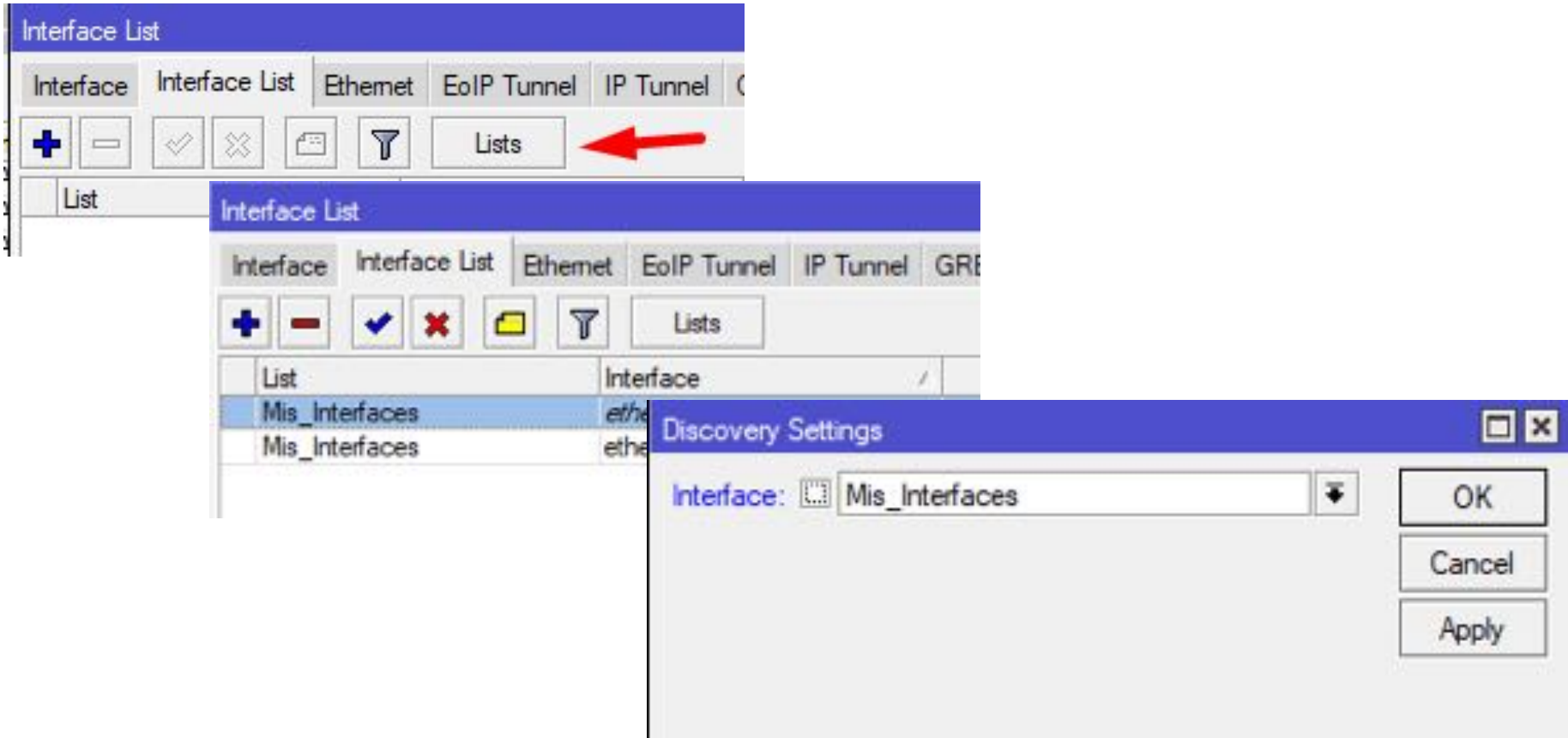
- MNDP (Mikrotik Neighbor Discovery Protocol)
  - IP -> Neighbors



