Buenas prácticas en enrutamiento de borde para nuevos sistemas autónomos (ISPs)

MUM 2019 – 11 de Febrero - CHILE

Por: João Alberto Barbosa de Oliveira

¿Quien soy?

- Brasileño
- Postgrado en gestión y seguridad en redes - UEG 2016;
- Gerente de Redes - Radar Internet y InternetUP;
- Certificaciones Mikrotik: MTCNA, MTCTCE, MTCIPv6E, MTCRE, MTCINE y TRAINER
- Fundador y Trainer Oficial - Pro Networks;
- Artículo: "*Boas Práticas em roteamento de borda para Sistemas autônomos provedores de acesso à internet em processo de Dual Stack" – UEG 2016*

Agradecimiento a Chile y Chilenos

- Hoy, hace 15 días que estoy aquí, y todos los detalles me encantaron, pude conocer a Viña del Mar, Valpo y Santiago.
- La simpatía de las personas, los lugares son hermosos!

Felicitaciones a los Chilenos! :D

Radar Internet

- 37 ciudades en el estado de Goiás – BR;
- Más de 15Gbps de throughput;
- Red con más de 200 dispositivos Mikrotik;
- Sistema Autónomo (AS);
- Protocolos como BGP y OSPF;
- Atiende clientes domésticos y transito a otros ASs;

InternetUP

- 2 ciudades en el estado de Goiás – BR;
- 100% de routers Mikrotik;
- Sistema Autónomo (AS);
- Protocolos como BGP y OSPF;
- Atiende clientes en Wireless y Fibra óptica;

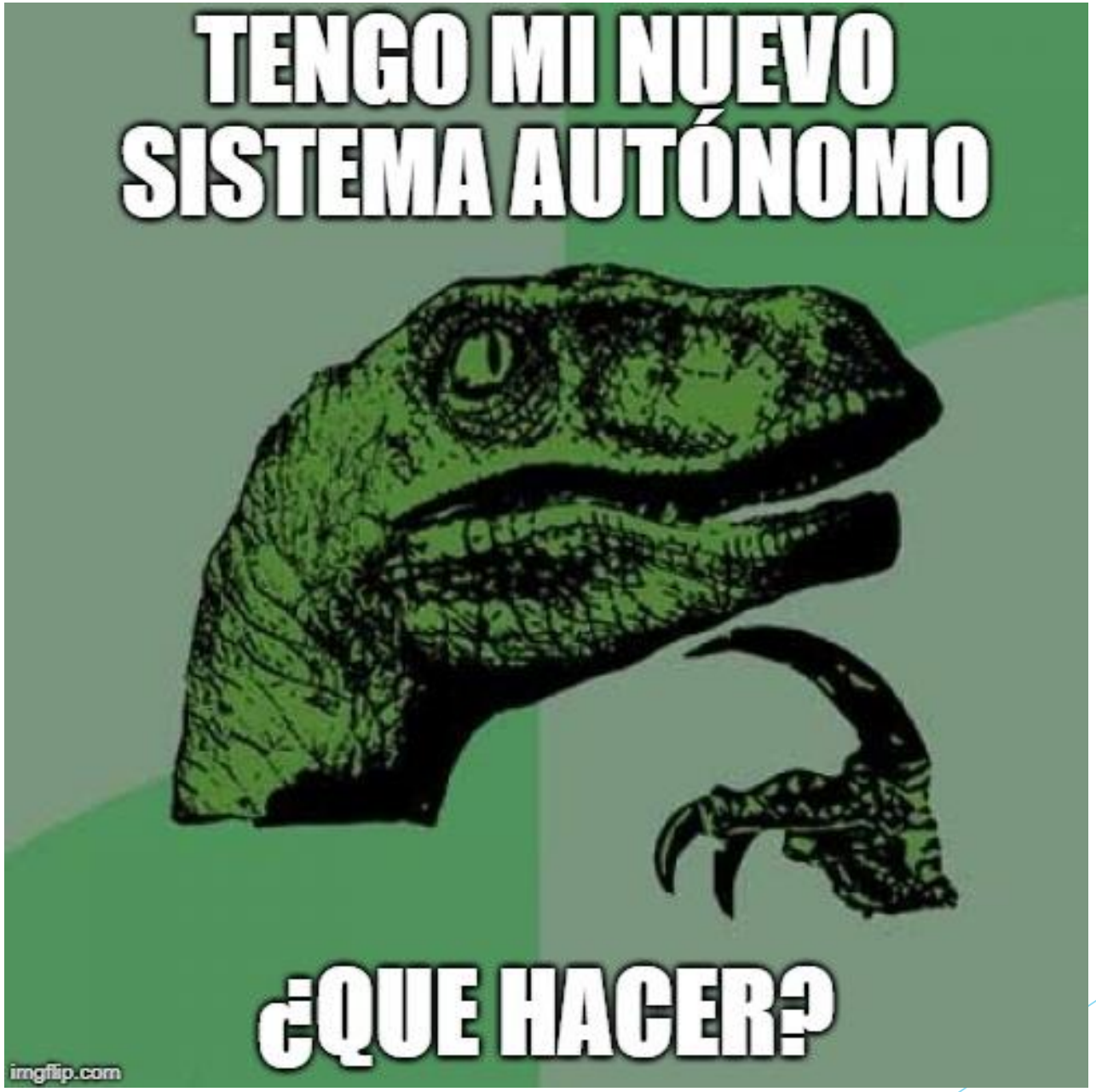
pronetworks

MikroTik
TRAINING CENTER

- Entrenamientos en Redes y Mikrotik (Brasil)

Conociendo a la audiencia

- ¿Quien estás en processo de convertirse a um AS?
- ¿Quien ya posee un AS?


TENGO MI NUEVO
SISTEMA AUTÓNOMO
¿QUE HACER?
imgflip.com

Temas

- Estadísticas / Motivaciones;
- BGP y Dual Stack;
- Autenticación de sesiones BGP;
- Filtrado de prefijos (segmentos) de entrada y salida;
- Filtros de Bogons;
- Buenas prácticas para el sistema operativo RouterOS;
- Algunas herramientas de prueba y resultados;

¿Para quién es esa presentación?

- Nuevos sistemas autónomos (AS);
- Administradores principiantes en BGP;
- Sistemas autonómos simples (que no son tránsitos de otros ASs);
- Quien desea mejorar su configuración de borde;
- Quem desea provechar mejor su router Mikrotik en enrutamiento de borde;

Objectivos

- Incentivar y propagar la adopción de buenas prácticas en AS's proveedores de acceso;
- Orientar nuevos AS's en prácticas inmediatas ante el protocolo BGP bajo IPv4 e IPv6;
- Incentivar a los administradores de redes en la búsqueda y exploración de documentos como BCP's y RFC’s.;
- Demostrar algunos ejemplos de aplicaciones de buenas prácticas (BCP) usando el Mikrotik RouterOS;
- Mejorar la Internet. : D

Recomendación de Lectura! (La BCP 194)

Internet Engineering Task Force (IETF)
Request for Comments: 7454
BCP: 194
Category: Best Current Practice
ISSN: 2070-1721

J. Durand
Cisco Systems, Inc.
I. Pepelnjak
NIL
G. Doering
SpaceNet
February 2015

BGP Operations and Security

Abstract

The Border Gateway Protocol (BGP) is the protocol almost exclusively used in the Internet to exchange routing information between network domains. Due to this central nature, it is important to understand the security measures that can and should be deployed to prevent accidental or intentional routing disturbances.

Más en: https://tools.ietf.org/html/bcp194

Sistemas Autónomos (Estadística 1/5)

- El número de nuevos sistemas autónomos está en aumento, es necesario fomentar el uso de prácticas esenciales para su participación en el contexto de Internet.

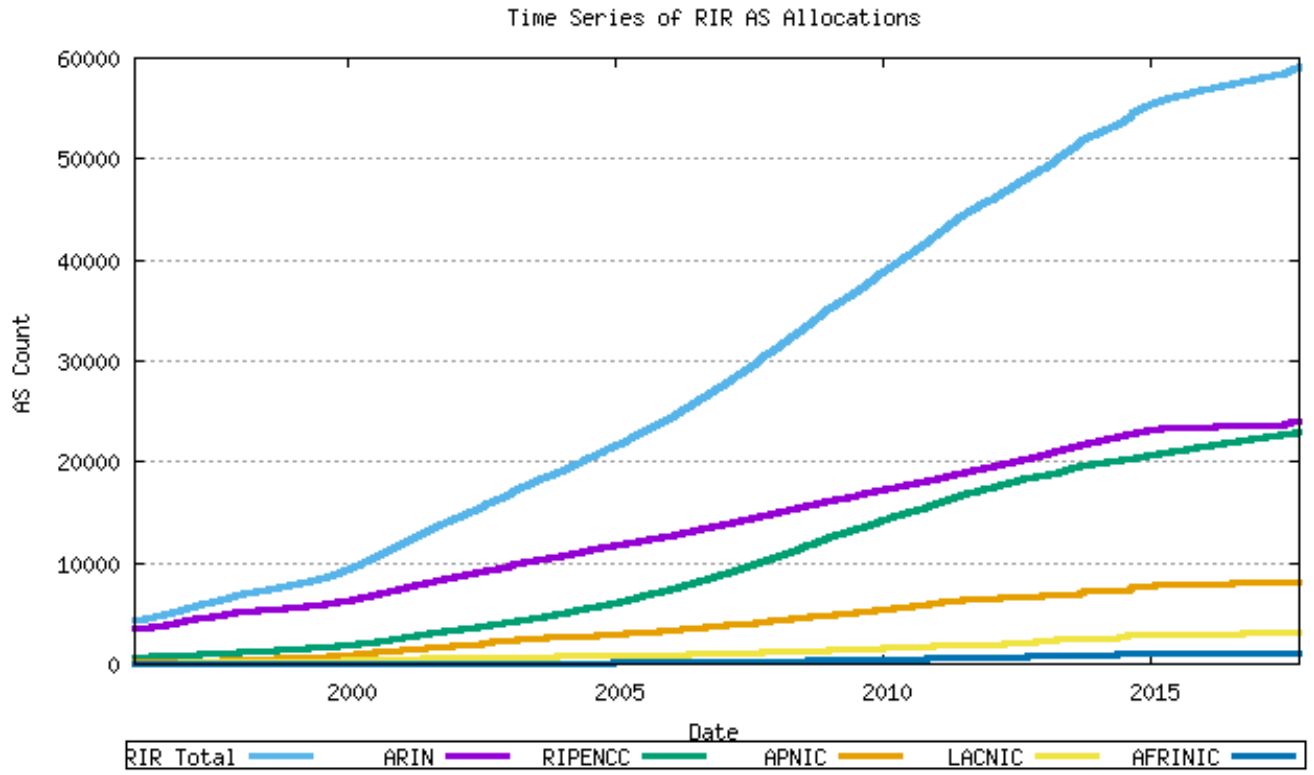
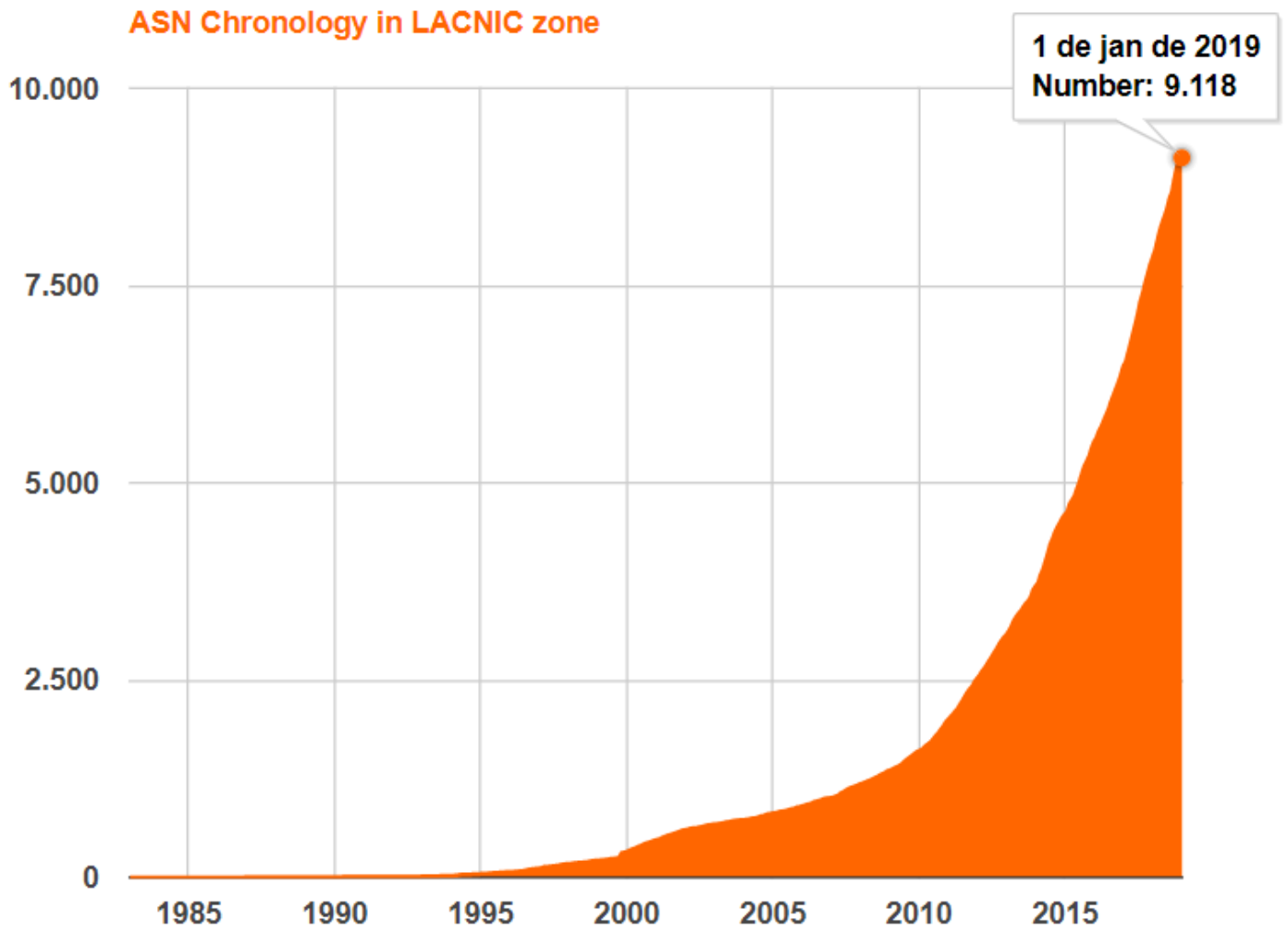


