

Tips & Tricks to connect to a Layer2 IXP

MUM Chile 2019



Agenda

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

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.



- Interconnection Strategy en IXP Pit Chile.

Agenda

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

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.

Introducción

- Que es un IXP?
- Esquema tradicional
Con un proveedor de Internet.



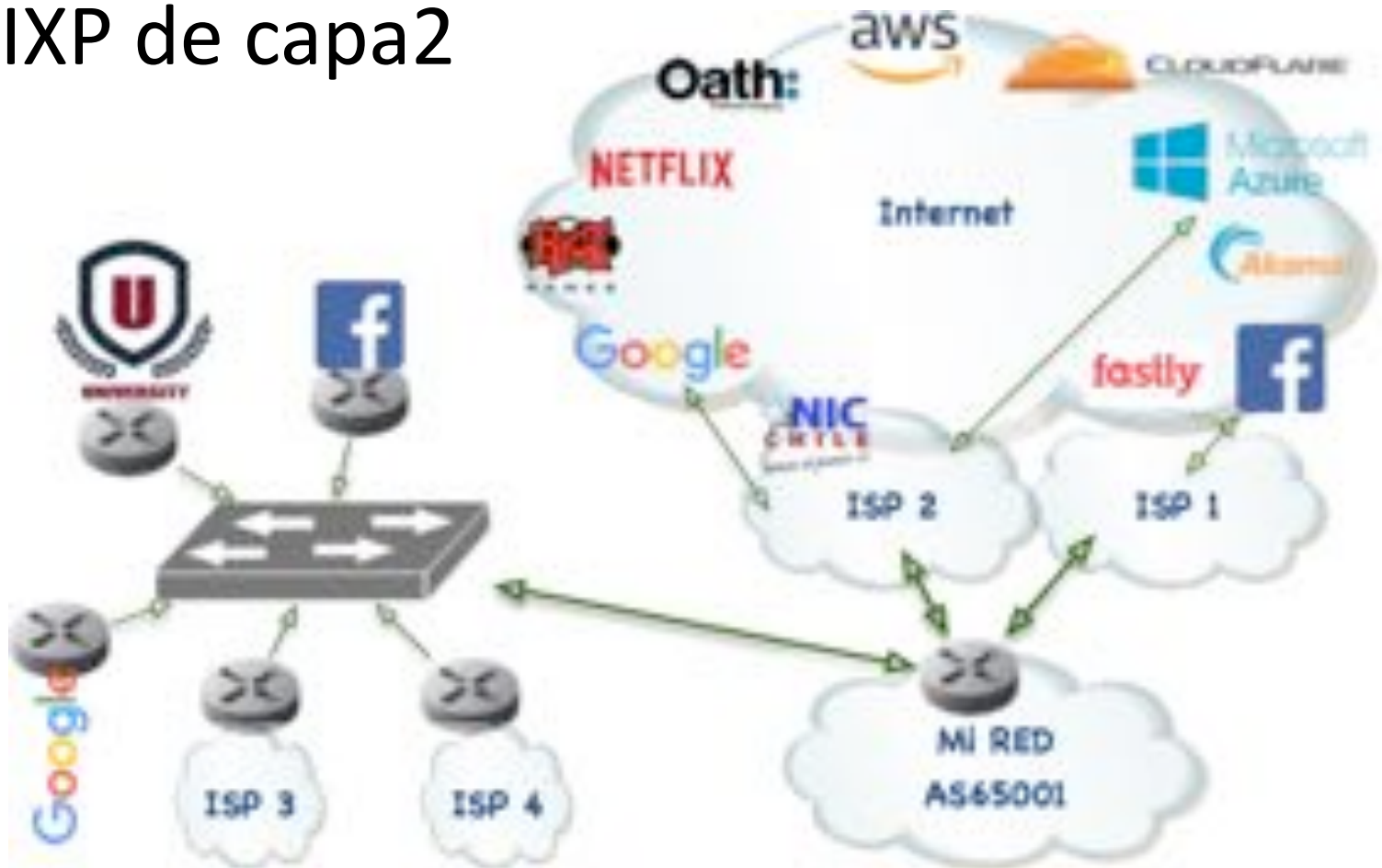
Introducción

- Que es un IXP?
- Esquema tradicional
Con /dos/ proveedores
De Internet.








Introducción

- Un IXP de capa2



Introducción

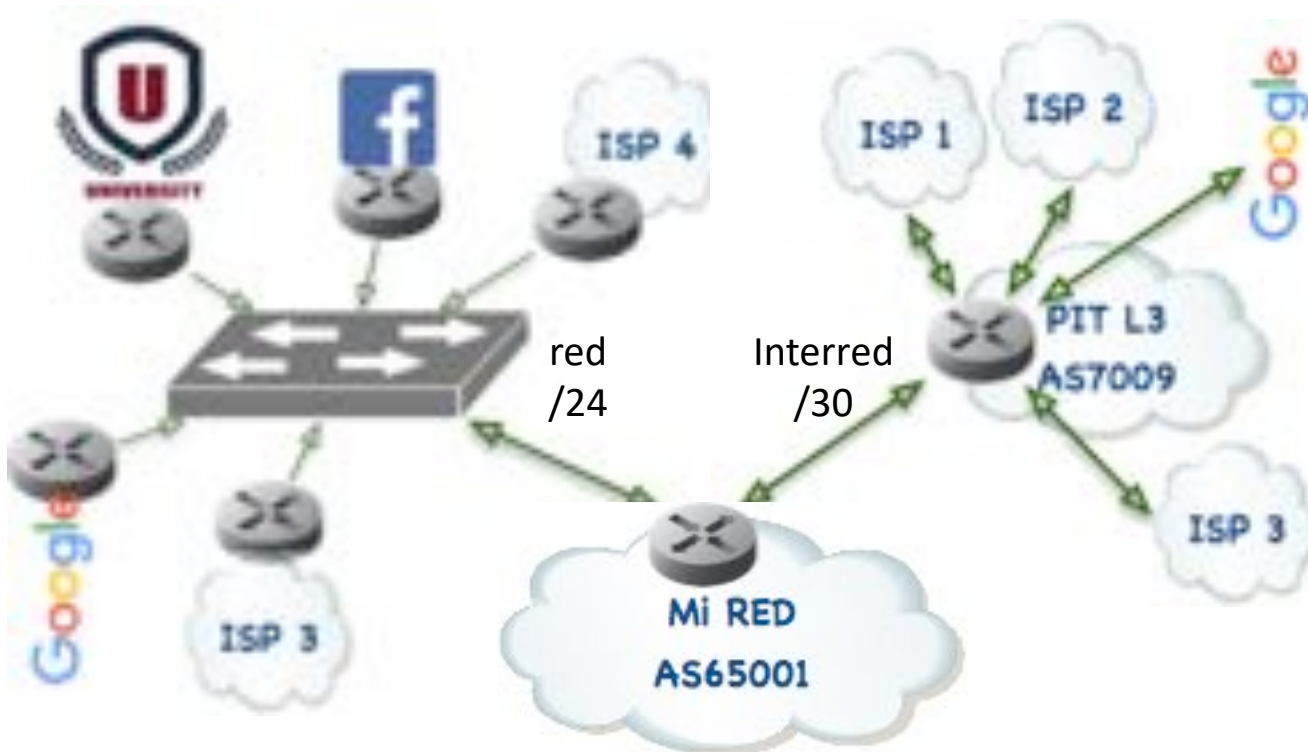
- IXP/PIT's en Chile: (según Subtel)
 - PIT Claro Chile PIT Orange
 - PIT Entel PIT Telefónica Mundo
 - PIT Level3 PIT Chile 
 - PIT Intercity PIT Tecnoera 
 - PIT NAP Chile  PIT Concepción 
-  Valparaíso

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

Introducción

- Diferencia entre IXP Layer3 v/s Layer2

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



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 ;-)

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.

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.

Agenda

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

Mikrotik en el borde

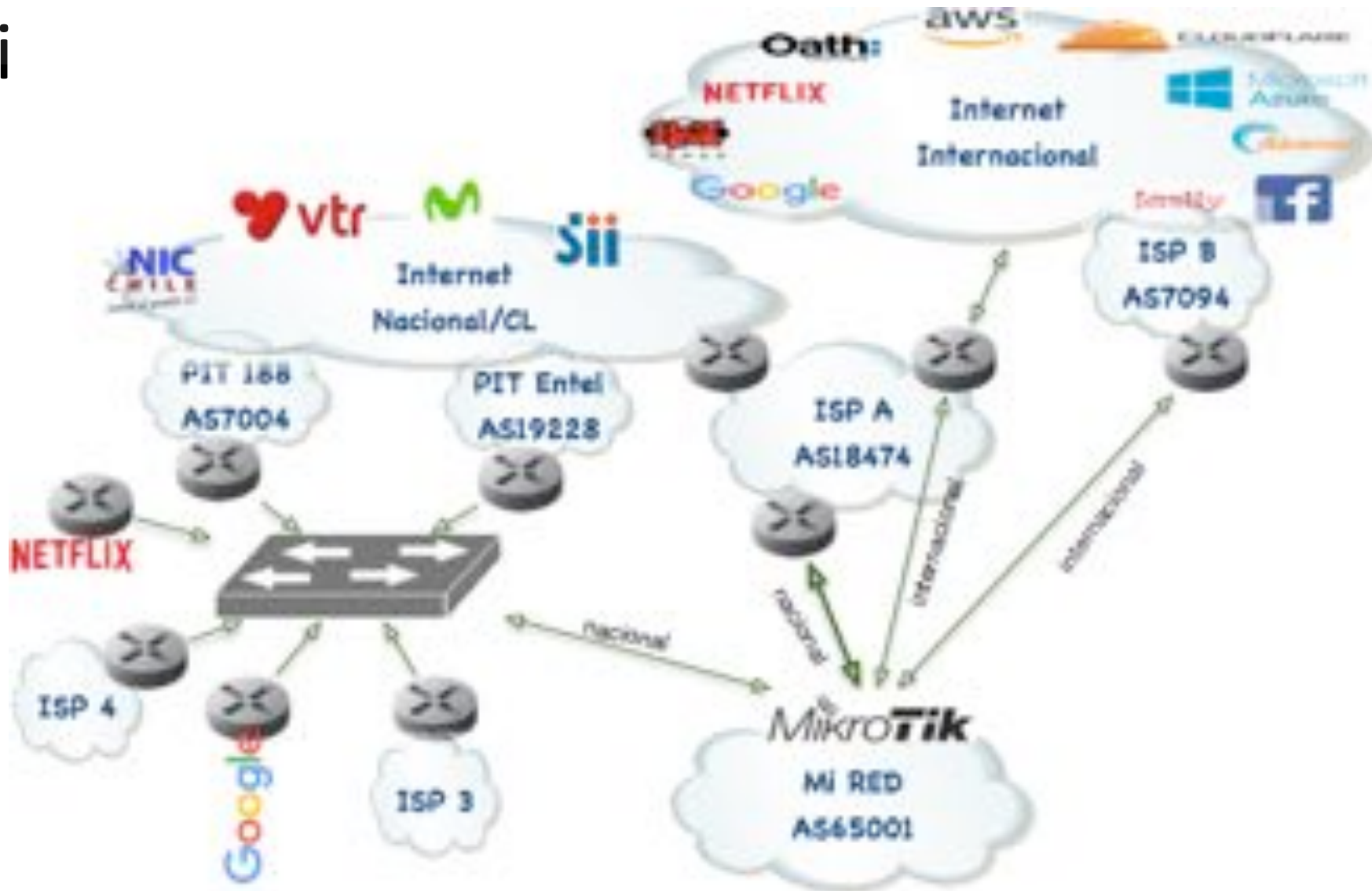
- Ejemplo de organización conectada a dos ISP's y un PIT.
 - RED a conectar: AS65001
 - ISP A: AS18474 nac. e inter.
 - ISP B: AS7094 inter.
 - PIT CL: AS61522