HablaIP
Integración & Desarrollo

Tips Layer2 IXP

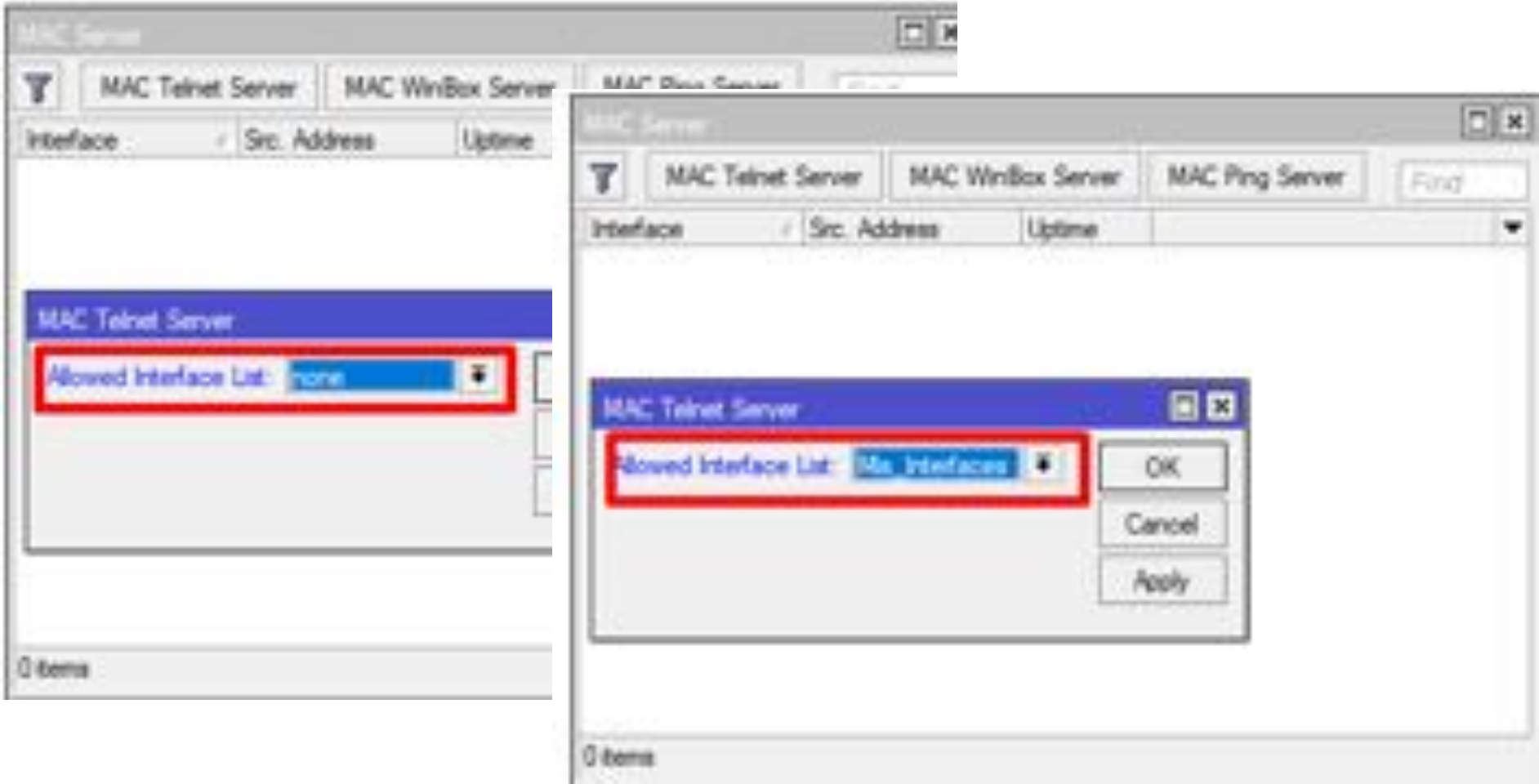
- MNDP (Mikrotik Neighbor Discovery Protocol)
  - Solo dejarlo para una interfaz particular?