Figura 1 - Asignaciones acumulativas de AS por RIR
Fuente: http://www.potaroo.net/tools/asns/

(Estadística 2/5)

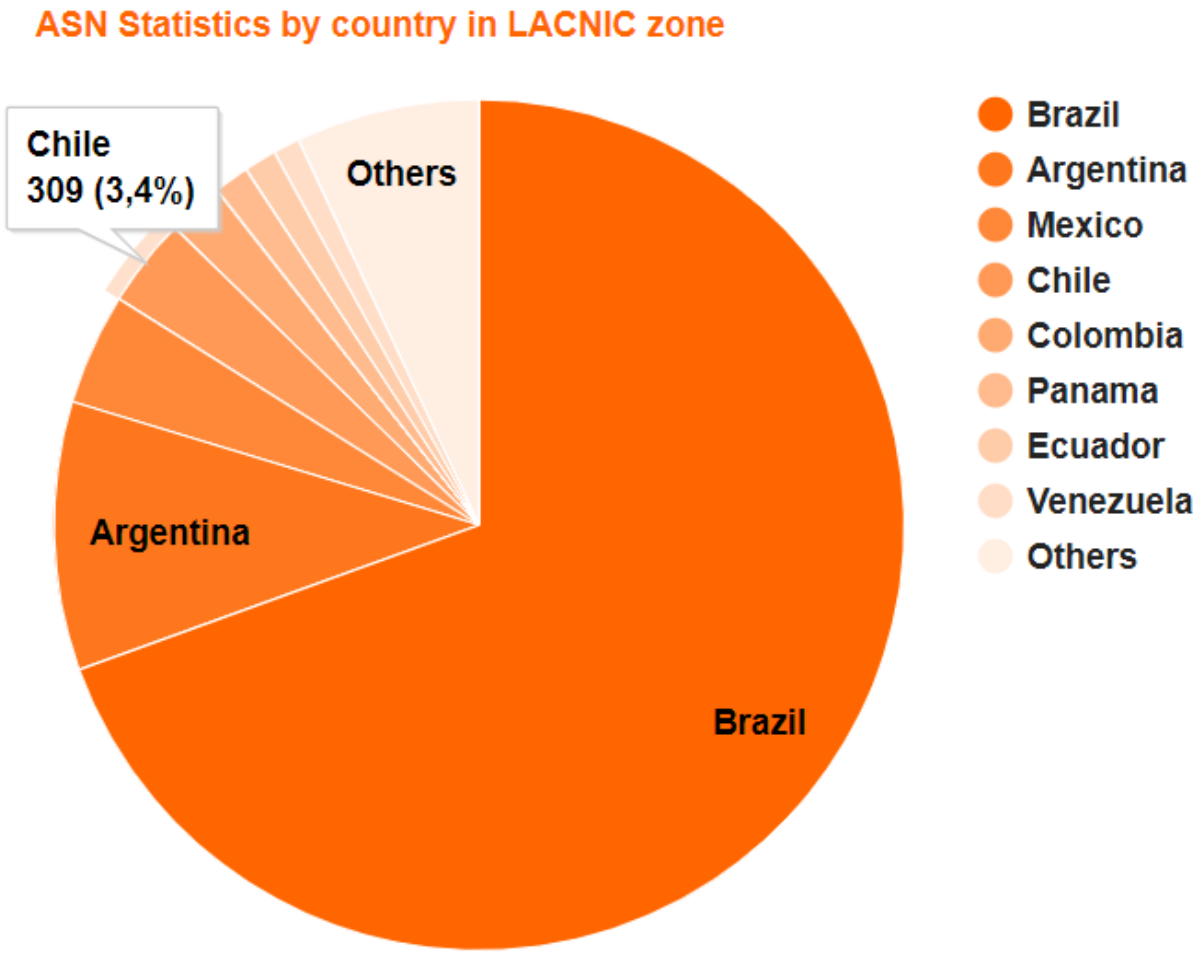
Alocaciones ASN – LACNIC



Fuente: https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

Estadística (3/5)

Alocaciones ASN – LACNIC - 2019



Fuente: https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

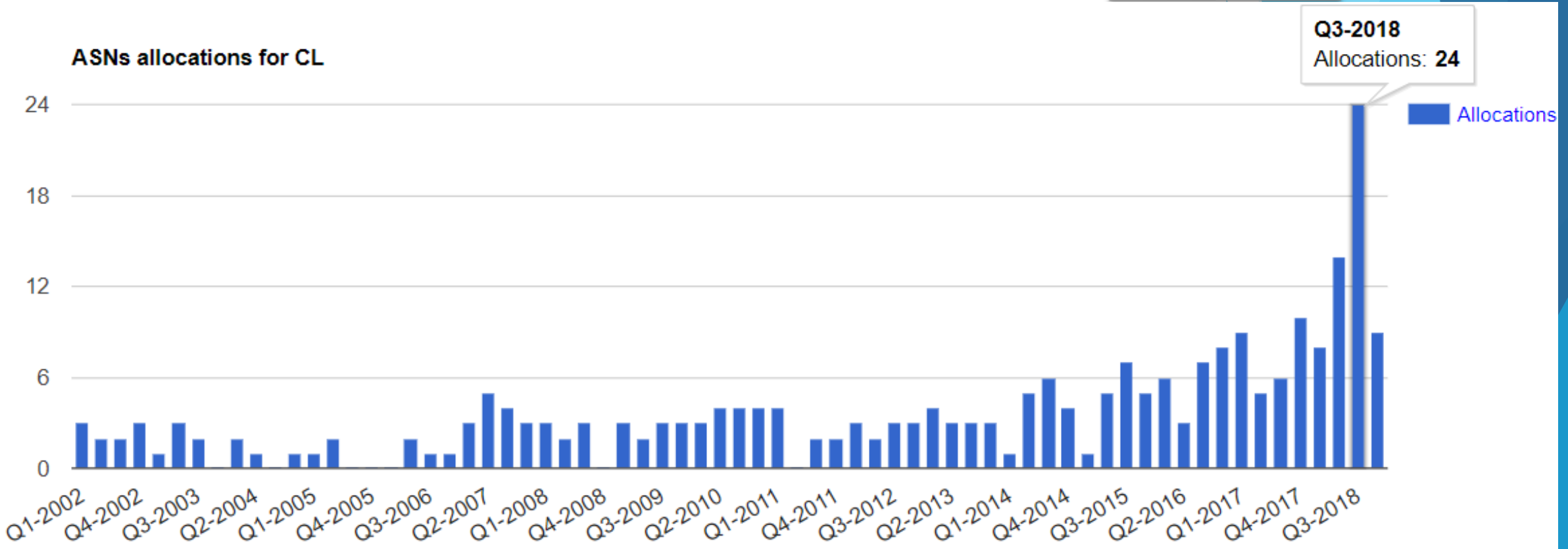
Estadística (4/5)

TOP 10 - Alocaciones - ASN – LACNIC - 2019

Rank	Country	Code	Number	Percentage
1	Brazil	BR	6 335	69.478 %
2	Argentina	AR	930	10.200 %
3	Mexico	MX	386	4.233 %
4	Chile	CL	309	3.389 %
5	Colombia	CO	193	2.117 %
6	Panama	PA	122	1.338 %
7	Ecuador	EC	113	1.239 %
8	Venezuela, Bolivarian Republic of	VE	92	1.009 %
9	Costa Rica	CR	89	0.976 %
10	Honduras	HN	83	0.910 %

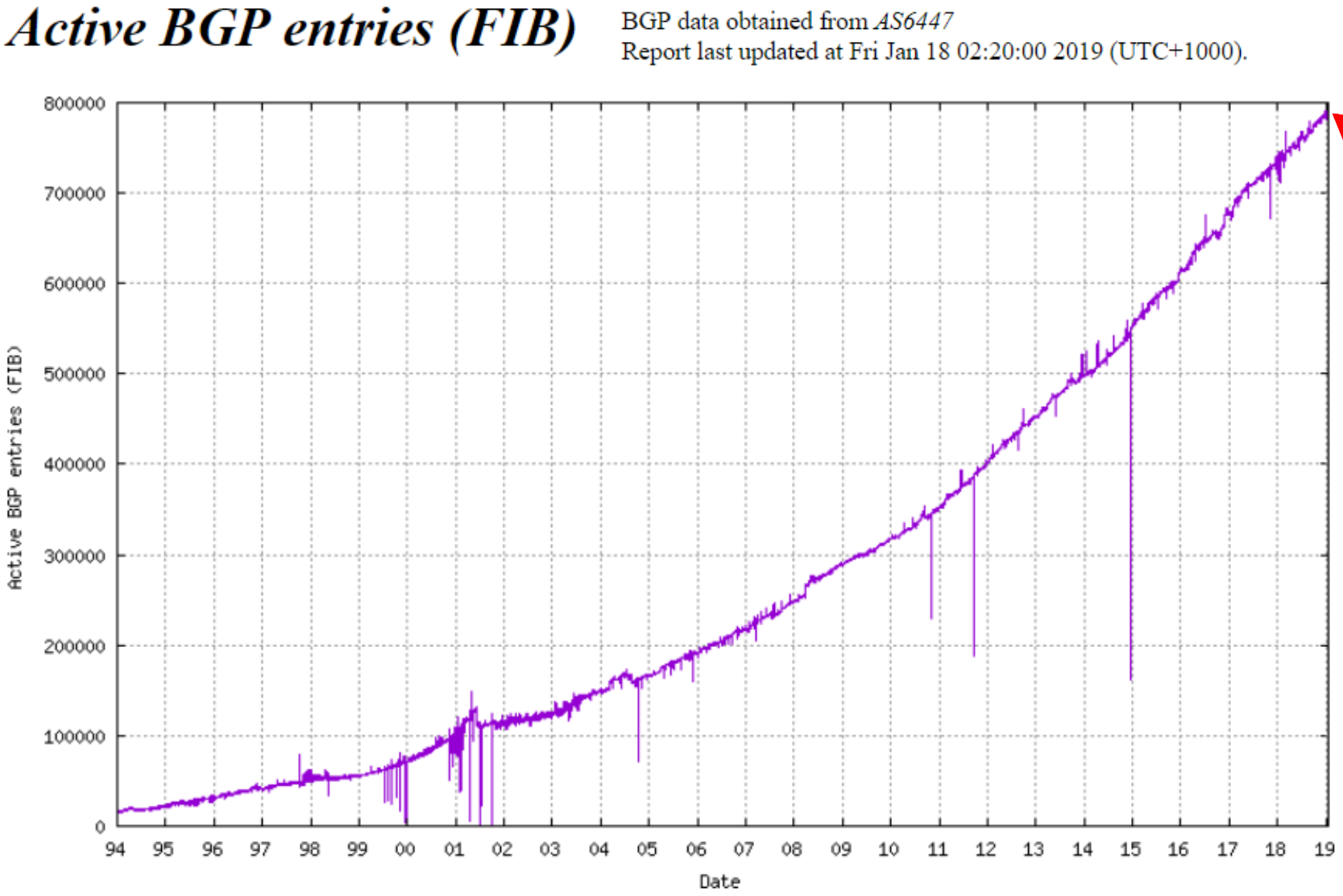
Fuente: https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/LACNIC/ASN-ByNb.html