Mikrotik en el borde



Mi



Creando peers BGP4

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

New BGP Instance

Name: bgpMiRed

AS: 65001

Router ID: [dropdown menu]

☐ Redistribute Connected

☐ Redistribute Static

☐ Redistribute RIP

☐ Redistribute OSPF

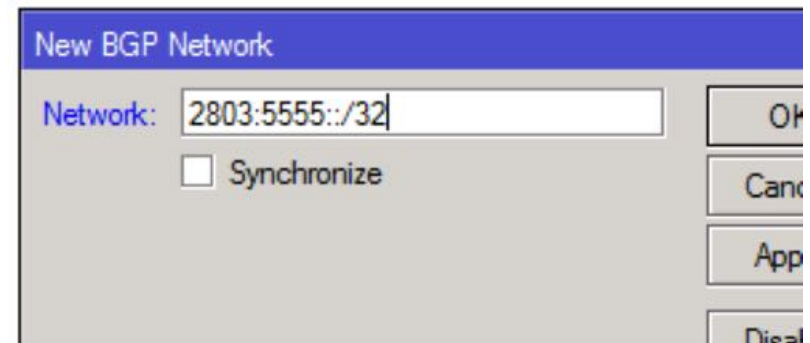
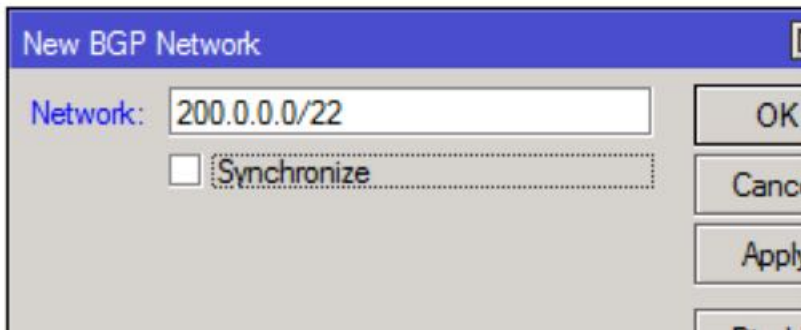
☐ Redistribute Other BGP

Out Filter: [dropdown menu]

Confederation: [dropdown menu]

Creando peers BGP4

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



Creando peers BGP4

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

The screenshot shows the 'New BGP Peer' configuration window with the 'General' tab selected. The following fields are highlighted with red boxes:

- Name: peer ISP-A
- Instance: bgpMiRed
- Remote Address: 10.1.1.1
- Remote AS: 7094

Other visible fields include Remote Port, TCP MD5 Key, Nexthop Choice (set to default), and checkboxes for Multihop and Route Reflect.

The screenshot shows the 'New BGP Peer' configuration window with the 'Advanced' tab selected. The following fields are highlighted with red boxes:

- Address Families: ☒ ip, ☐ ipv6, ☐ l2vpn, ☐ vpn4
- Update Source: none
- Cisco VPLS NLRI Length Format: auto bits

Creando peers BGP4

- Ejemplo de visualización de Peers BGP

Nombre	Remotos IP	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

Creando peers BGP4

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

The screenshot shows a configuration window for a BGP peer. The 'General' tab is selected. The following fields are visible and highlighted with red boxes:

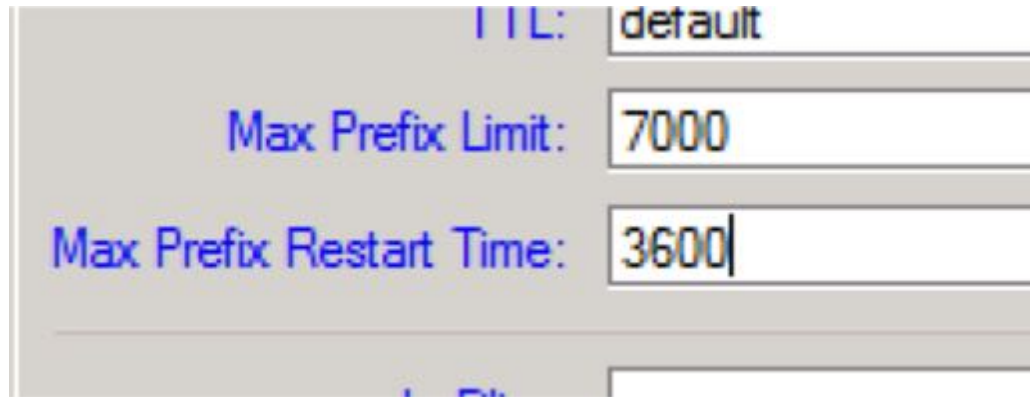
- TCP MD5 Key:** A text input field.
- Max Prefix Limit:** A text input field.
- Max Prefix Restart Time:** A text input field.
- In Filter:** A text input field.
- Out Filter:** A text input field.

Other visible fields include:

- Name:** peer_ISP-A
- Instance:** bgpMiRed
- Remote Address:** 10.1.1.1
- Remote Port:** (empty)
- Remote AS:** 7094
- Nexthop Choice:** default
- Hold Time:** 180
- Keepalive Time:** (empty)
- TTL:** default
- ☐ Multihop
- ☐ Route Reflect
- AllowAS In:** (empty)

Creando peers BGP4

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



The image shows a configuration window for BGP peers. It contains three input fields with labels in blue text. The first field is labeled 'TTL:' and has 'default' entered. The second field is labeled 'Max Prefix Limit:' and has '7000' entered. The third field is labeled 'Max Prefix Restart Time:' and has '3600' entered.

TTL:	default
Max Prefix Limit:	7000
Max Prefix Restart Time:	3600

(evitar recibir “escapes” de rutas)

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



Filtros BGP: IN & OUT

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



Filtros BGP: IN & OUT

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

Route Filter <200.0.0.0/22>

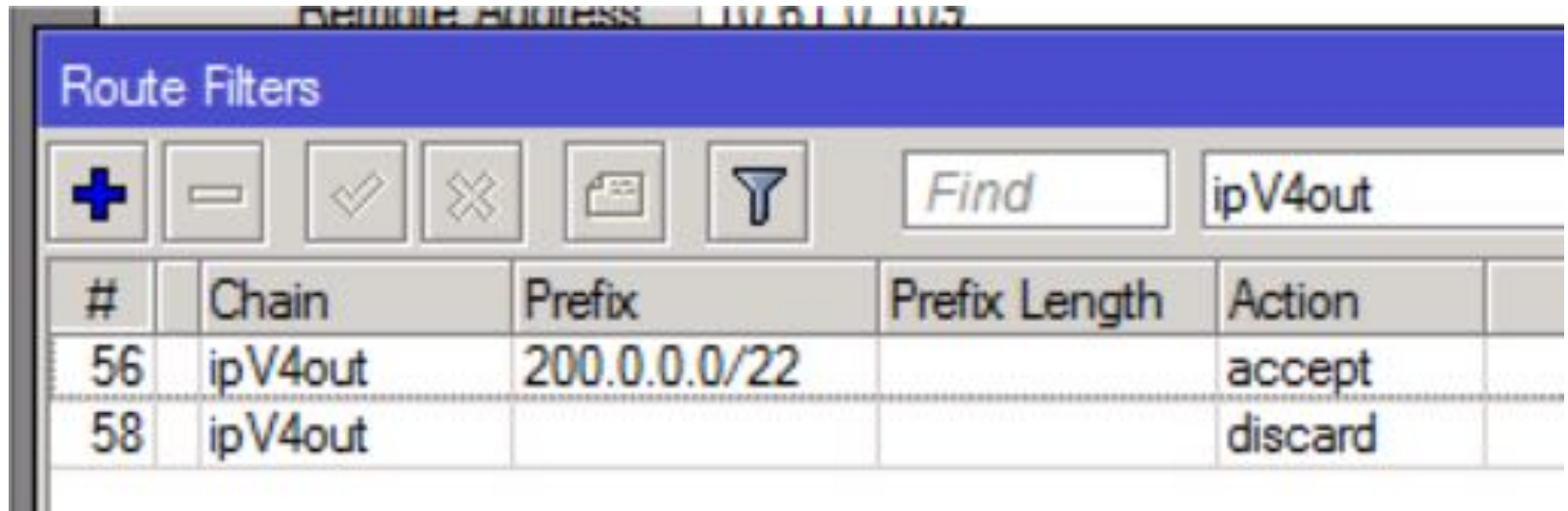
Matchers	BGP	Actions	BGP Actions
Chain:	pV4out		
Prefix:	<input type="checkbox"/> 200.0.0.0/22		
Prefix Length:			
Match Chain:			

Route Filter <200.0.0.0/22>

Matchers	BGP	Actions	BGP Actions
Action:	accept		
Jump Target:			
Set Distance:			

Filtros BGP: IN & OUT

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



The screenshot shows the 'Route Filters' configuration window in Mikrotik WinBox. The window has a blue title bar and a toolbar with icons for adding, deleting, saving, and applying filters, along with a search bar. Below the toolbar is a table listing the configured filters. Two filters are visible: one with ID 56 that accepts the 200.0.0.0/22 prefix, and another with ID 58 that discards all traffic.

#	Chain	Prefix	Prefix Length	Action
56	ipV4out	200.0.0.0/22		accept
58	ipV4out			discard

Filtros BGP: IN & OUT

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

The screenshot shows a configuration window for a BGP peer named 'peer_ISP-A'. The 'Advanced' tab is selected. The following fields are highlighted with red boxes:

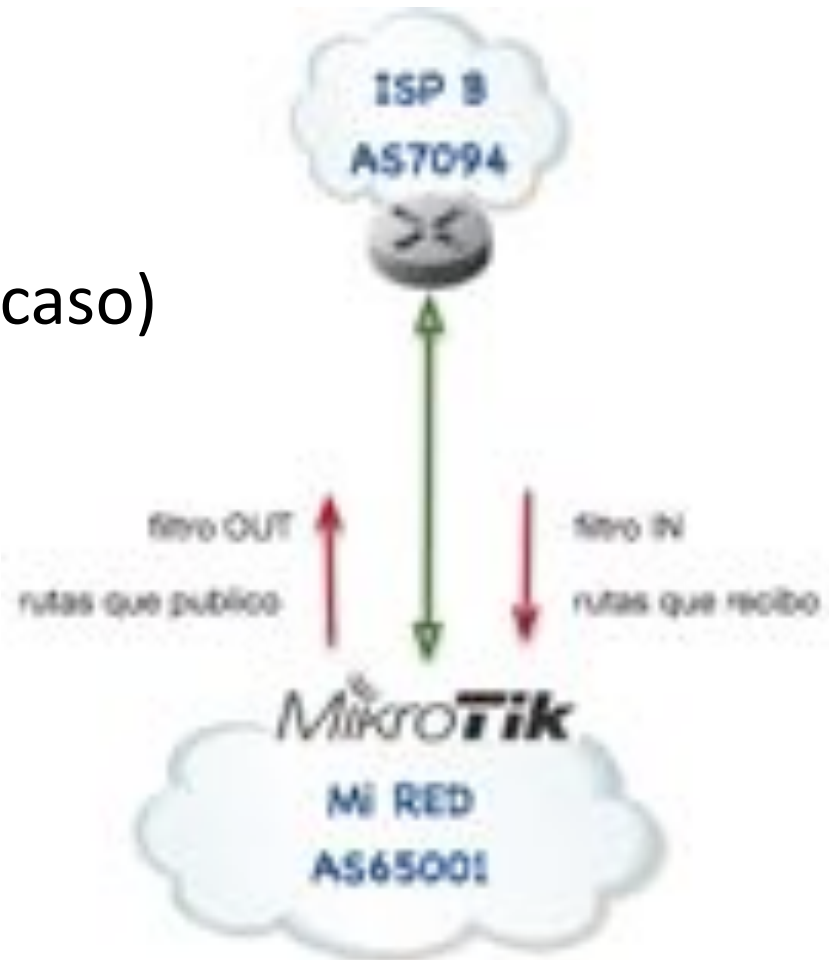
- TCP MD5 Key:** An empty text input field.
- Max Prefix Limit:** An empty text input field.
- Max Prefix Restart Time:** An empty text input field.
- In Filter:** An empty text input field.
- Out Filter:** A text input field containing the value 'ipV4out'.