HablaIP
Integración & Desarrollo

Tips Layer2 IXP

- Mejorando la seguridad de MKT en el borde:
- MAC telnet server // MAC winbox server



HablaIP
Integración & Desarrollo

Tips Layer2 IXP

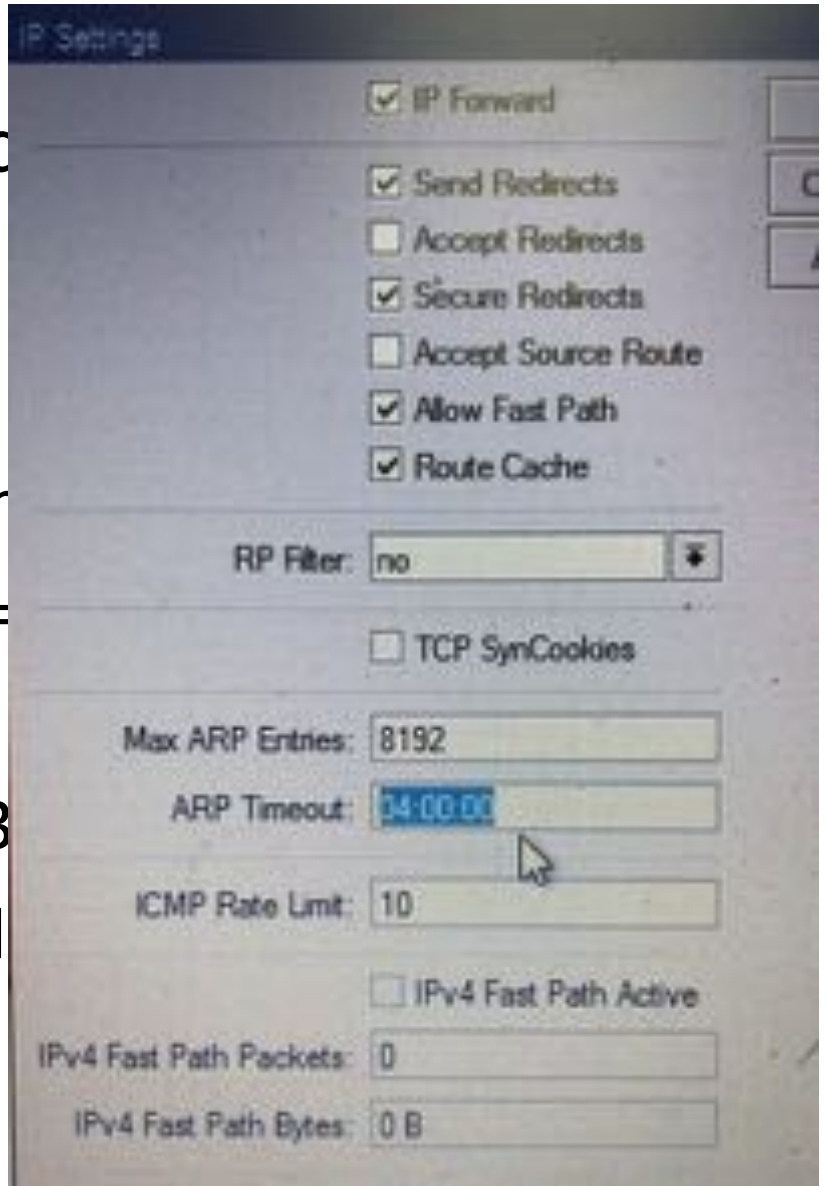
- Mejorando la seguridad d
- RTP Timeout

  – Mikrotik Default: 30 segur

  /ip settings set arp-timeout=

  – Por interfaz (versión >=6.3

  /interface ethernet set [find
  timeout=4h



HablaIP
Integración & Desarrollo

Agenda

- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- Filtros de seguridad mínimos
- Tips para Layer2
- **Q & A**

HablaIP
Integración & Desarrollo

Q & A

HablaIP
Integración & Desarrollo

Tips & Tricks to connect to a Layer2 IXP

MUM Chile 2019

MikroTik