Estadística (5/5)
Alocaciones ASN – CHILE - 2018



Fuente:https://stats.labs.lacnic.net/REGISTRO/asnpercc.html
Día:18/01/2019

Full Routing (IPv4)



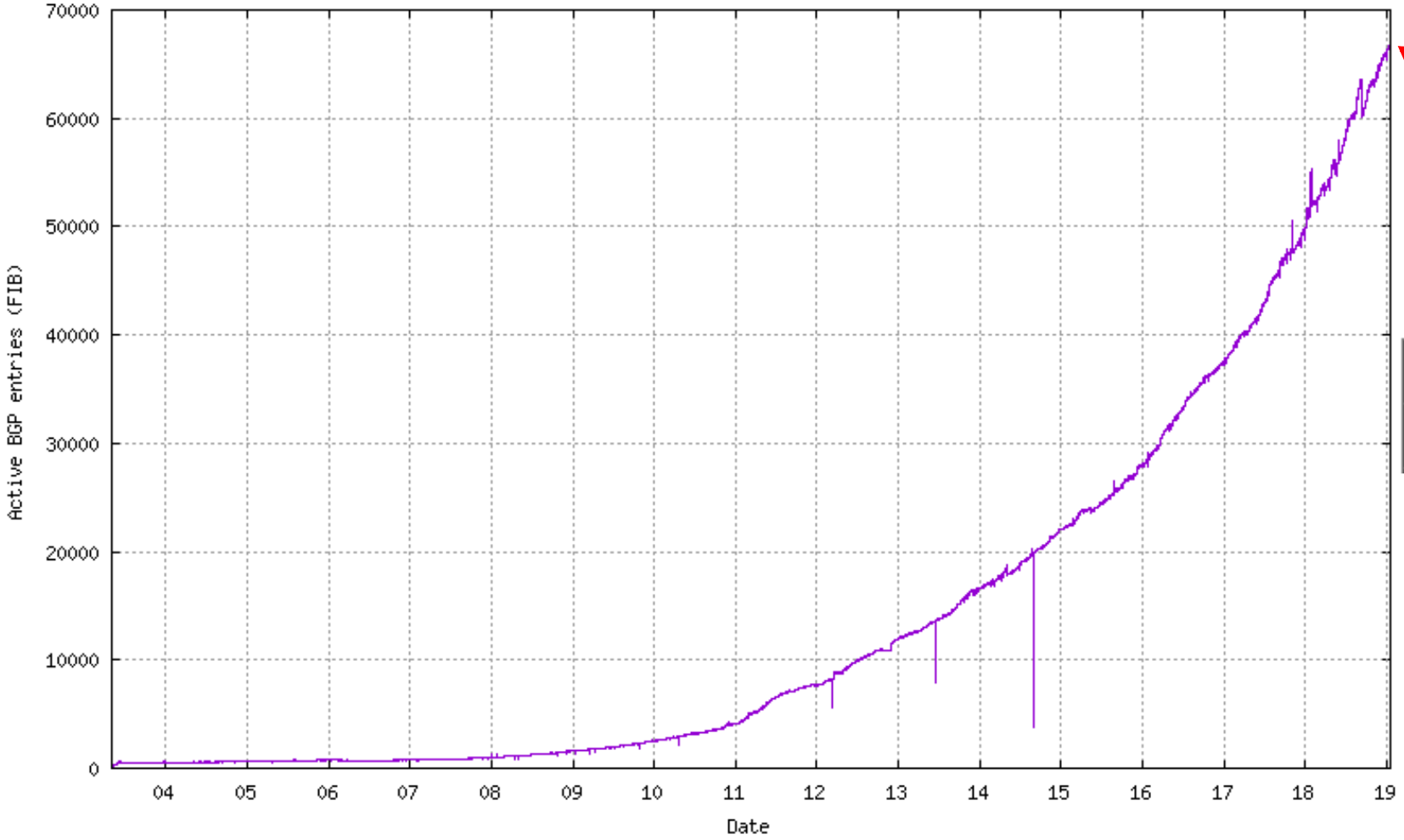
FIB / RIB Table Reports (plots)	Data Sets(txt)
Active BGP entries (FIB)	789681

Fuente: https://bgp.potaroo.net/as6447/

Full Routing (IPv6)

Active BGP entries (FIB)

BGP data obtained from *AS6447*.
Report last updated at Fri Jan 18 04:00:00 2019 (Australian Eastern Time).

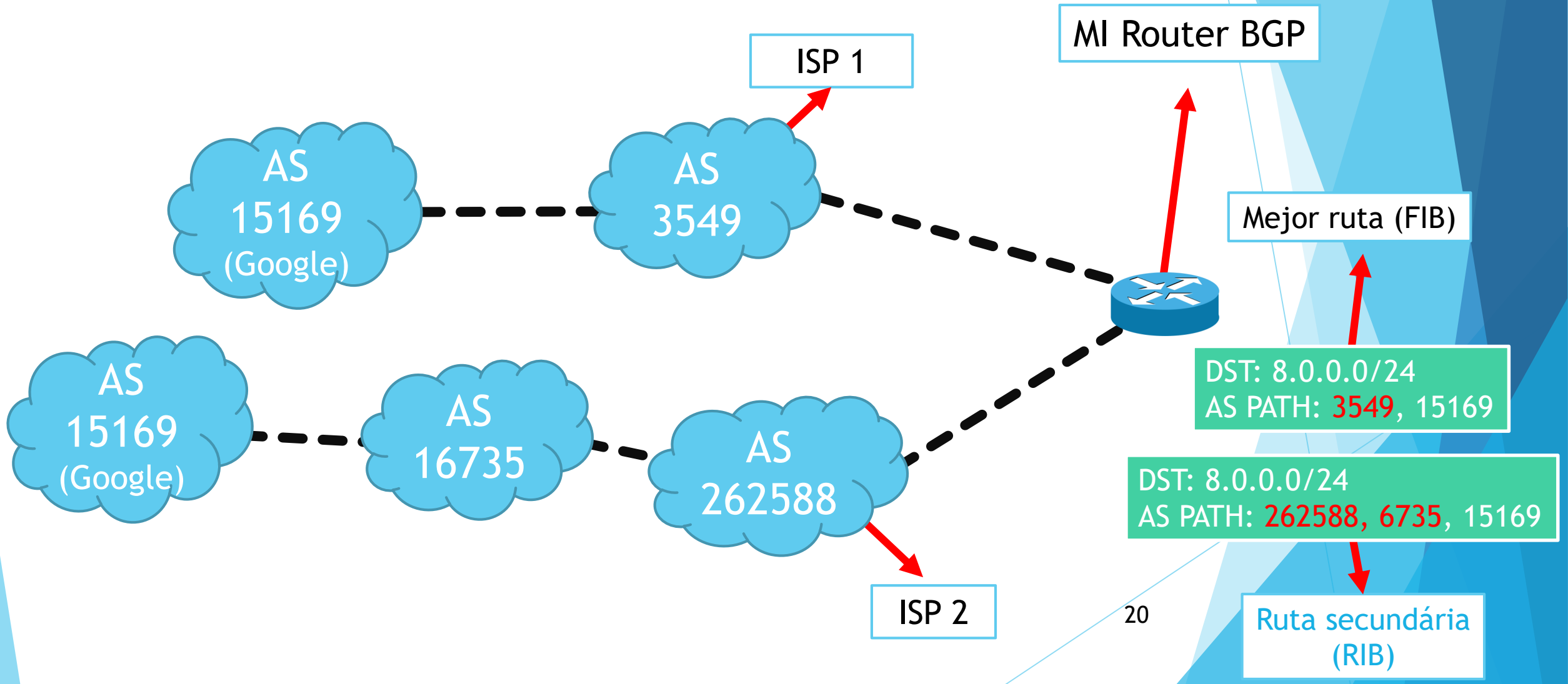


FIB / RIB Table Reports (plots)	Data Sets(txt)
Active BGP entries (FIB)	66778

Fuente: http://bgp.potaroo.net/v6/as6447/

Conceptos fundamentales del BGP

Algoritmo de distancia vector
¿como funciona?



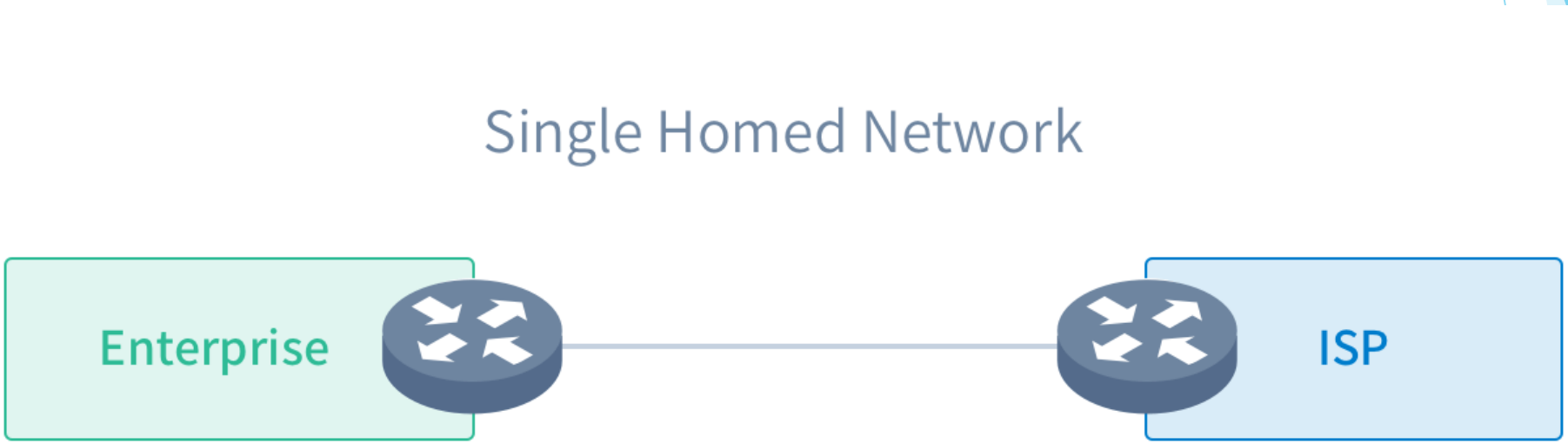
Conceptos fundamentales del BGP

- Opera en el puerto TCP 179;
- Protocolo de enrutamiento para la conexión entre AS en Internet;

- Topologías más comunes:
  - **"Single Homed"**
    - Sólo 1 upstream (operador)
  - **"Multihomed"**
    - 2 o más upstreans (operadores)