Other visible fields include:

- Name:** peer_ISP-A
- Instance:** bgpMiRed
- Remote Address:** 10.1.1.1
- Remote Port:** (empty)
- Remote AS:** 7094
- Nexthop Choice:** default
- Hold Time:** 180
- Keepalive Time:** (empty)
- TTL:** default
- Route Reflect:** (unchecked checkbox)

Filtros BGP: IN & OUT

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



Filtros BGP: IN & OUT

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

Route Filter <10.0.0.0/8>

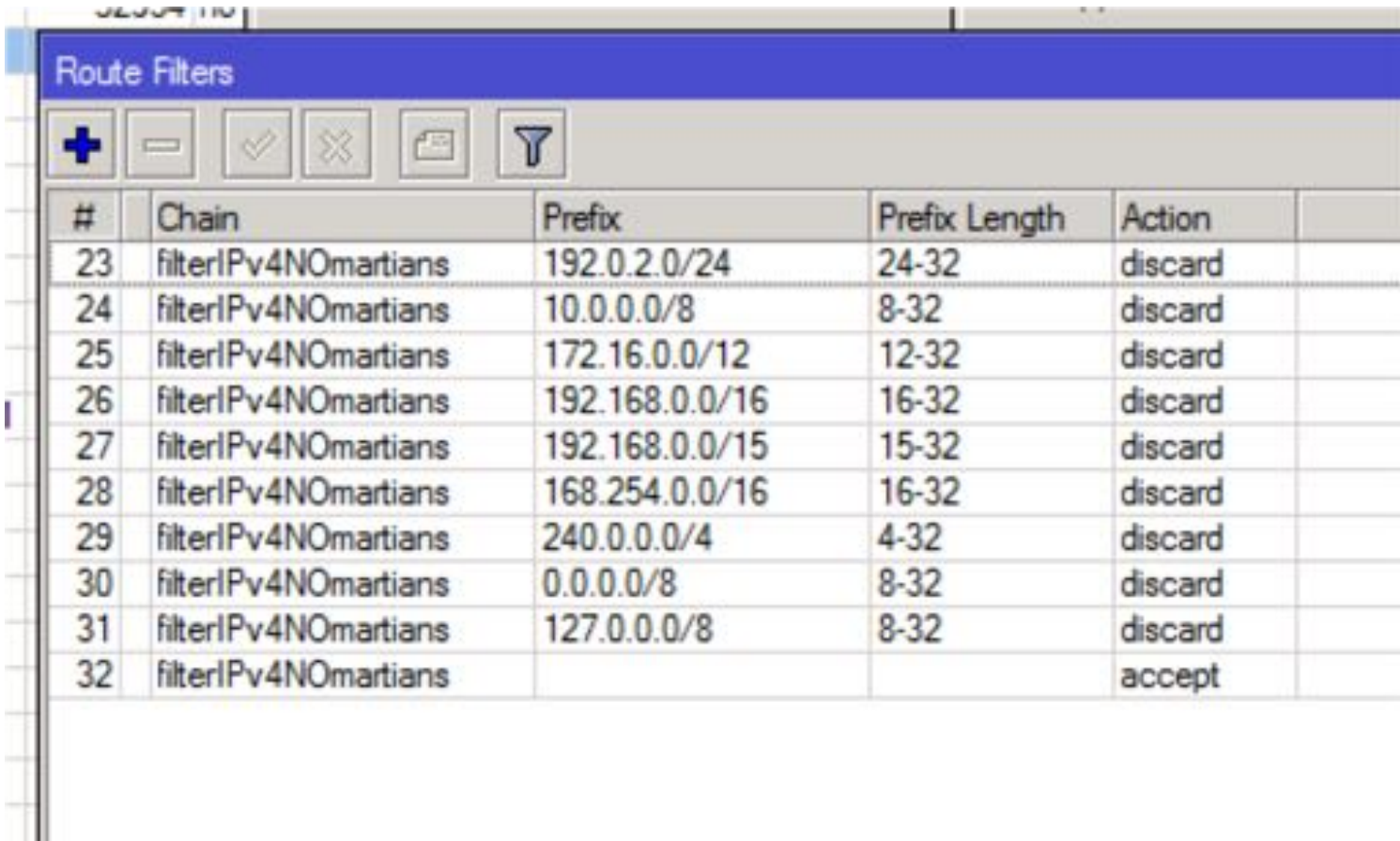
Matchers	BGP	Actions	BGP Actions
Chain:	filterIPv4NOmartians		
Prefix:	<input type="checkbox"/> 10.0.0.0/8		
Prefix Length:	<input type="checkbox"/> 8-32		
Match Chain:			
Protocol:			
Distance:			

Route Filter <10.0.0.0/8>

Matchers	BGP	Actions	BGP Actions
Action:	discard		
Jump Target:			

Filtros BGP: IN & OUT

- Filtros IN: (Martian Routes)



The screenshot shows the 'Route Filters' configuration window in Mikrotik WinBox. It contains a table with 6 columns: #, Chain, Prefix, Prefix Length, Action, and an empty column. The table lists 10 filters (rows 23-32) that block specific IP ranges. The last row (32) is an 'accept' rule.

#	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	

Filtros BGP: IN & OUT

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

New Route Filter

Matchers BGP Actions BGP Actions

Chain: filterIPv4NOMartians

Prefix: ☐ 200.0.0.0/22

Prefix Length: ☐ 22-32

Match Chain:

New Route Filter

Matchers BGP Actions BGP Actions

Action: discard

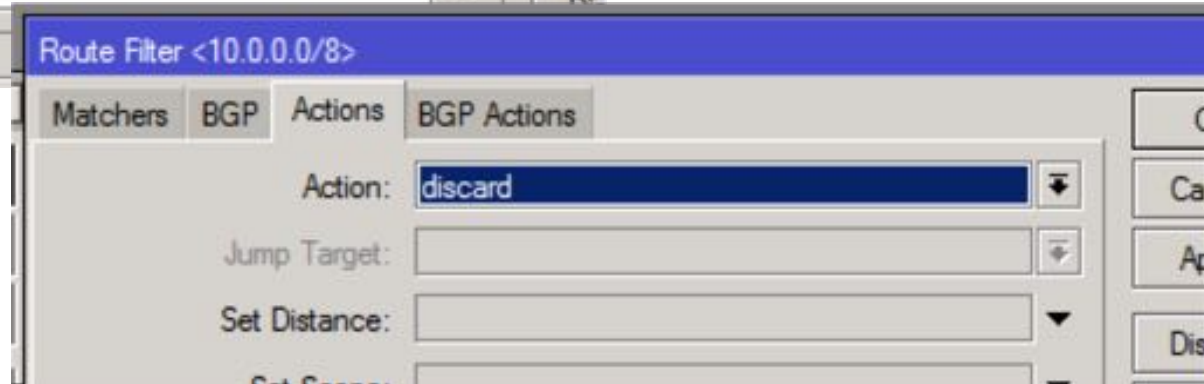
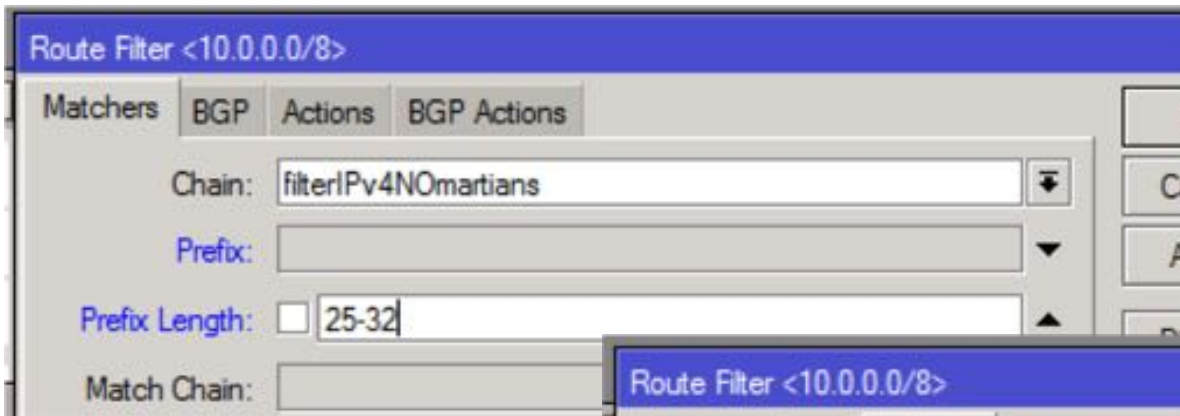
Jump Target:

Set Distance:

Set Scope:

Filtros BGP: IN & OUT

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



Filtros BGP: IN & OUT

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

General Advanced Status

Name: peer_ISP-A

Instance: bgpMiRed

Remote Address: 10.1.1.1

Remote Port:

Remote AS: 7094

TCP MD5 Key:

Nexthop Choice: default

☐ Multihop

☐ Route Reflect

Hold Time: 180

Keepalive Time:

TTL: default

Max Prefix Limit:

Max Prefix Restart Time:

In Filter: filterIPv4NoMartians

Out Filter:

AllowAS In:

Agenda

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

Comunidades BGP

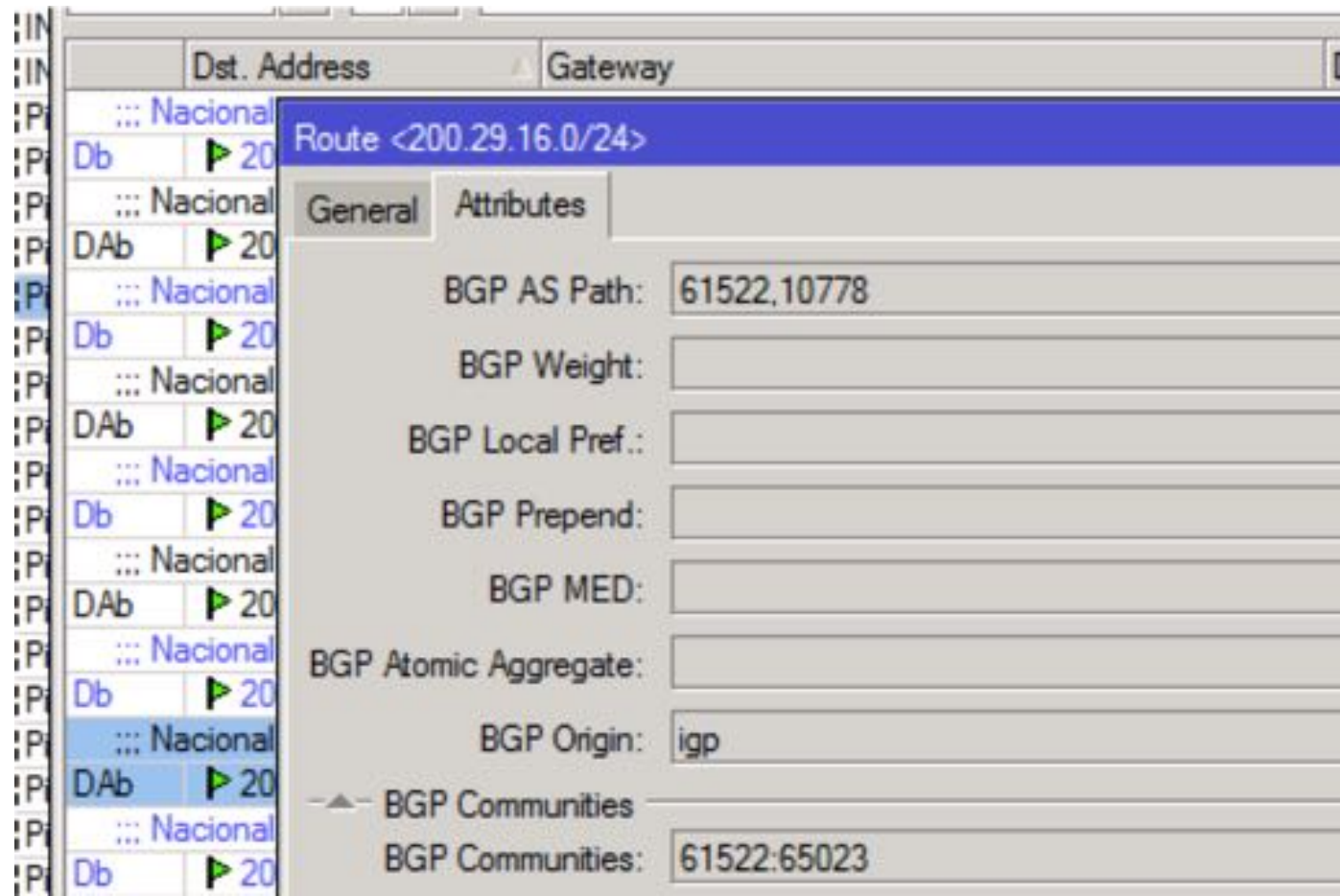
- Que son las comunidades BGP
 - Son un atributo BGP y es un atributo transitivo opcional de longitud variable.
 - Las Comunidades se traspasan de Router a Router, aunque el Router no las “entienda”.
 - A cada prefijo anunciado se le pueden incorporar comunidades.

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.

Comunidades BGP

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



Comunidades BGP

- Como se aplican las Comunidades en Mikrotik

The image shows two overlapping screenshots from the Mikrotik WinBox interface. The top screenshot displays the 'Route Filters' window with a table of filters. The bottom screenshot shows the configuration for a specific route filter, with the 'BGP Actions' tab selected and the 'Set BGP Communities' action configured.

Route Filters Table:

#	Chain	Prefix	Prefix Length	Action
56	ipV4out	200.0.0.0/22		accept
58	ipV4out			discard

Route Filter Configuration (200.0.0.0/22):

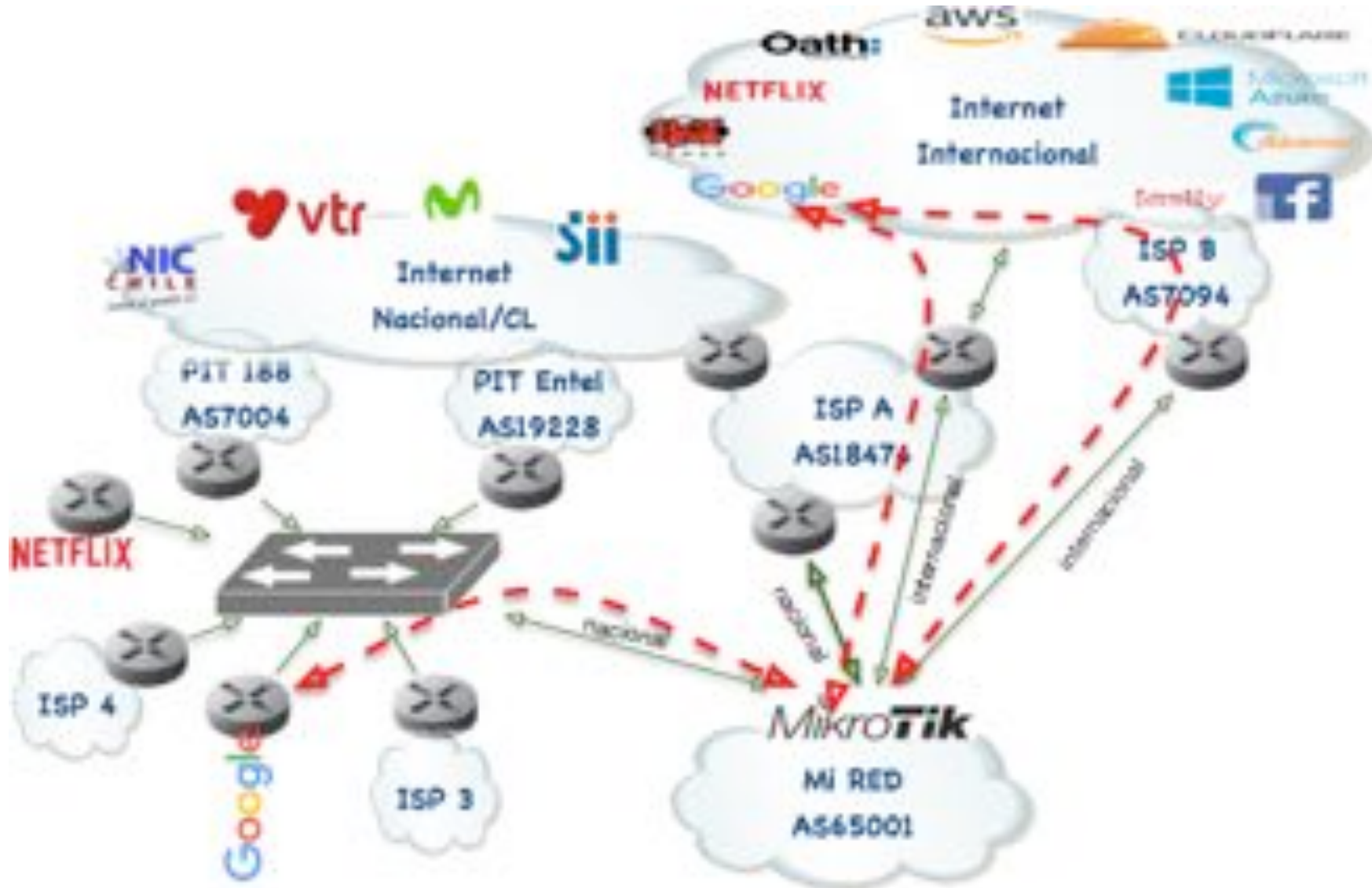
- Tab: **BGP Actions**
- Set BGP Weight: []
- Set BGP Local Pref.: []
- Set BGP Prepend: []
- Set BGP Prepend Path: []
- Set BGP MED: []
- Set BGP Communities: **15169:13000**
- Append BGP Communities: []

Comunidades BGP

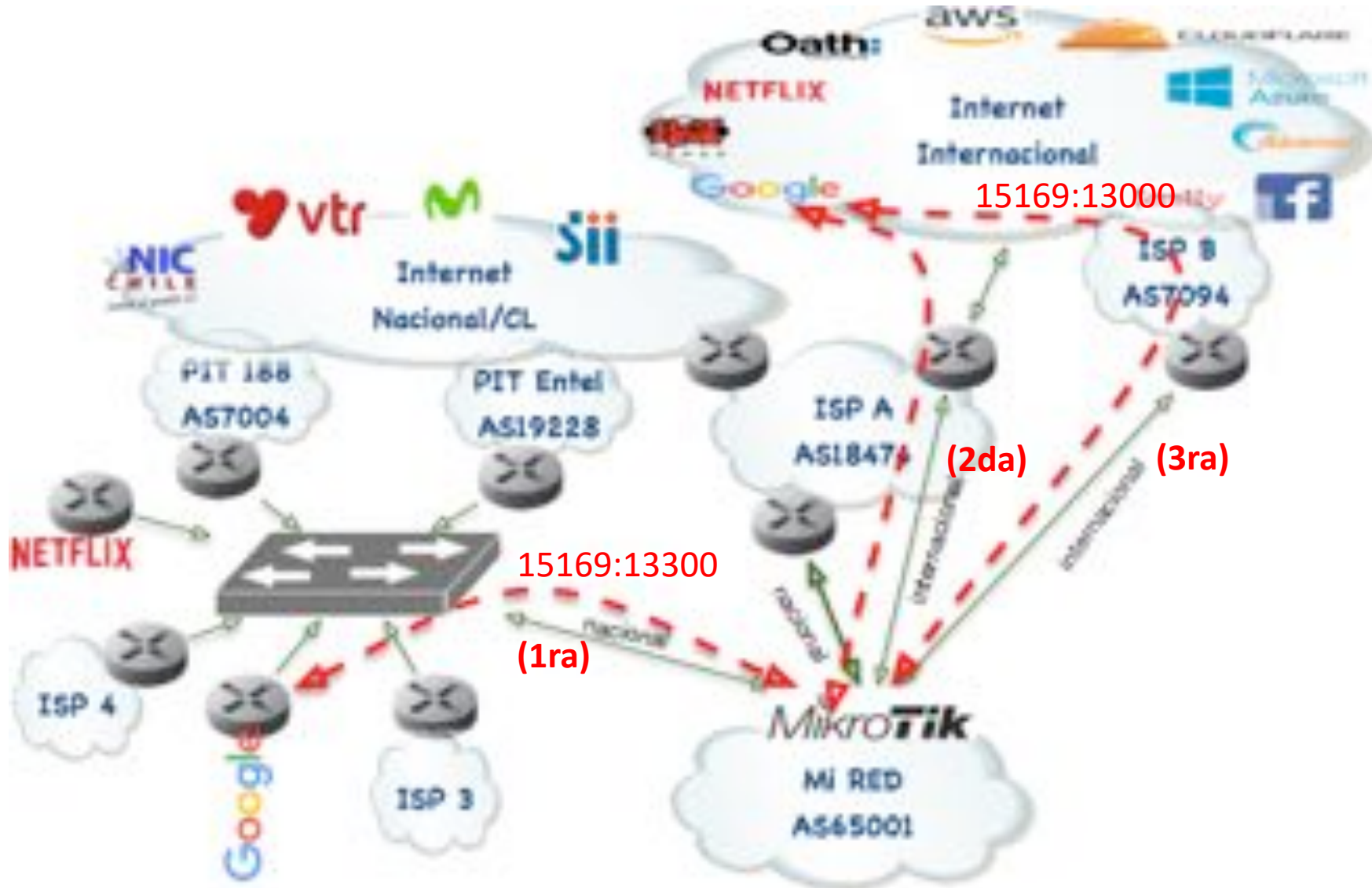
- Ejemplo Peering con Google (AS15169):

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).

Comunidades BGP



Comunidades BGP



Comunidades BGP

- Ejemplo Peering con Netflix (AS2906):

<https://www.netflix.com>

- AWS
- Streaming
 - OCA



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

Comunidades BGP

- Como verificar desde cual OCA recibo una pelicula?