Conceptos fundamentales del BGP

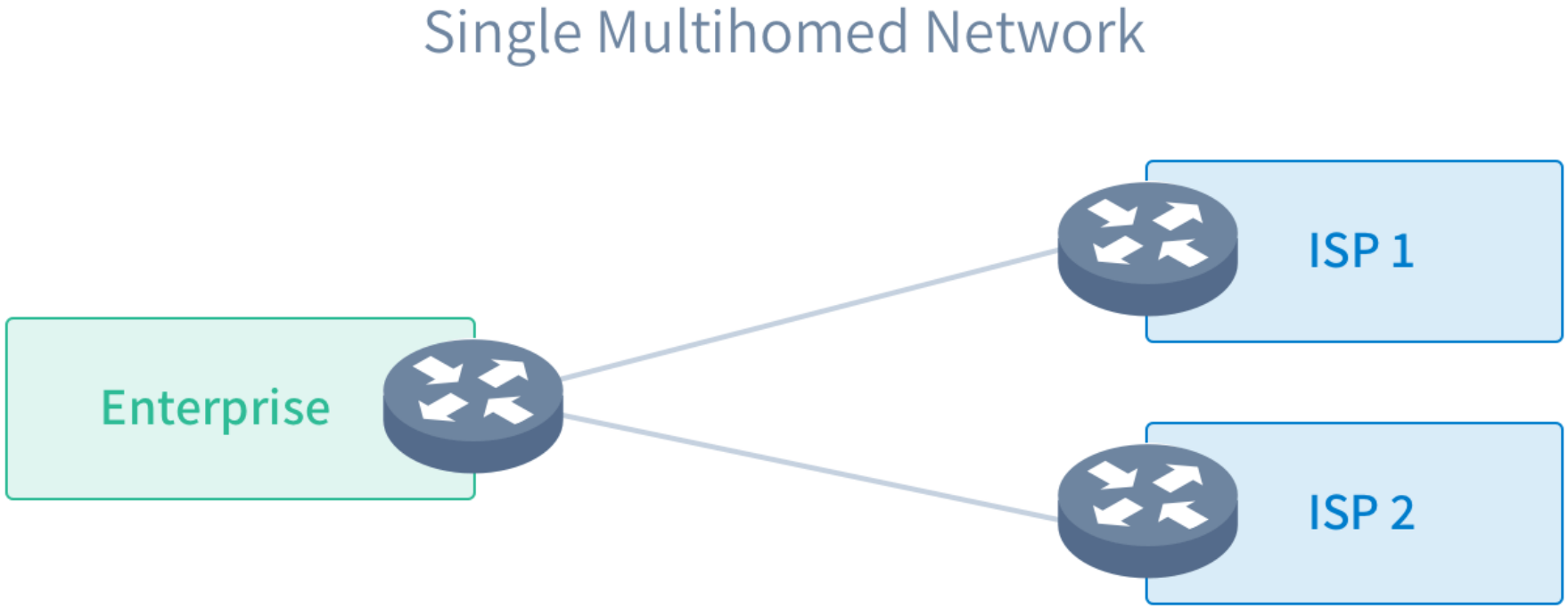
Topologías comunes



Fuente:https://datapacket.com/blog/wp-content/uploads/2017/08/Single_Homed_Network.png

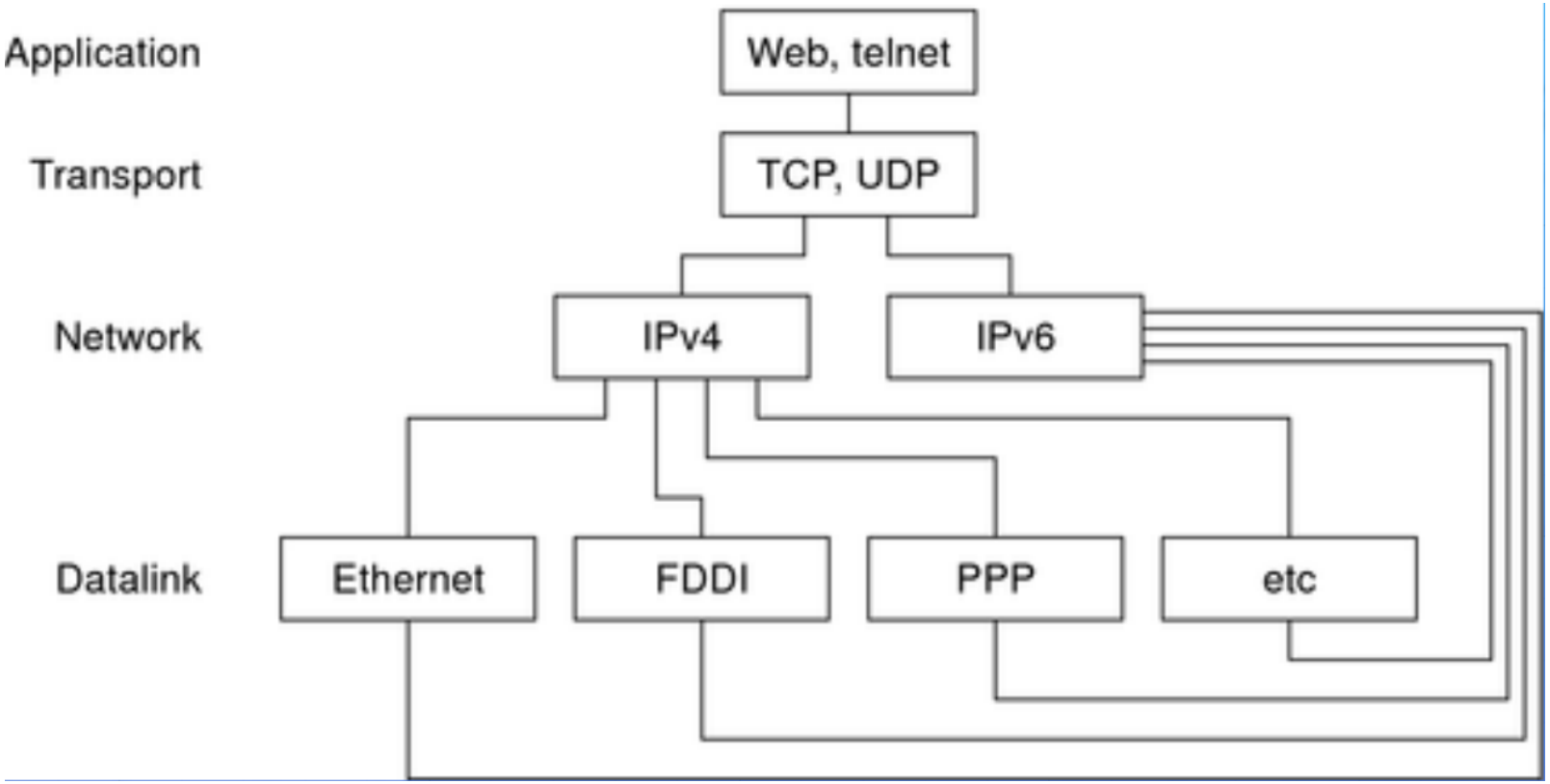
Conceptos fundamentales del BGP

Topologías comunes



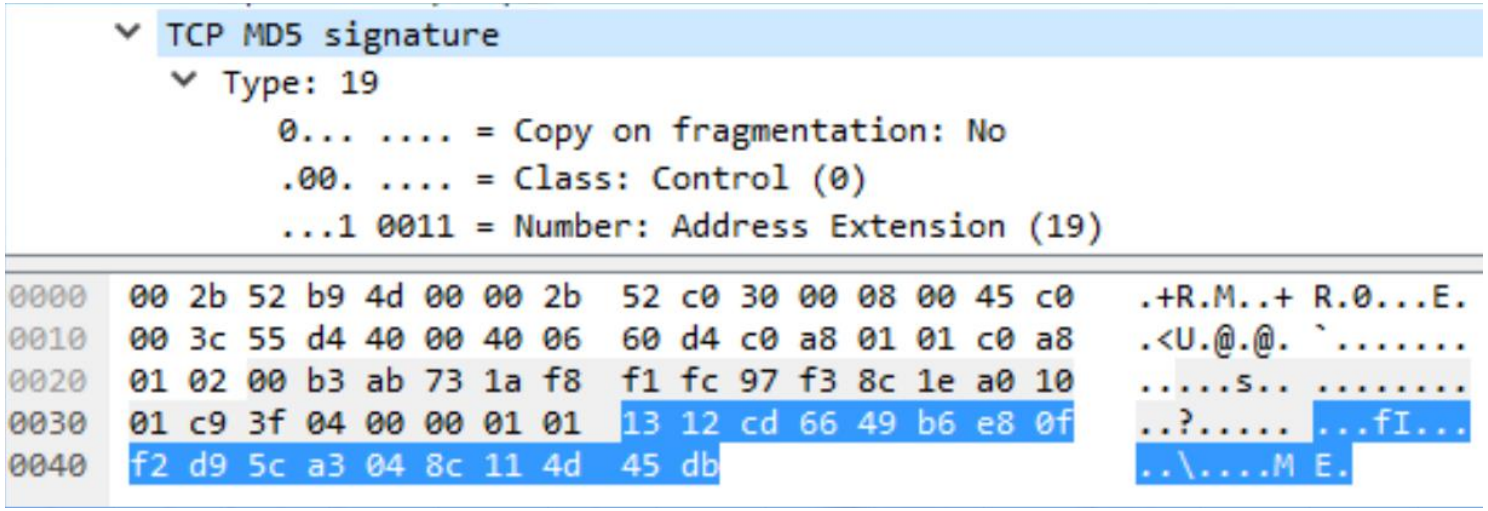
Fuente:https://datapacket.com/blog/wp-content/uploads/2017/08/Single_Multihomed_Network.png

Dual Stack ¿qué es?



Consejo #1
La autenticación de sesiones BGP

- Garantiza la autenticidad de pares TCP en una sesión BGP.
- Dificulta ataques del tipo "MITM" (man in the middle)
- Extremadamente necesario en sesiones "multihoping".



Fuente: Autoria própria,2016

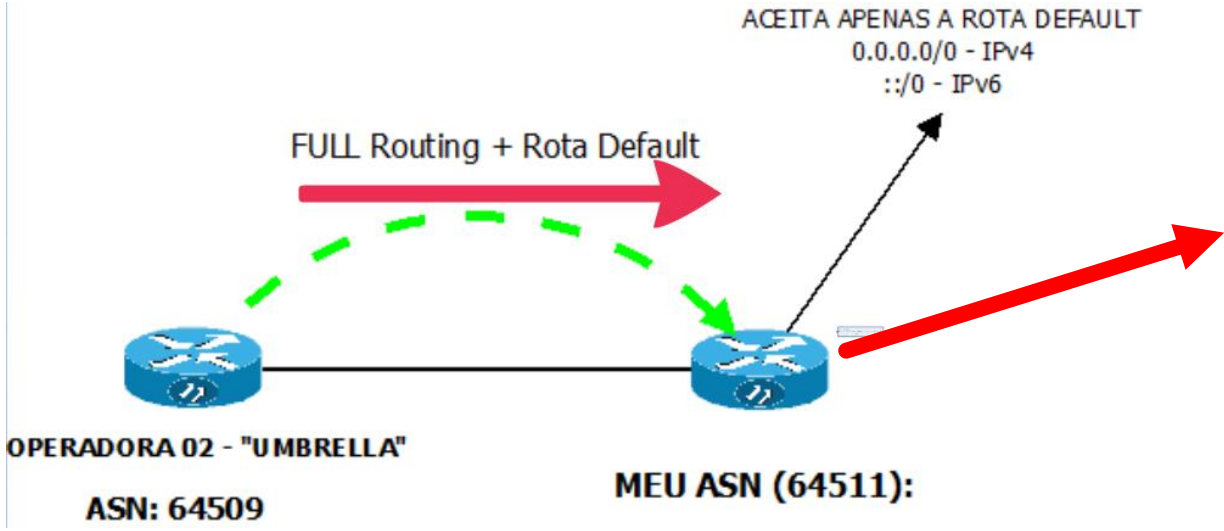
La autenticación de sesiones BGP (ejemplo)

```
add address-families=ipv6 in-filter=Operadora01_IPv6_in name=Operadora01_IPv6 out-filter=\
    Operadora02_IPv6_out remote-address=2001:db8::f0ca remote-as=28329 tcp-md5-key=M1krOtik-MUM@2019 \
    ttl=default update-source=sfp-sfpplus3
```

Fuente: Autoria própria,2017

Consejo #2
Uso de Ruta por defecto

- La BCP 194 también indica el uso de la ruta default, si es necesario;
- Ventaja para ahorrar procesamiento de la tabla "full";
- Se puede descartar todo y crear una ruta predeterminada estatica, o recibir sólo la ruta por defecto (si el “upstream” envía).



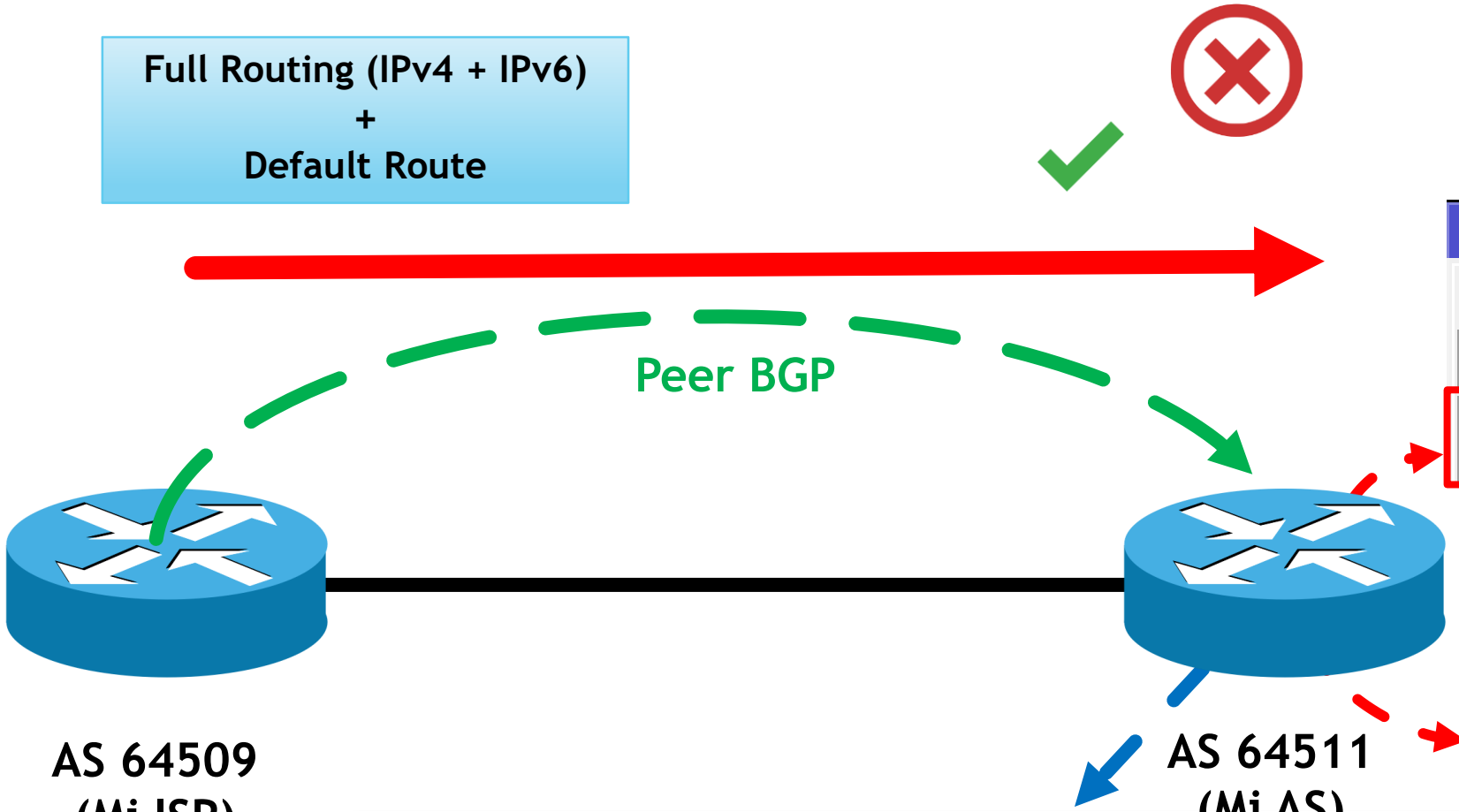
Fuente: Autoria própria, 2017

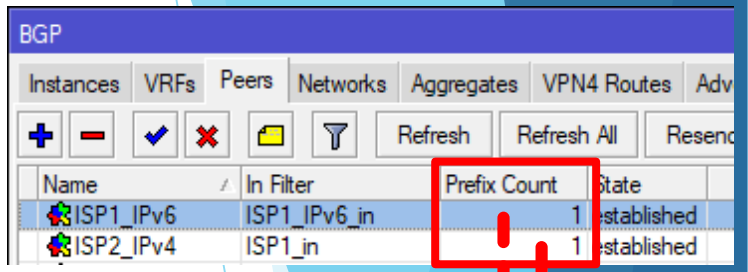
```
/routing filter
add action=discard chain=Operadoral_in prefix=!0.0.0.0/0
add action=discard chain=Operadoral_IPv6_in prefix=!::/0
```

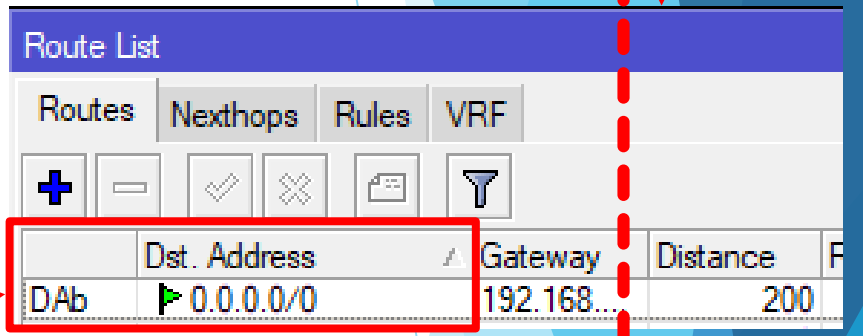
Fuente: Autoria própria, 2017

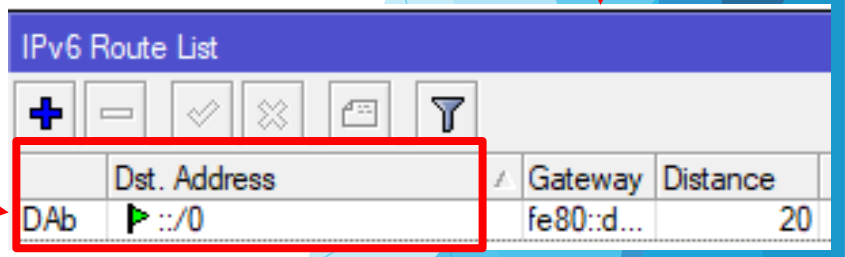
Uso de Ruta “default”

Full Routing (IPv4 + IPv6)
+
Default Route










```
/routing filter
add action=discard chain=ISP1_in prefix=!0.0.0.0/0 :
add action=discard chain=ISP1_IPv6_in prefix=!::/0
```

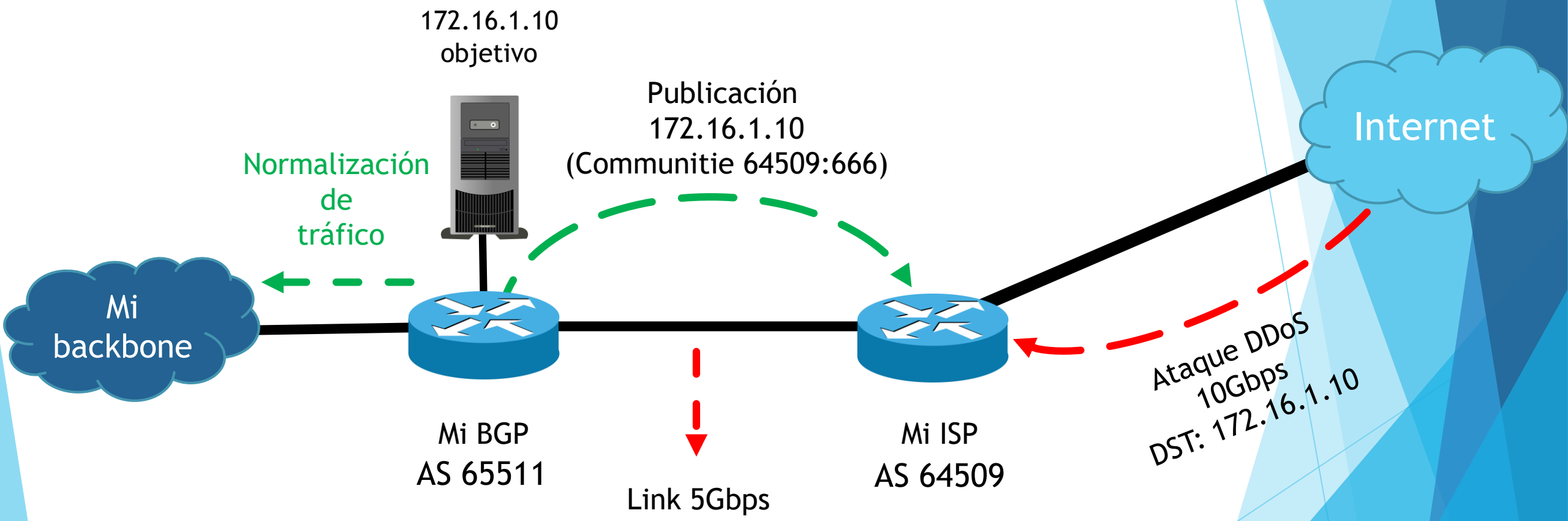
Consejo #3
El uso de Communities

- Imprescindible para tomas de acciones sin la dependencia directa del operador de tránsito;
- Utilidad para manipular el tráfico de descarga de forma mejorada;
- De extrema importancia en casos de DDoS (que generalmente son internacionales);
  - Ejemplos:

Controlling Route Propagation		
Community	Action	Region Enabled
3549:600	Deny inter-continental export of tagged prefix [iBGP].	EU/SA
3549:601	Deny inter-cluster export of tagged prefix [iBGP].	SA
3549:602	Deny inter-country export of tagged prefix [iBGP].	SA
3549:603	Deny inter-metro export of tagged prefix [iBGP].	TBD
3549:604	Deny inter-Hub export of tagged prefix [iBGP].	TBD
3549:605	Deny inter-router export of tagged prefix [iBGP].	TBD
3549:666	Deny inter-as export of tagged prefix (deny to peers, send to customers) [eBGP].	NA/SA/EU/AS
3549:695	Deny in country peers but export globally	SA

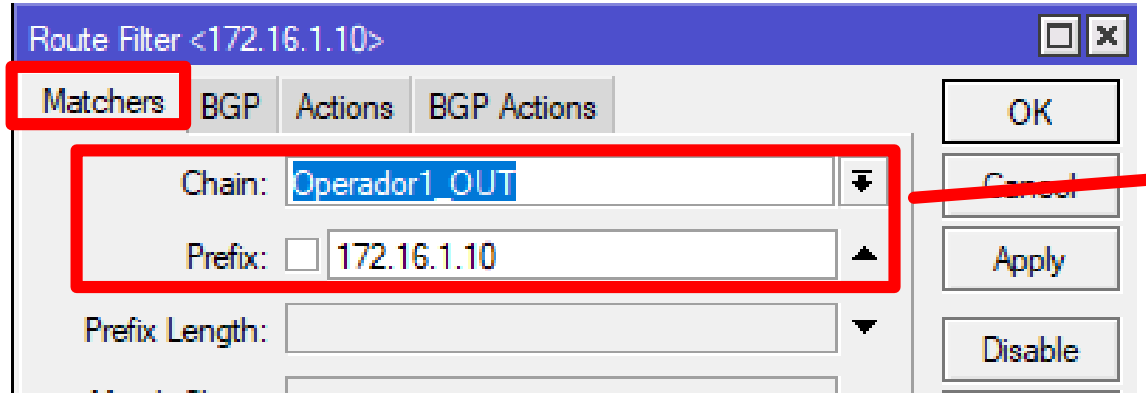
28329:666	BLACKHOLE

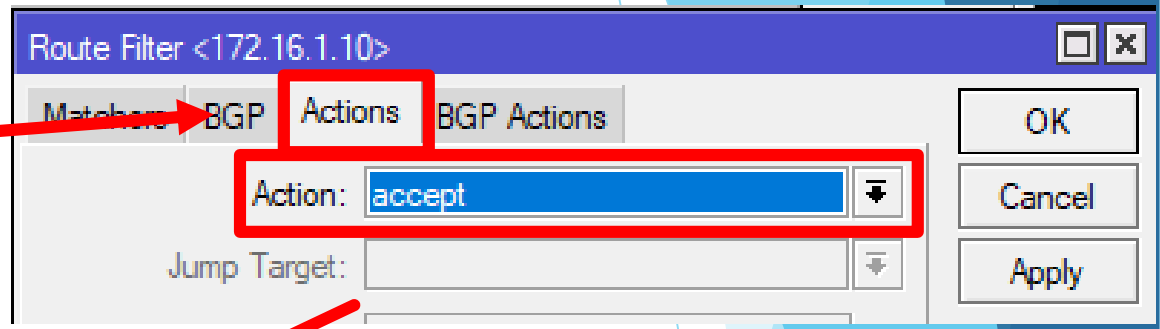
Uso de Communities (Ejemplo) (1/3)