Shift + Ctrl + Alt + Cmd + D

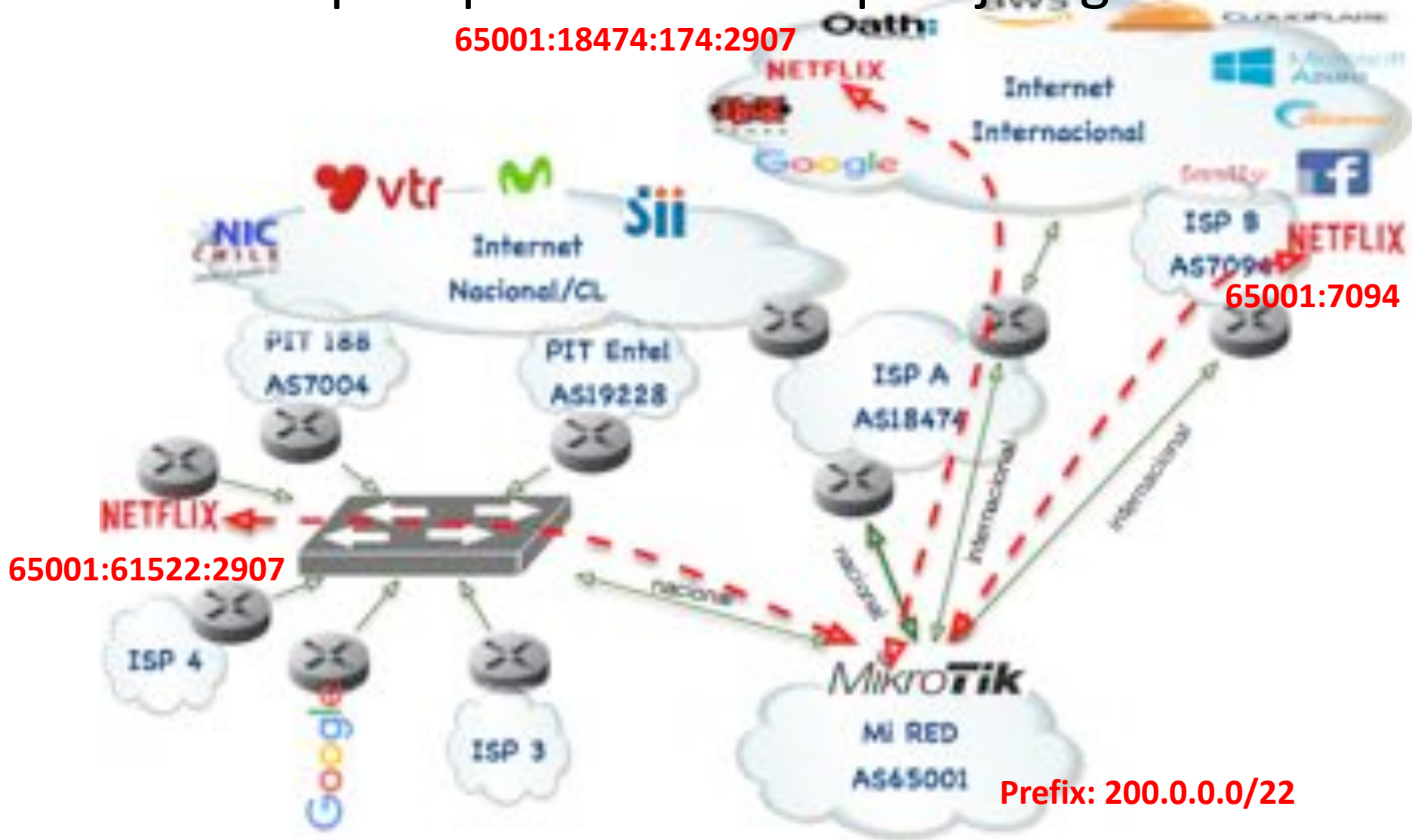


Buffering bitrate (a/v): 96 / 846
Buffer size in Bytes (a/v): 3167429 / 35612411
Buffer size in Bytes: 38779840
Buffer size in Seconds (a/v): 249.604 / 244.672
Current CDN (a/v): c001.sdc002.telefonica-cl.isp.nflxvideo.net, I: 50151 / c001.sdc0
Audio Track: en, Id: A:1:1;2;en;1;, Channels: 2.0, Codec: audio/mp4;codecs=mp4a.4
Video Track: Codec: video/mp4;codecs=vp09.00.11.08.02 (vp9)
Timed Text Track: es, Profile: dfxp-ls-sdh, Id: T:1:0;1;es;0;0;
Framerate: 23.977
Current Dropped Frames: 0

Comunidades BGP

- Calculo para publicación de prefijos iguales

65001:18474:174:2907



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}

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))

Comunidades BGP

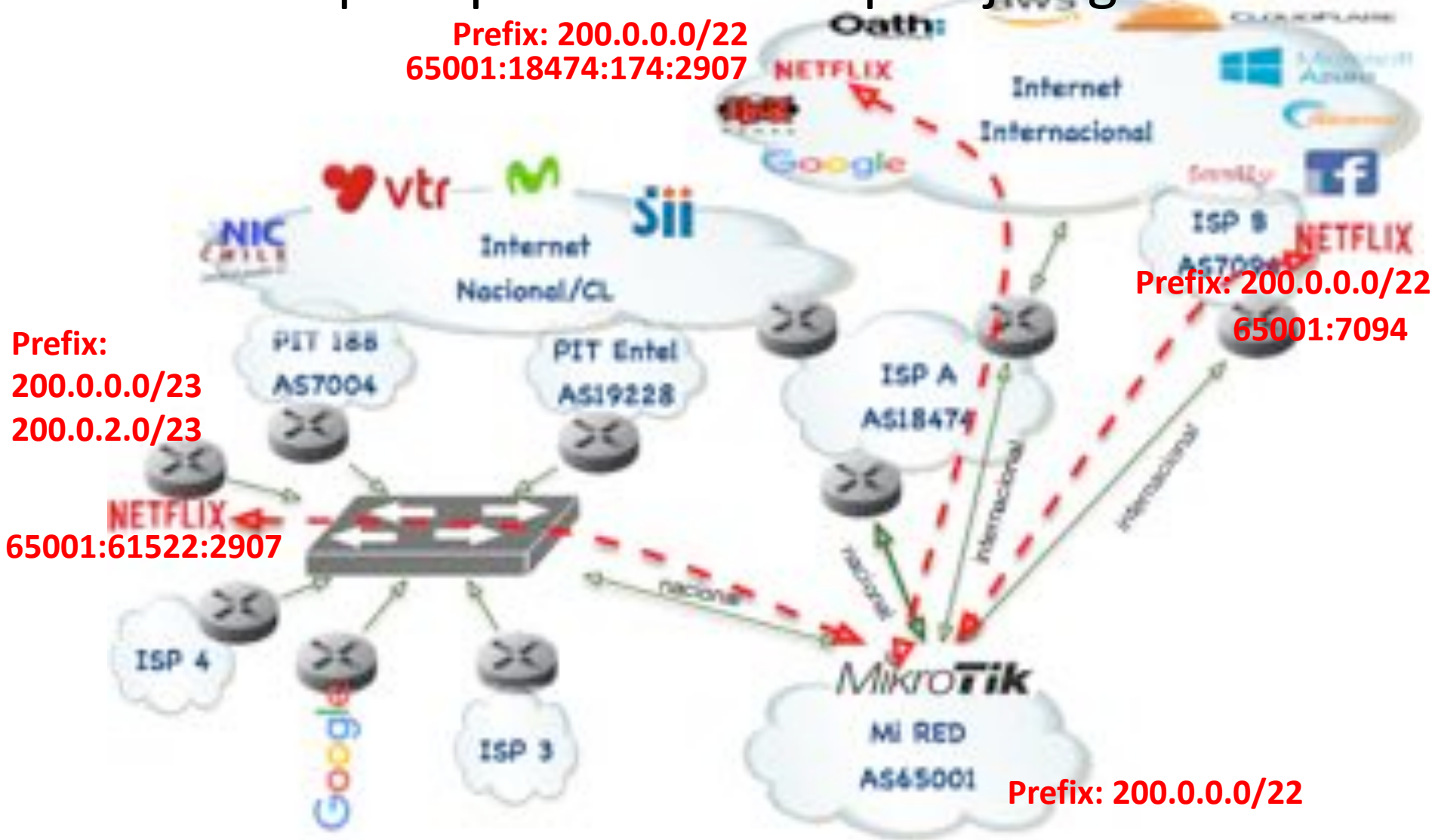
- Calculo para publicación de prefijos iguales

Prefix: 200.0.0.0/22
65001:18474:174:2907

Prefix:
200.0.0.0/23
200.0.2.0/23

Prefix: 200.0.0.0/22
65001:7094

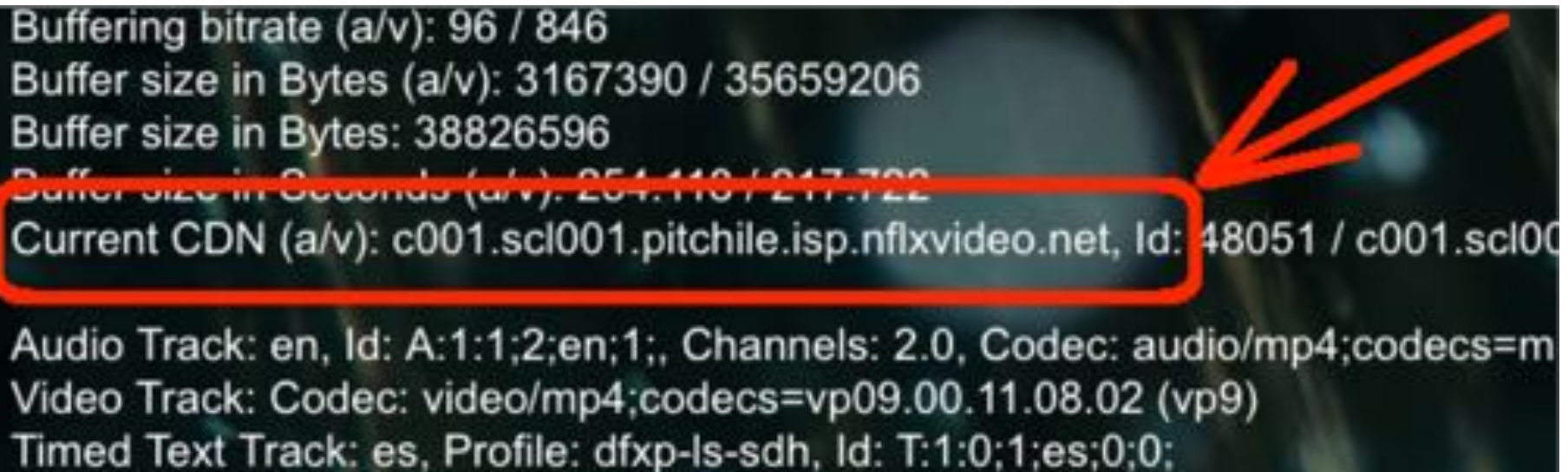
Prefix: 200.0.0.0/22



Comunidades BGP

- Como verificar desde cual OCA recibo una pelicula?

Shift + Ctrl + Alt + Cmd + D



Buffering bitrate (a/v): 96 / 846
Buffer size in Bytes (a/v): 3167390 / 35659206
Buffer size in Bytes: 38826596
Buffer size in Seconds (a/v): 254.118 / 217.722
Current CDN (a/v): c001.scl001.pitchile.isp.nflxvideo.net, Id: 48051 / c001.scl00
Audio Track: en, Id: A:1:1;2;en;1;, Channels: 2.0, Codec: audio/mp4;codecs=m
Video Track: Codec: video/mp4;codecs=vp09.00.11.08.02 (vp9)
Timed Text Track: es, Profile: dfxp-ls-sdh, Id: T:1:0;1;es;0;0;

A red rectangular box highlights the line "Current CDN (a/v): c001.scl001.pitchile.isp.nflxvideo.net, Id: 48051 / c001.scl00". A red arrow points from the right side of the box towards the top right corner of the image.

Agenda

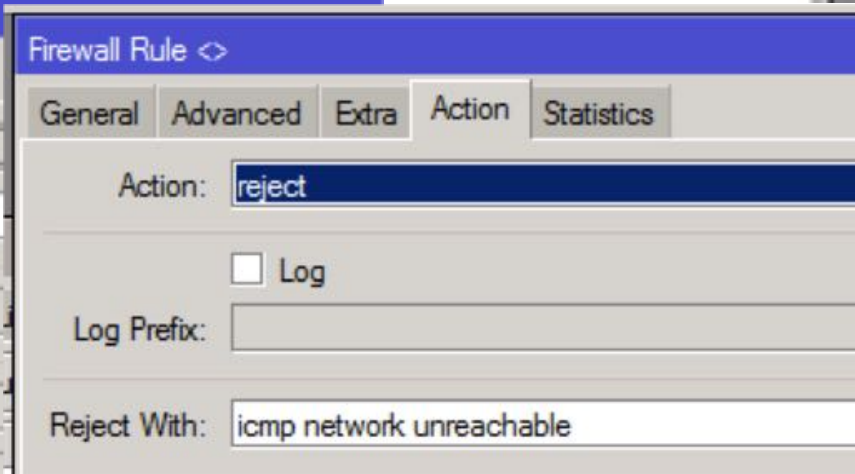
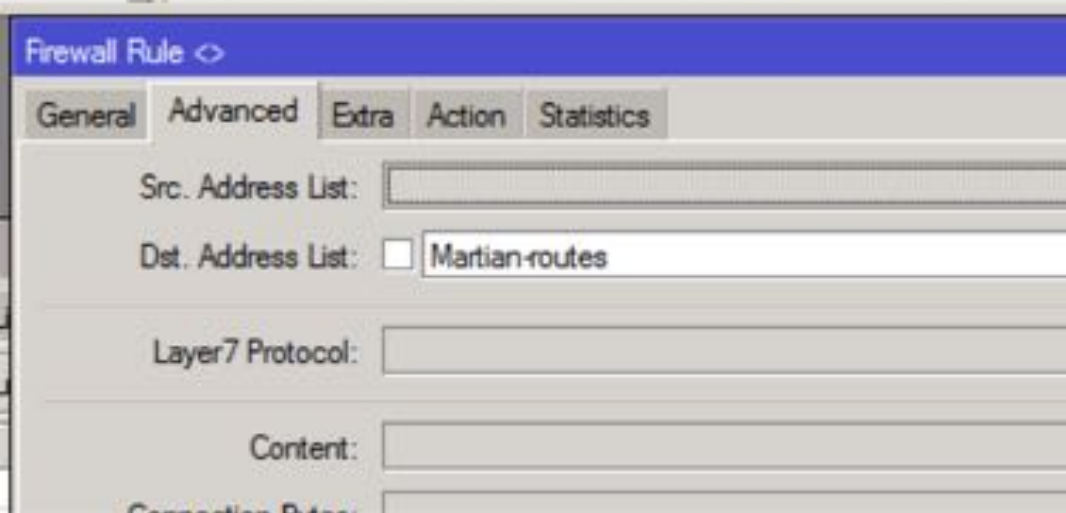
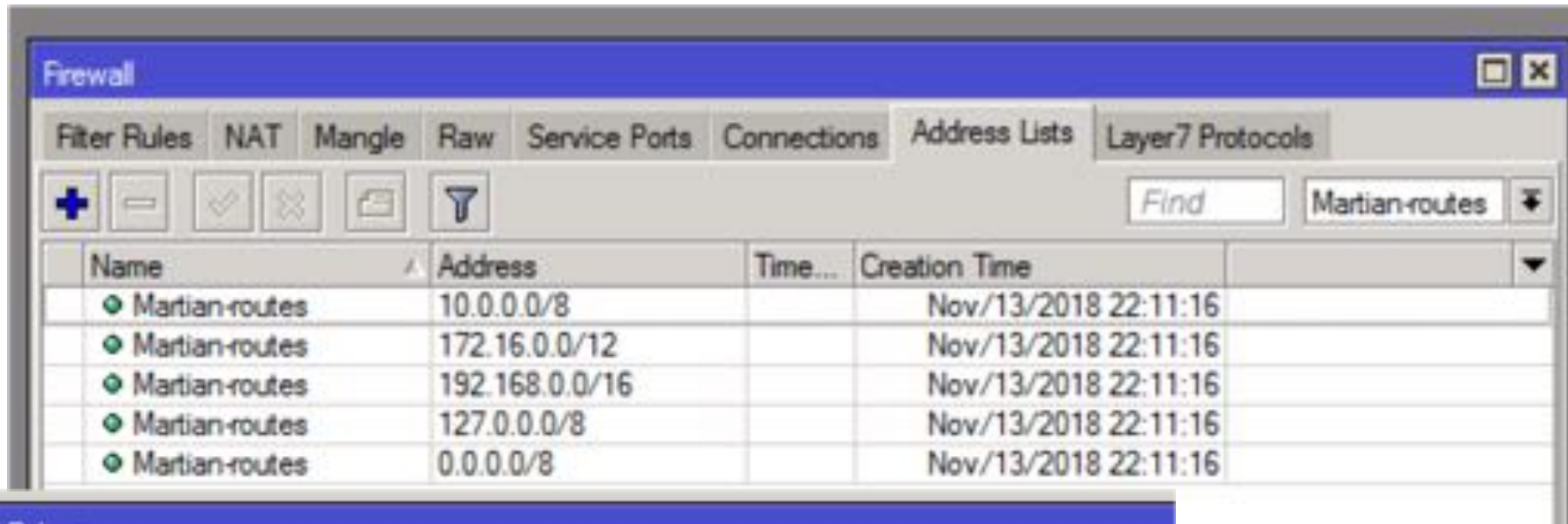
- Introducción
- creando peers BGP4
- Filtros BGP (in & out)
- Usando Comunidades BGP
- **Filtros de seguridad mínimos**
- Tips para Layer2
- Q & A

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

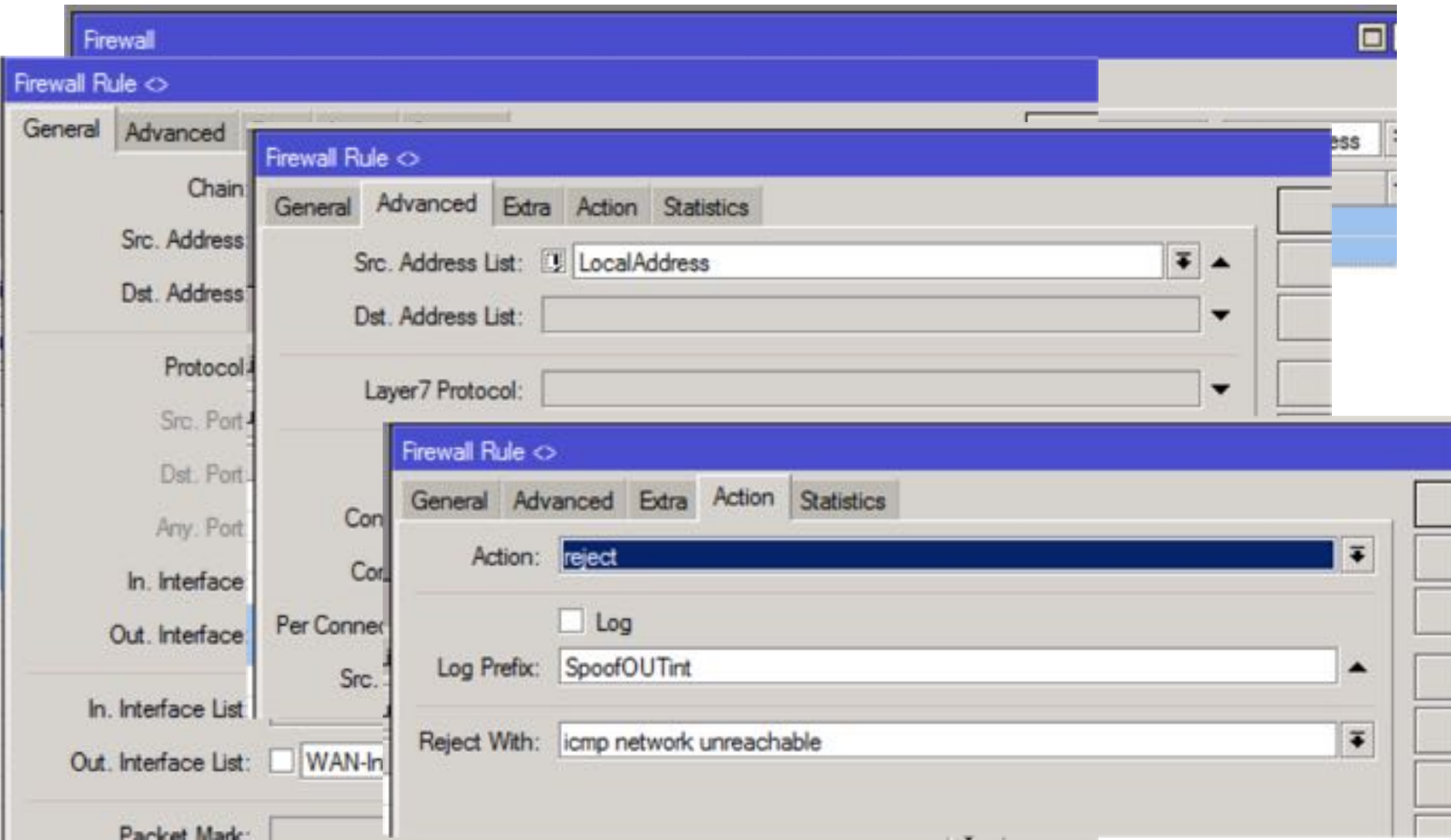
Minimo Security Filters

- Martian Routes Filter:



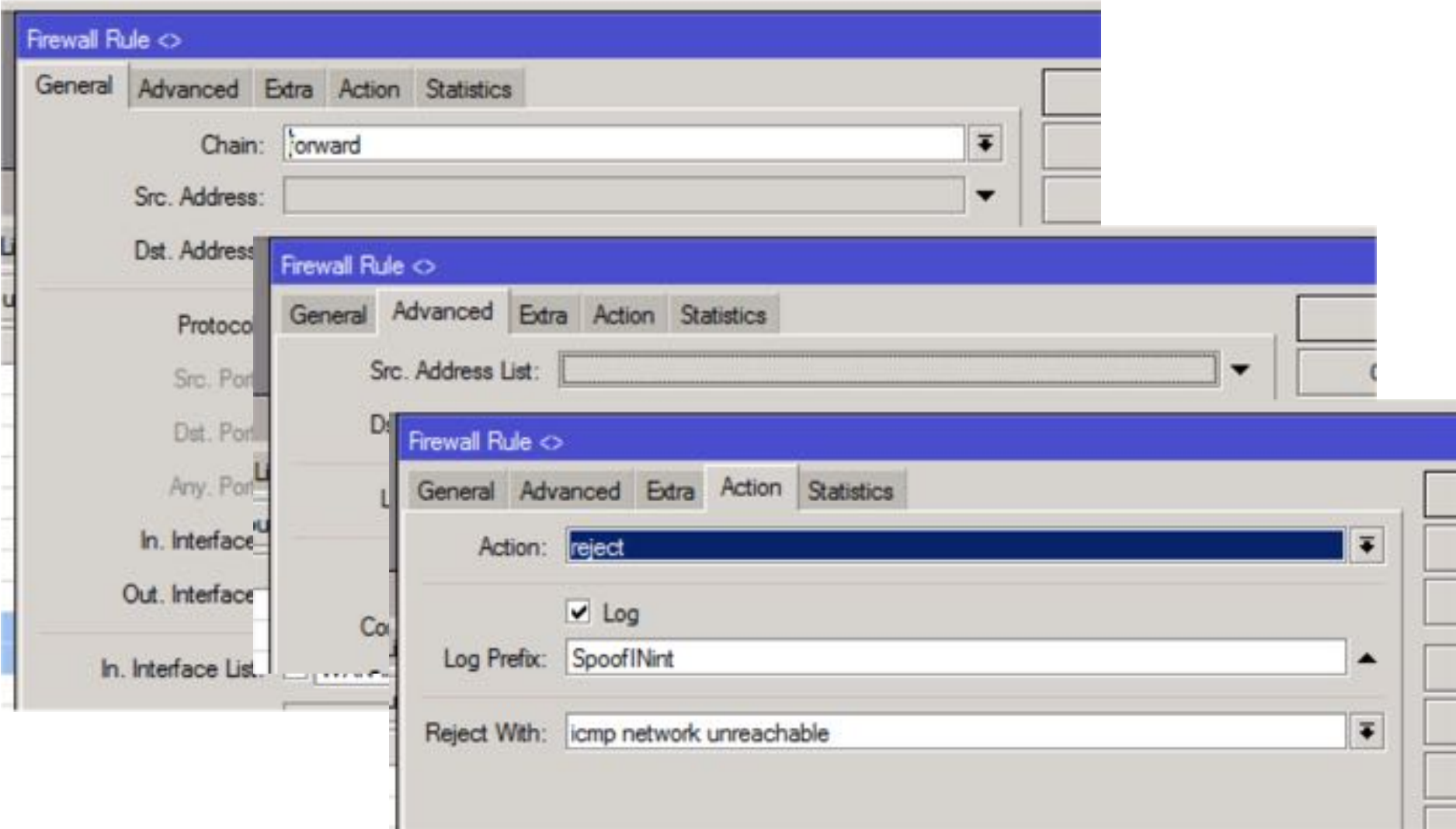
Minimo Security Filters

- Spoofing IP Filter (IN & OUT)



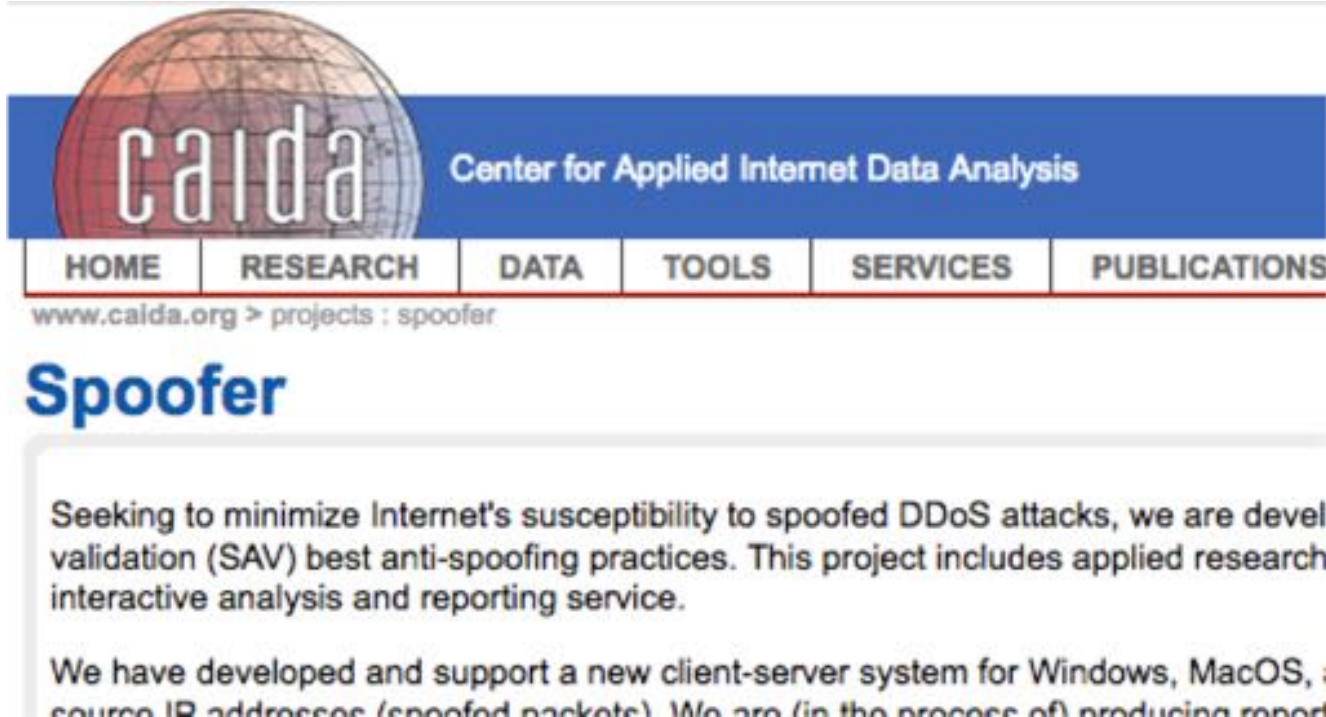
Minimo Security Filters

- Spoofing IP Filter (IN & OUT)



Minimo Security Filters

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



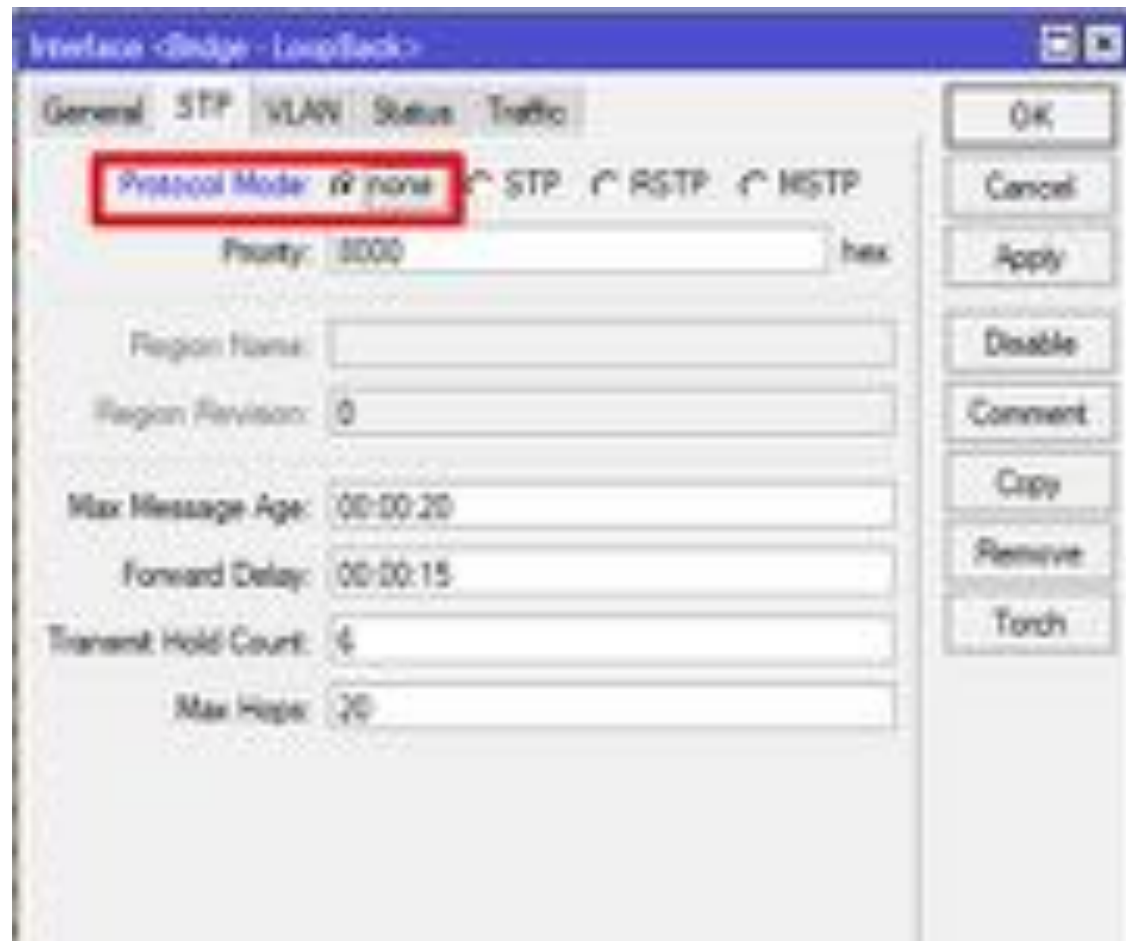
- <https://www.caida.org/projects/spoofer>