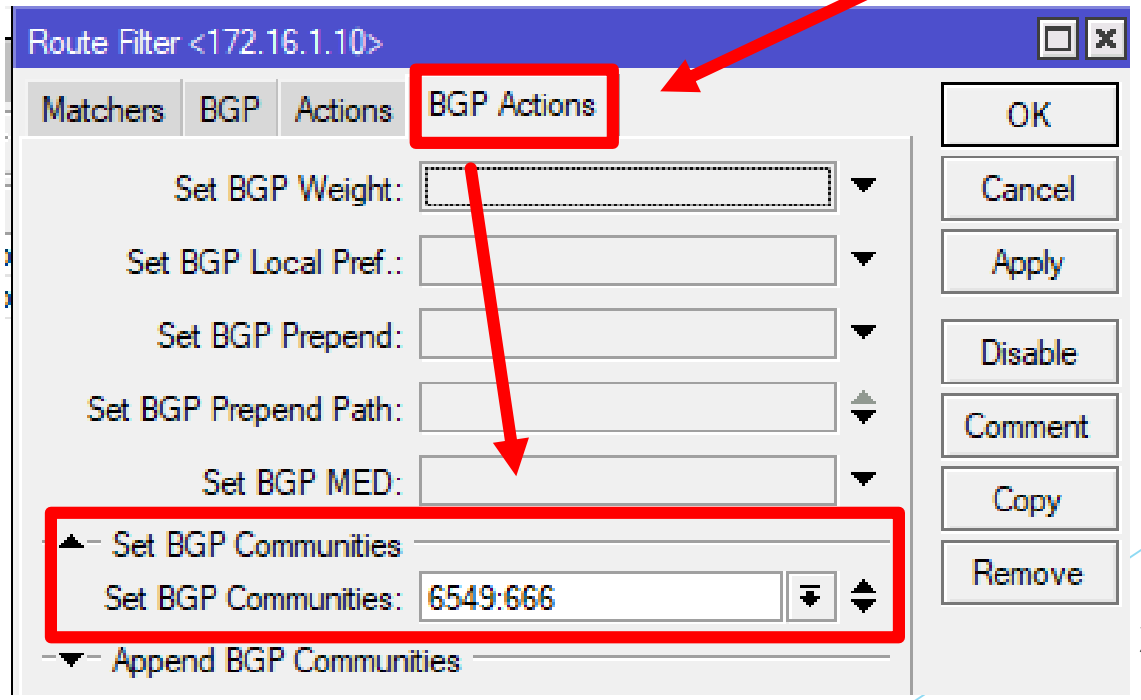


¡ Importante!
La configuración también depende de su operador de Transito (upstream)

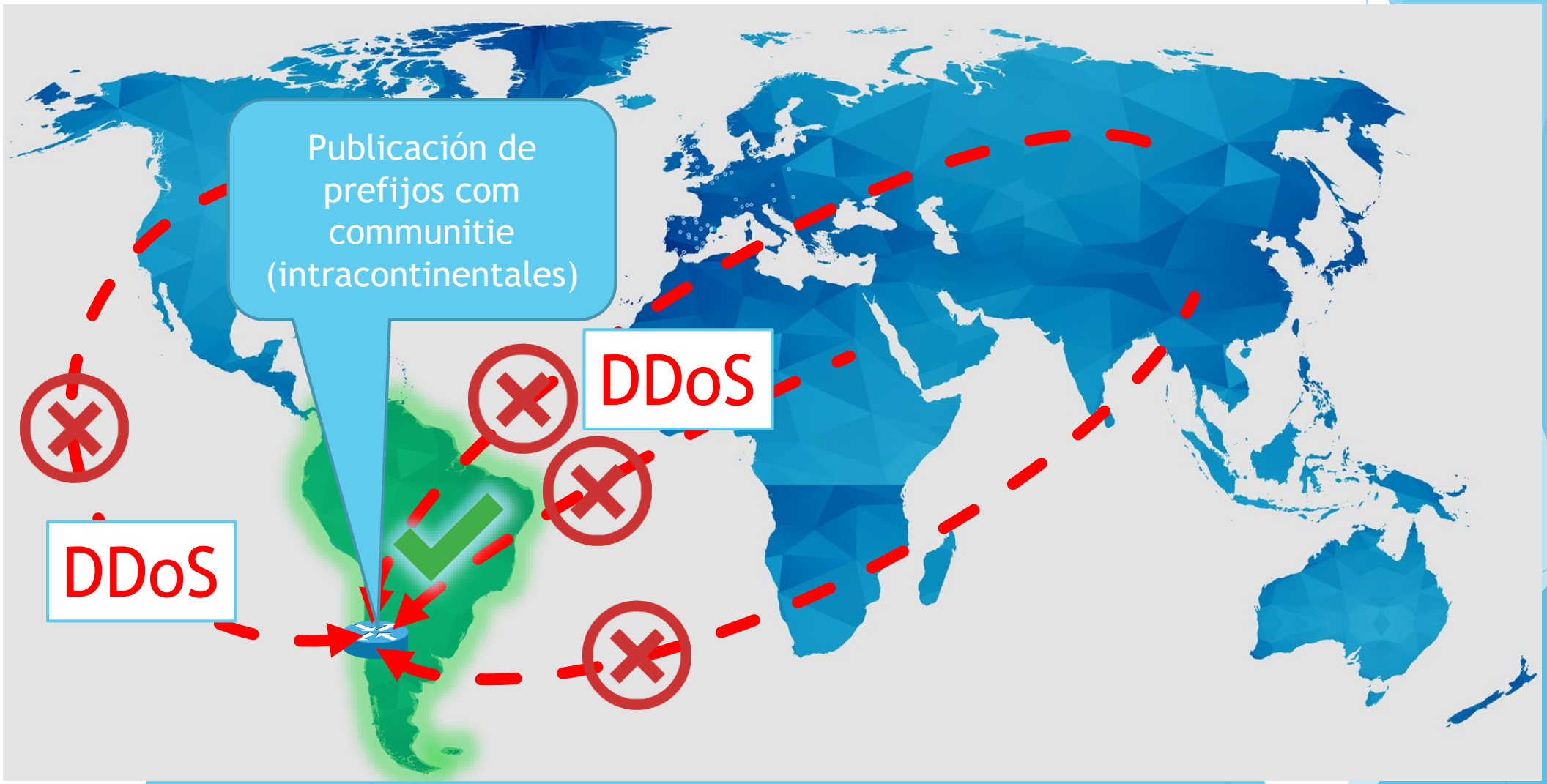
Uso de Communities (Ejemplo) (2/3)







Uso de Communities (Ejemplo) (3/3)



¡Importante!
La configuración también depende de su operador de Transito (upstream)

Consejo #4
Filtrado de Prefijo

- Básicamente la BCP 194, en peerings con la operadora (upstream), recomienda adoptar algunas políticas.
  - Prefijos de entrada "in":
    - (Descartar) Pertenecen al propio AS.
    - (Descartar) De uso privado, especial o reservado, (que no deben tener enrutamiento en Internet, y también se utilizan para spoofing)
  - Prefijos de salida "out“
    - (No puede) Más específicos que / 24 en IPv4 y / 48 en IPv6.
    - (Debe) Todos los Prefijos pertenecientes al AS en cuestión.

Filtraje de prefijos

¿Qué es?
¿lo que evita?

- Cualquier posibilidad de recibir prefijos de mi propio AS;
- Servir de tránsito a terceros, de forma no deseada;
- "Route Leaking";
- "Flood" descontrolado de la tabla global de enrutamiento;

Algunos Ejemplos...

IPv4:

```
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora01" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_01_in comment="DESCARTA ENTRADA MEU BLOCO 2  - Operadora01" prefix=172.16.16.0/21 prefix-length=21-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 1 - Operadora02" prefix=172.16.0.0/20 prefix-length=20-32
add action=discard chain=MinhaOperadora_02_in comment="DESCARTA ENTRADA MEU BLOCO 2 - Operadora02" prefix=172.16.16.0/21 prefix-length=21-32
```

IPv6:

```
add action=discard chain=Operadora01_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 01" prefix=2001:db8::/32 prefix-length=32-128
add action=discard chain=Operadora02_IPv6_in comment="DESCARTA MEU BLOCO IPv6 - OPERADORA 02" prefix=2001:db8::/32 prefix-length=32-128
```

Algunos Ejemplos...

IPv4:

```
/routing filter
add action=discard chain=BGP-IN-IPV4 prefix=0.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=10.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=100.64.0.0/10 prefix-length=10-32
add action=discard chain=BGP-IN-IPV4 prefix=127.0.0.0/8 prefix-length=8-32
add action=discard chain=BGP-IN-IPV4 prefix=169.254.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=172.16.0.0/12 prefix-length=12-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.0.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.0.2.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=BGP-IN-IPV4 prefix=198.18.0.0/15 prefix-length=15-32
add action=discard chain=BGP-IN-IPV4 prefix=198.51.100.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=203.0.113.0/24 prefix-length=24-32
add action=discard chain=BGP-IN-IPV4 prefix=224.0.0.0/4 prefix-length=4-32
```

IPv6:

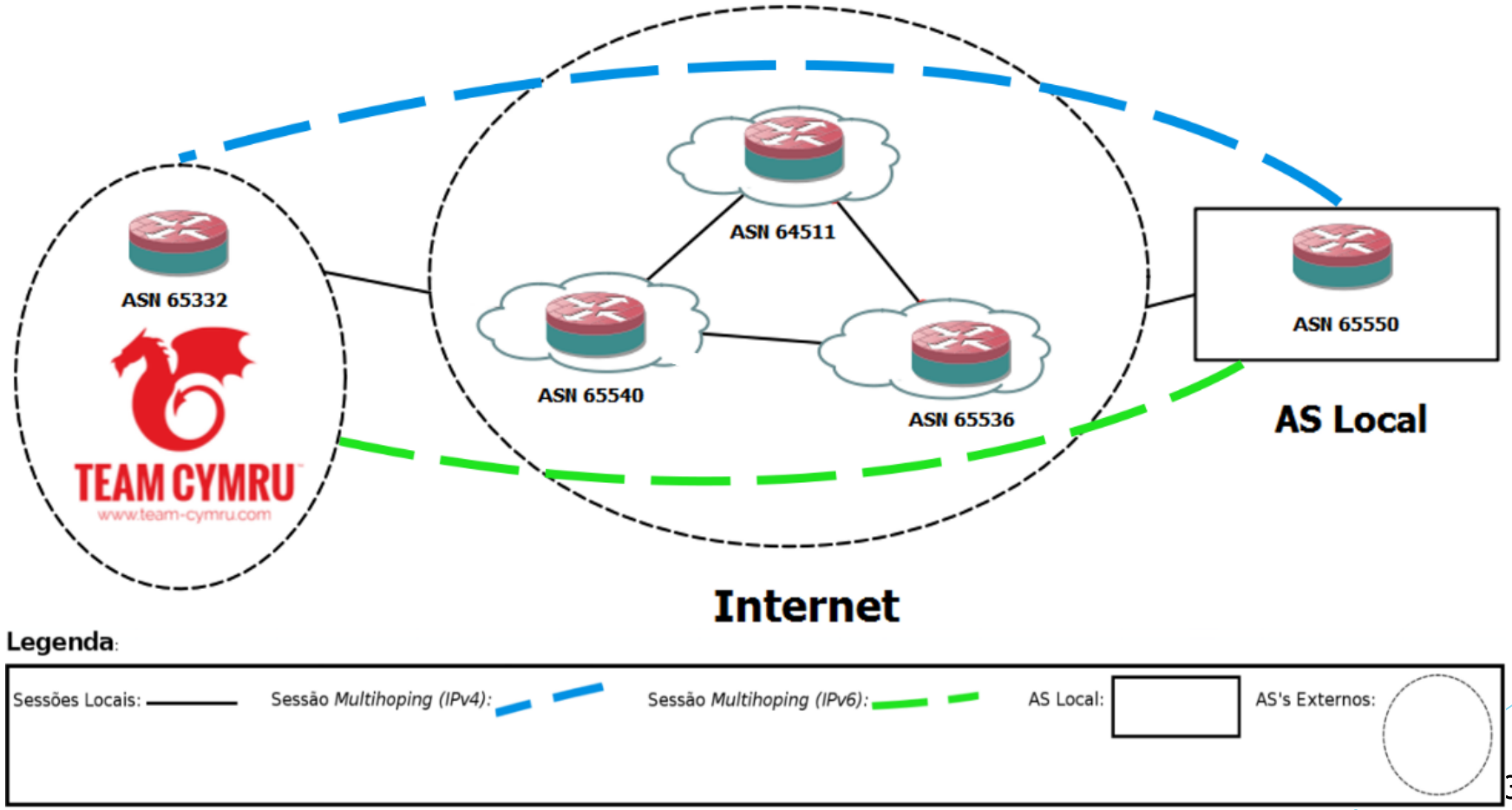
```
/routing filter
add action=accept chain=BGP-IN-IPV6 comment="ACEITA - GLOBAL - IPv6" prefix=2000::/3 prefix-length=3-48
add action=discard chain=BGP-IN-IPV6 comment="DESCARTA - RESTO - IPv6"
```

Anunciando sólo los prefijos de mi AS (ejemplo de winbox):

Chain	Prefix	Prefix Length	Action	Set BGP Prepend
;;; ANUNCIA MEU BLOCO 1 - Operadora01				
MinhaOperadora_01_out	172.16.0.0/20		accept	
;;; ANUNCIA MEU BLOCO 1 - Operadora01				
MinhaOperadora_01_out	172.16.0.0/24		accept	
MinhaOperadora_01_out			discard	
;;; ANUNCIA MEU BLOCO 1 - Operadora02				
MinhaOperadora_02_out	172.16.0.0/20		accept	
;;; DESCARTA RESTO ANUNCIOS - Operadora02				
MinhaOperadora_02_out			discard	
;;; ANUNCIO MEU BLOCO IPv6 - OPERADORA 01				
Operadora01_IPv6_out	2001:db8::/32		accept	
;;; DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 01				
Operadora01_IPv6_out			discard	
;;; ANUNCIA BLOCO IPv6 - OPERADORA 02				
Operadora02_IPv6_out	2001:db8::/32		accept	
;;; DESCARTA RESTO ANUNCIOS IPv6 - OPERADORA 02				
Operadora02_IPv6_out			discard	

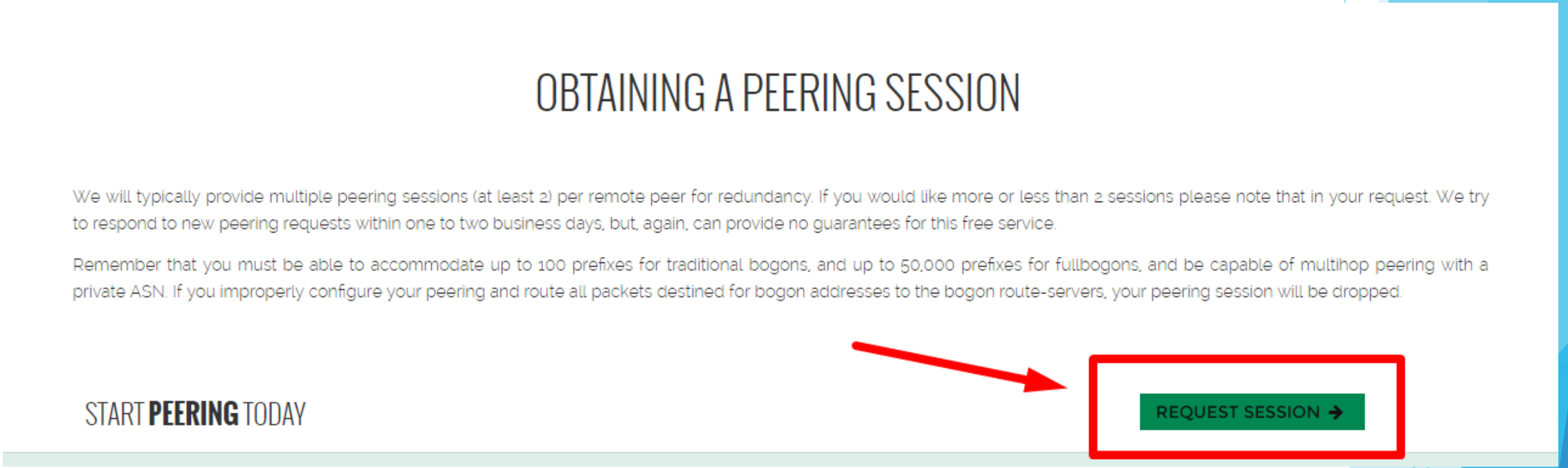
Punta: ¡Prepare los filtros ANTES de establecer cualquier sesión!

Consejo #5
Obteniendo lista dinámica de prefijos para descarte (bogons)



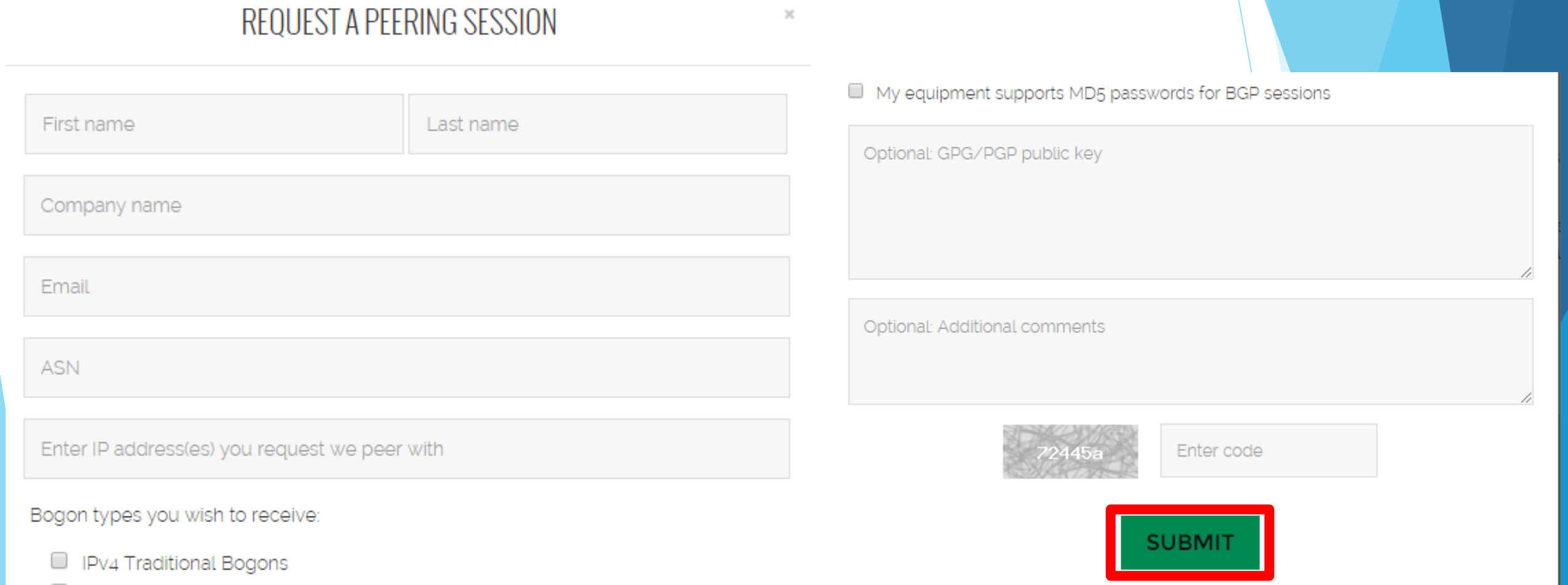
Fuente: Autoria própria,2016

Team CYMRU Obtener su sesión



https://www.team-cymru.com/bogon-reference-bgp.html

Obteniendo lista dinámica de prefijos para descarte (bogons)



Completar el formulario

Team CYMRU – Implementación

(ejemplo em RouterOS)

```
# Full Bogons Mikrotik Template
# Work on RouterOS 4.X
# 2010-11-01 by Ricardo Ozelo

# BGP instance setup

/routing bgp instance set default as=<YOUR_ASN> \
 router-id=<WAN_IP_ADDRESS>

# ROUTING FILTERS - Install these routes as blackholes,
# does NOT receive or announce anything else

/routing filter add action=accept bgp-communities=65332:888 \
 chain=cymru-in comment="" disabled=no invert-match=no \
 set-type=blackhole
/routing filter add action=discard chain=cymru-in comment="" \
 disabled=no invert-match=no
/routing filter add action=discard chain=cymru-out comment="" \
 disabled=no invert-match=no
```

Fuente: http://www.team-cymru.com/bgp-examples.html#mikrotik-full

Team CYMRU – Implementación

(ejemplo em RouterOS)

```
# Peering #1

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-1 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_1> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>

# Peering #2

/routing bgp peer add address-families=ip,ipv6 disabled=no in-filter=cymru-in \
 instance=default multihop=yes name=FULLBOGONS-CYMRU-2 out-filter=cymru-out \
 remote-address=<CYMRU_IP_ADDRESS_2> remote-as=65332 tcp-md5-key=<CYMRU_MD5_PASSWORD>
```

Fuente: http://www.team-cymru.com/bgp-examples.html#mikrotik-full

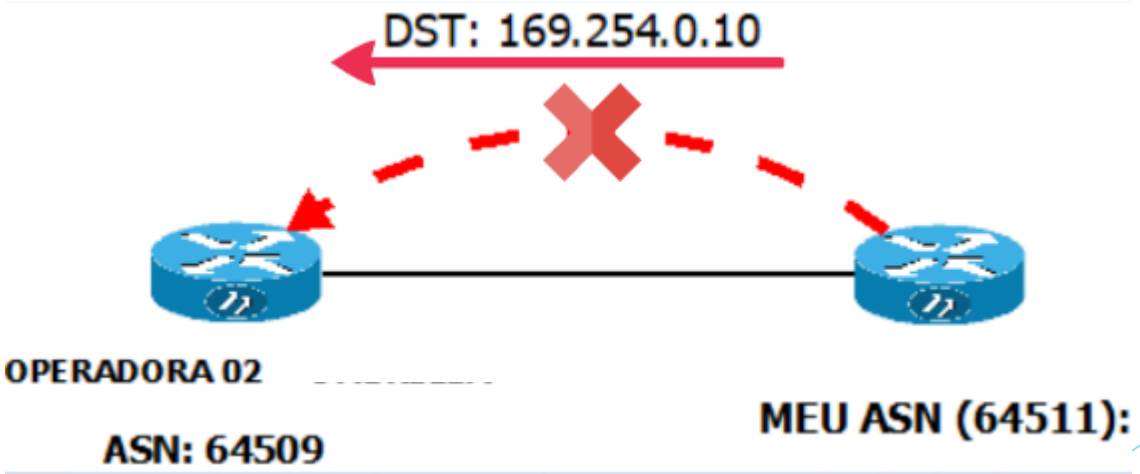
Team CYMRU – Sesión activa (ejemplo)

```
E name="TeamCYMRU_Bogons_IPv4" instance=default remote-address=193.[redacted] remote-as=65332
  tcp-md5-key="[redacted]" nexthop-choice=default multihop=yes route-reflect=no hold-time=3m
  ttl=default max-prefix-limit=10000 max-prefix-restart-time=30m in-filter=Cymru_in
  out-filter=Cymru_out address-families=ip default-originate=never remove-private-as=no
  as-override=no passive=no use-bfd=no
```

```
[redacted] > ip route print where type=blackhole
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 ADbB 0.0.0.0/8                                                 20
 1 ADbB 2.56.0.0/14                                               20
 2 ADbB 5.8.248.0/21                                              20
 3 ADbB 5.39.200.0/21                                             20
 4 ADbB 5.45.32.0/20                                              20
 5 ADbB 5.100.240.0/21                                            20
 6 ADbB 5.104.72.0/21                                             20
 7 ADbB 5.133.64.0/18                                             20
 8 ADbB 5.172.176.0/21                                            20
 9 ADbB 5.180.0.0/14                                              20
10 ADbB 5.199.184.0/21                                            20
```

Team CYMRU – Sesión activa (ejemplo)

```
[                                    ] > tool traceroute 169.254.0.10
 # ADDRESS                                LOSS SENT    LAST      AVG
 1                                        100%    2 timeout
 2                                        100%    2 timeout
 3                                        100%    1 timeout
 4                                        100%    1 timeout
 5                                        100%    1 timeout
```



Consejo #6

¡Importante!

- SIEMPRE anunciar los prefijos originados a partir de su AS sólo con recursos pertenecientes al mismo, de lo contrario, podemos cometer un error llamado "Route Leaking" que puede entorpecer el funcionamiento de Internet.

- El anuncio de prefijos no pertenecientes al AS en cuestión también puede ser utilizado con principios maliciosos, como intentos de "Hijacking".