Agenda

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

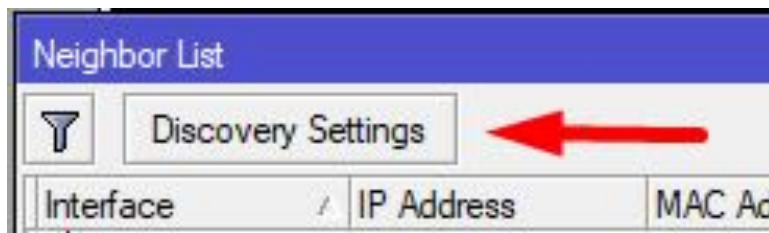
Tips Layer2 IXP

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



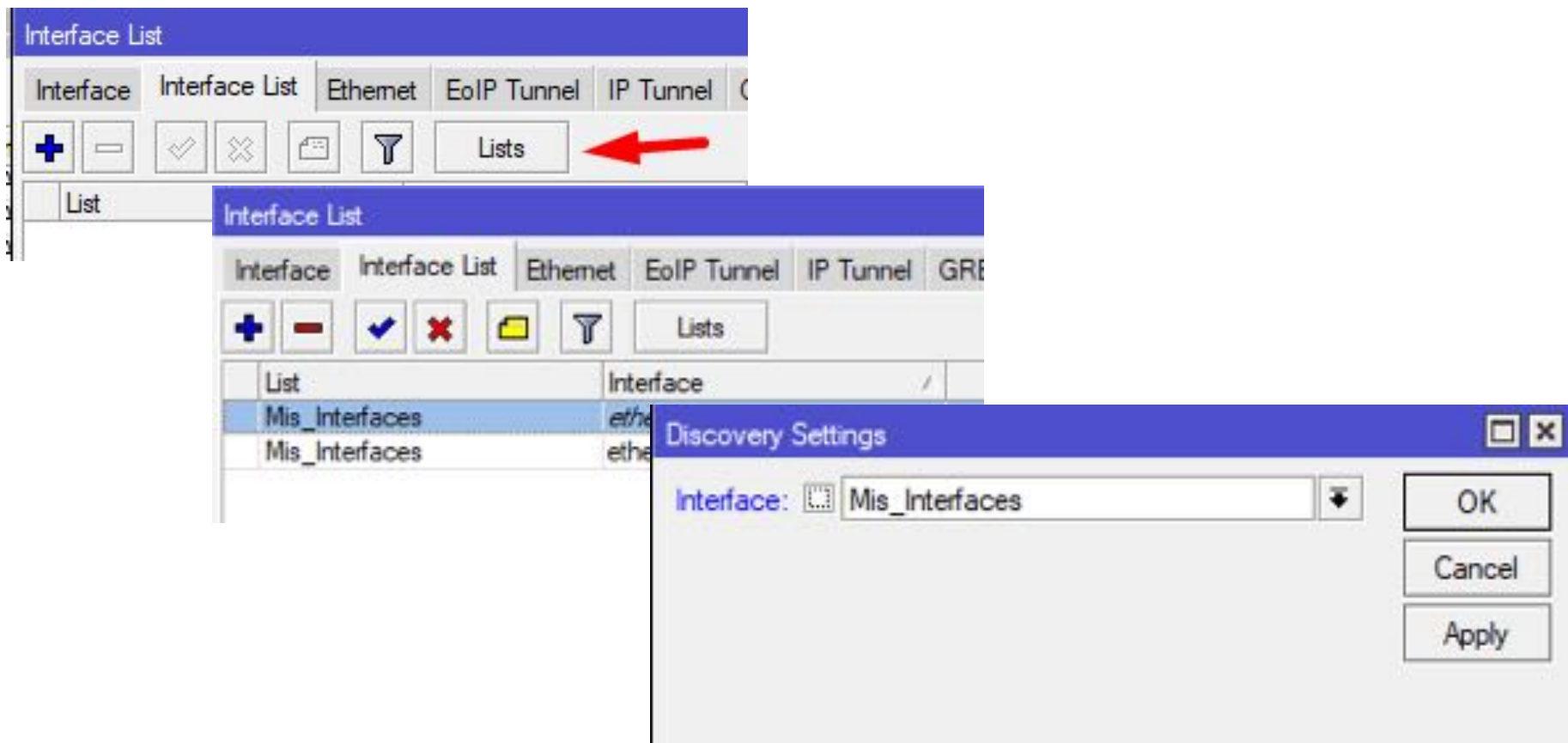
Tips Layer2 IXP

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



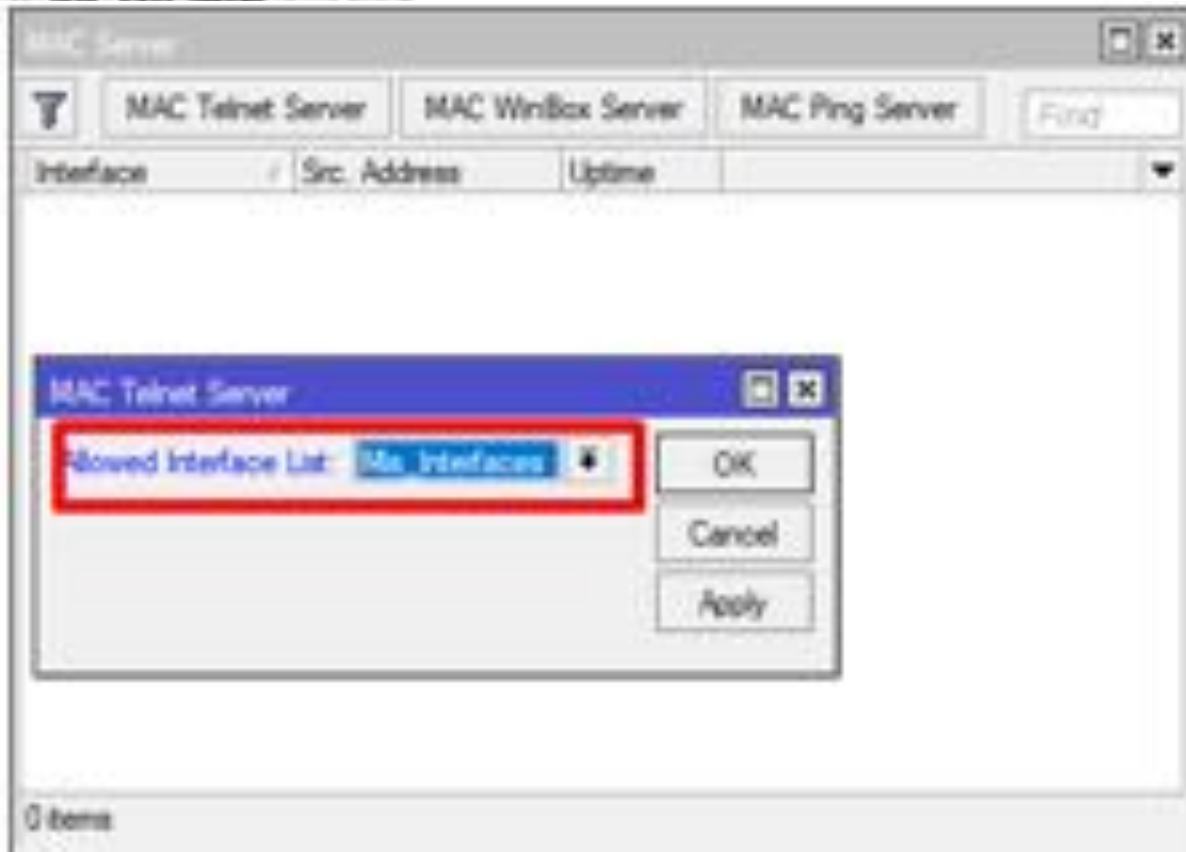
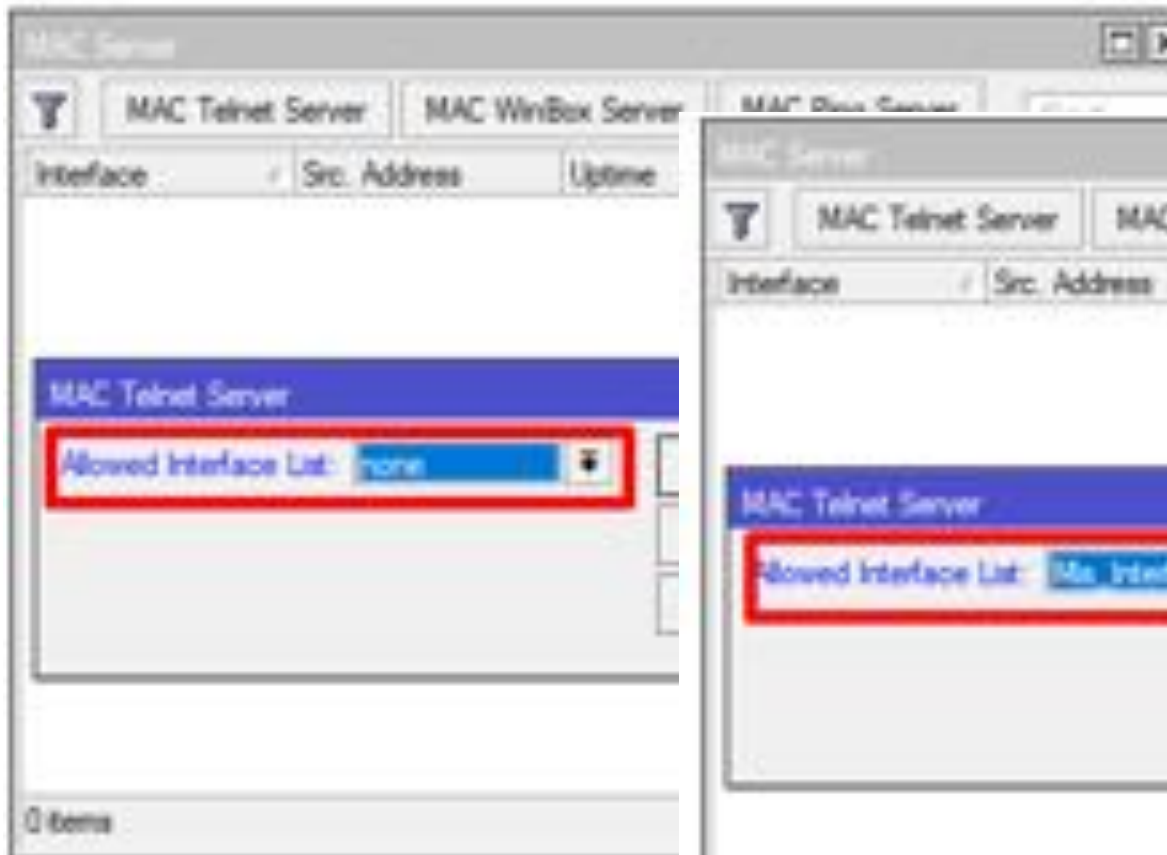
Tips Layer2 IXP

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



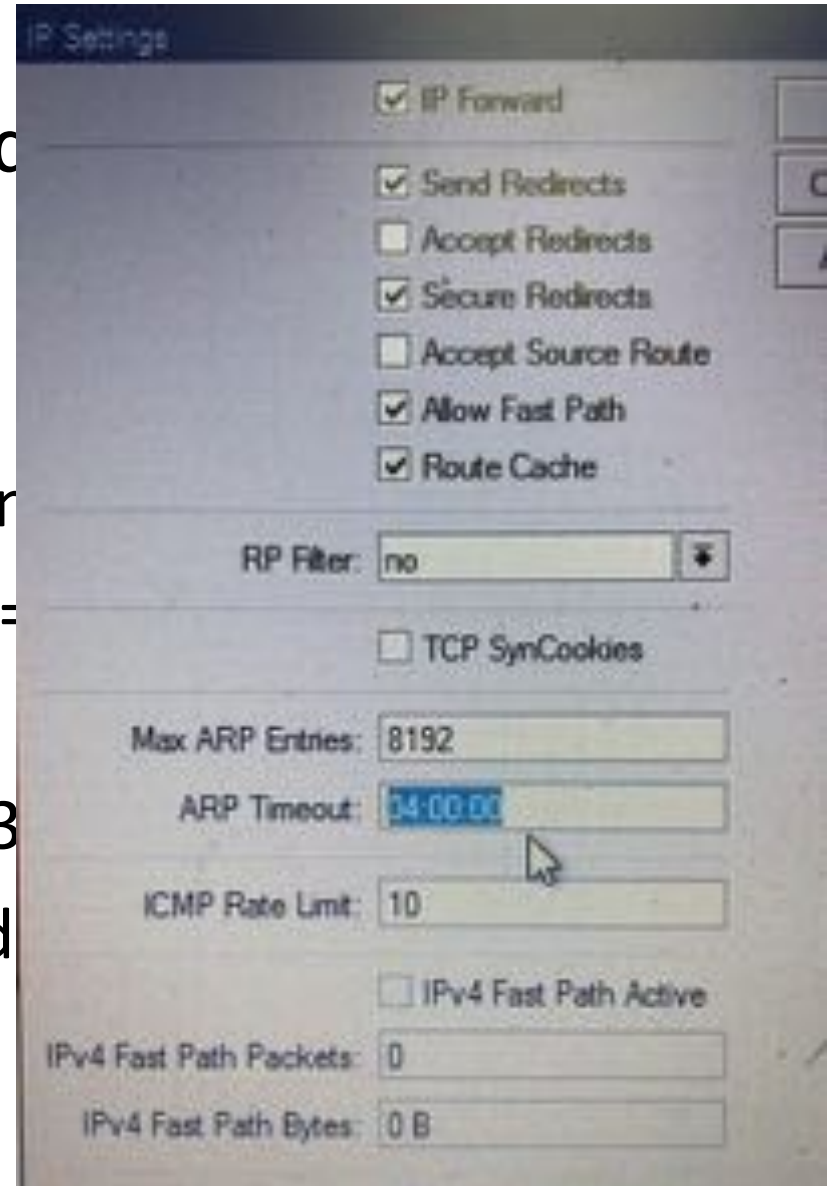
Tips Layer2 IXP

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



Tips Layer2 IXP

- Mejorando la seguridad de
- RTP Timeout
 - Mikrotik Default: 30 segundos
 - `/ip settings set arp-timeout=`
 - Por interfaz (versión ≥ 6.3)
 - `/interface ethernet set [find`
 - `timeout=4h`



Agenda

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

Q & A

Tips & Tricks to connect to a Layer2 IXP

MUM Chile 2019