Route Leaking: Google y Nigerian ISP Telecom (12 de febrero de 2018)

- Problemas en Google debido a la publicación de rutas indebidas:

Fuente: https://www.manrs.org/2018/11/route-leak-causes-major-google-outage/

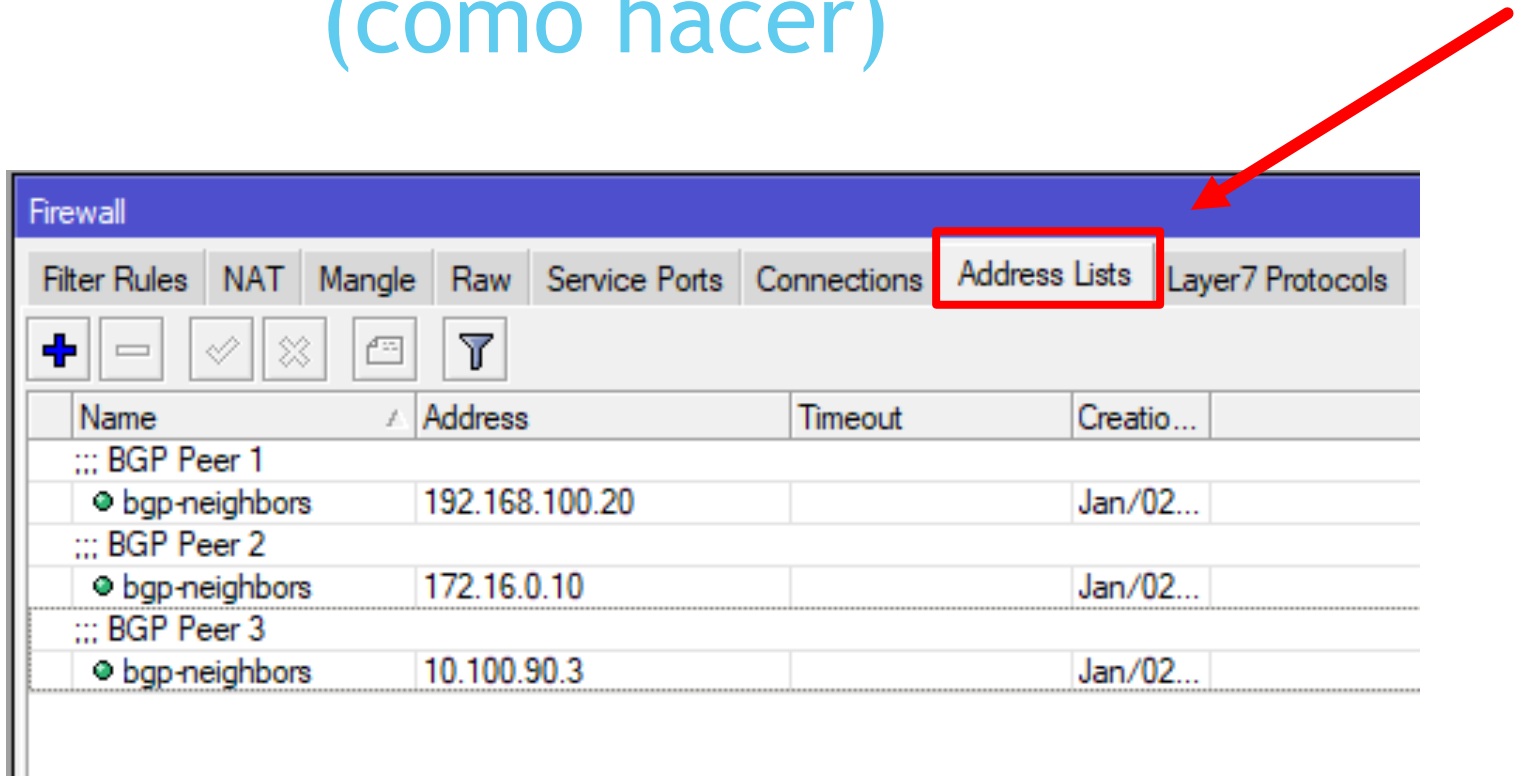
Consejo #7
Protección para el servicio BGP

4. Protection of the BGP Speaker

The BGP speaker needs to be protected from attempts to subvert the BGP session. This protection SHOULD be achieved by an Access Control List (ACL) that would discard all packets directed to TCP port 179 on the local device and sourced from an address not known or permitted to become a BGP neighbor. Experience has shown that the natural protection TCP should offer is not always sufficient, as it is sometimes run in control-plane software. In the absence of ACLs, it is possible to attack a BGP speaker by simply sending a high volume of connection requests to it.

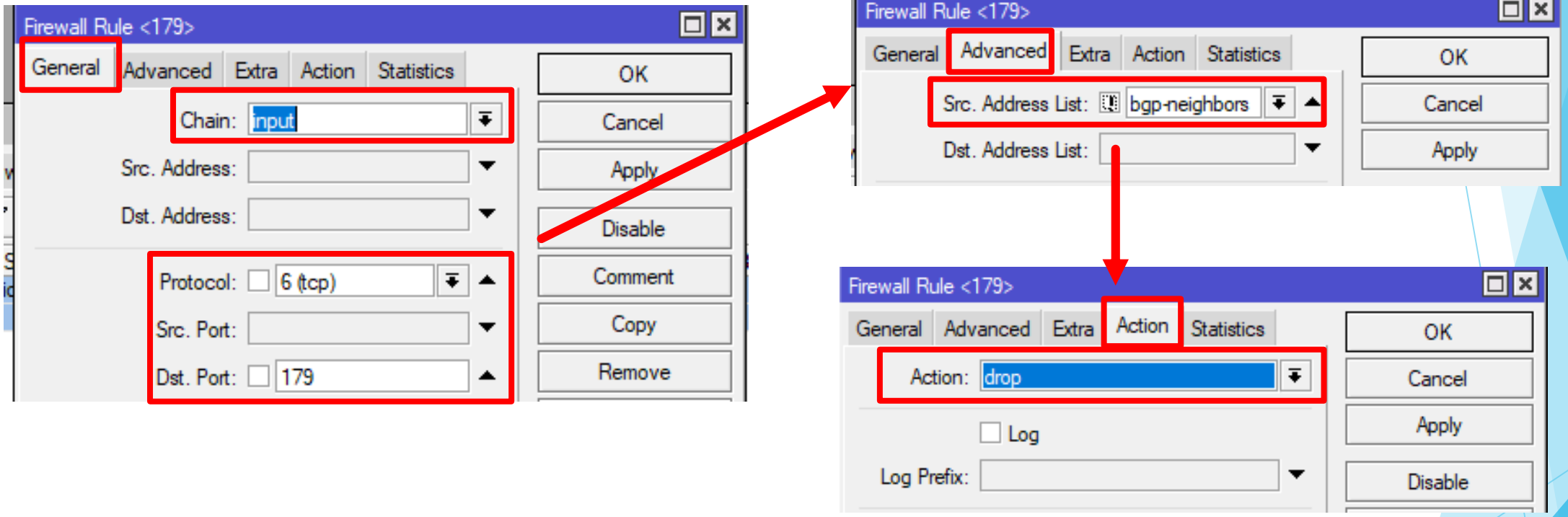
Fuente: https://tools.ietf.org/html/bcp194#page-13

Protección simples para el servicio BGP (como hacer)



1- Añadir direcciones permitidas para sesiones BGP en: IP>Firewall>Adress List

Protección simples para el servicio BGP (como hacer)



2 – Añadir una regla de Firewall en: IP>Firewall>Filter

Protección simples para el servicio BGP (exemplo)

1- Añadir direcciones permitidas para sesiones BGP:

```
/ip firewall address-list
add address=192.168.100.20 comment="BGP Peer 1" list=bgp-neighbors
add address=172.16.0.10 comment="BGP Peer 2" list=bgp-neighbors
add address=10.100.90.3 comment="BGP Peer 3" list=bgp-neighbors
```

2 – Añadir una regla de Firewal:

```
/ip firewall filter
add action=drop chain=input comment="DROP peers BGP desconocidos"
dst-port=179 protocol=tcp \
   src-address-list=!bgp-neighbors
```

Consejo #8
Buenas prácticas para el enrutador de borde (recursos)

Son recursos innecesarios:

- ⊗ DHCP;
- ⊗ DNS recursivo;
- ⊗ Hotspot
- ⊗ PPPoE Server
- ⊗ NTP Server
- ⊗ FTP Server
- ⊗ IGP en las interfaces de sesiones *InterAS* como OSPF
- ⊗ IPv6 RA (Router Advertisement) en las interfaces de sesión *InterAS*

Buenas prácticas para el enrutador de borde

¡importante!

Algunos servicios innecesarios y mal configurados pueden convertirse en potenciales vulnerabilidades exploradas como amplificación de tráfico (muy utilizado para ataques DDoS)

Buenas prácticas para el enrutador de borde

System>Packages

```
Flags: X - disabled
 #    NAME                VERSION                  SCHEDULED
 0    routeros-tile       6.42.11
 1    system              6.42.11
 2    ipv6                6.42.11
 3 X  wireless            6.42.11
 4 X  hotspot             6.42.11
 5 X  dhcp                6.42.11
 6    mpls                6.42.11
 7    routing             6.42.11
 8 X  ppp                 6.42.11
 9    security            6.42.11
10    advanced-tools      6.42.11
```

Buenas prácticas para el enrutador de borde

IP>Services

```
Flags: X - disabled, I - invalid
 #   NAME
 0 XI telnet
 1 XI ftp
 2 XI www


 3   ssh
 4 XI www-ssl
 5 XI api
 6   winbox
 7 XI api-ssl
```

Atención a los siguientes recursos:

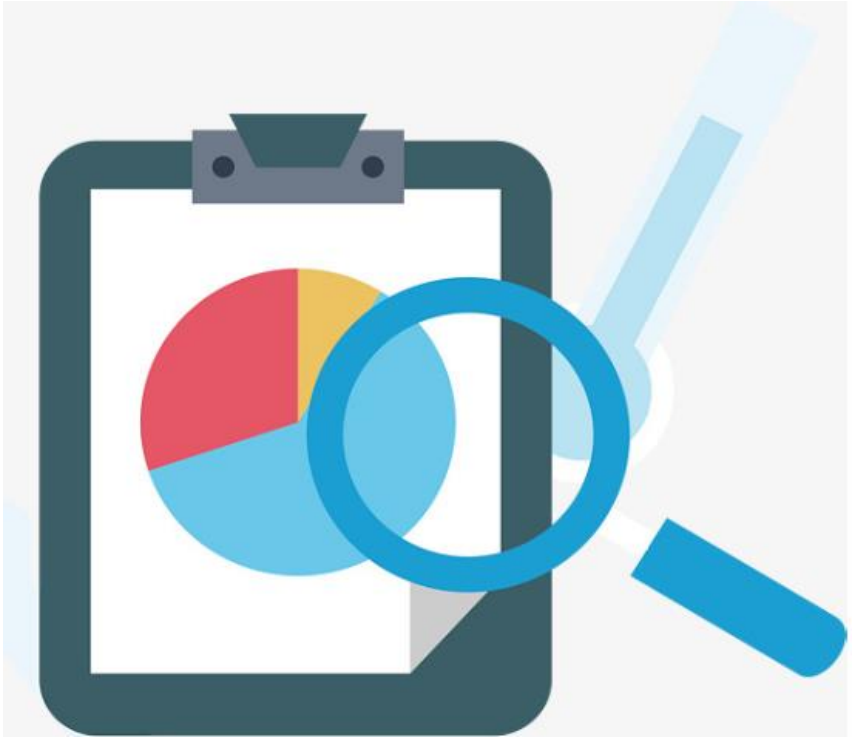
- SNMP con configuraciones por defecto;
- MNDP (Mikrotik Neighbor Discovery Protocol) en interfaces no necesarias (como upstreans);
- RoMON con configuraciones por defecto.

No se olvide:

- Política de copia de seguridad.

Resultados ¿Cómo analizar?

- Las buenas prácticas deben tenerse en cuenta y aplicarse siempre que sea posible y de acuerdo con el escenario.
- El resultado viene a través del conjunto de ellas



Herramienta “Looking Glass”

Looking Glass Results

```
bbr01.eq01.sng02> show route protocol bgp 177.10.232.0 table inet.0
inet.0: 759726 destinations, 6268780 routes (759057 active, 0 holddown, 4710 hidden)
+ = Active Route, - = Last Active, * = Both

177.10.232.0/24                *[BGP/170] 2d 20:41:05, MED 31, localpref 125, from 173.192.18.31
                                  AS Path: 262880 I
                                > to 169.45.19.176 via ae21.0, label-switched-path 173.192.18.57:dt-rsvp-AUTO-TUNNEL
                                  to 169.45.19.172 via ae20.0, label-switched-path Bypass->169.45.19.176->169.45.19.188
                               [BGP/170] 2d 20:41:04, MED 31, localpref 125, from 173.192.18.32
                                  AS Path: 262880 I
                                > to 169.45.19.176 via ae21.0, label-switched-path 173.192.18.57:dt-rsvp-AUTO-TUNNEL
                                  to 169.45.19.172 via ae20.0, label-switched-path Bypass->169.45.19.176->169.45.19.188
                               [BGP/170] 2d 20:41:04, MED 31, localpref 125, from 173.192.18.61
                                  AS Path: 262880 I
                                > to 169.45.19.176 via ae21.0, label-switched-path 173.192.18.57:dt-rsvp-AUTO-TUNNEL
                                  to 169.45.19.172 via ae20.0, label-switched-path Bypass->169.45.19.176->169.45.19.188
```

Más en: http://lg.softlayer.com/

Herramienta “BGP.He”

Escriba el número de AS o el prefijo

Ver informaciónes

HURRICANE ELECTRIC INTERNET SERVICES

14259 Search

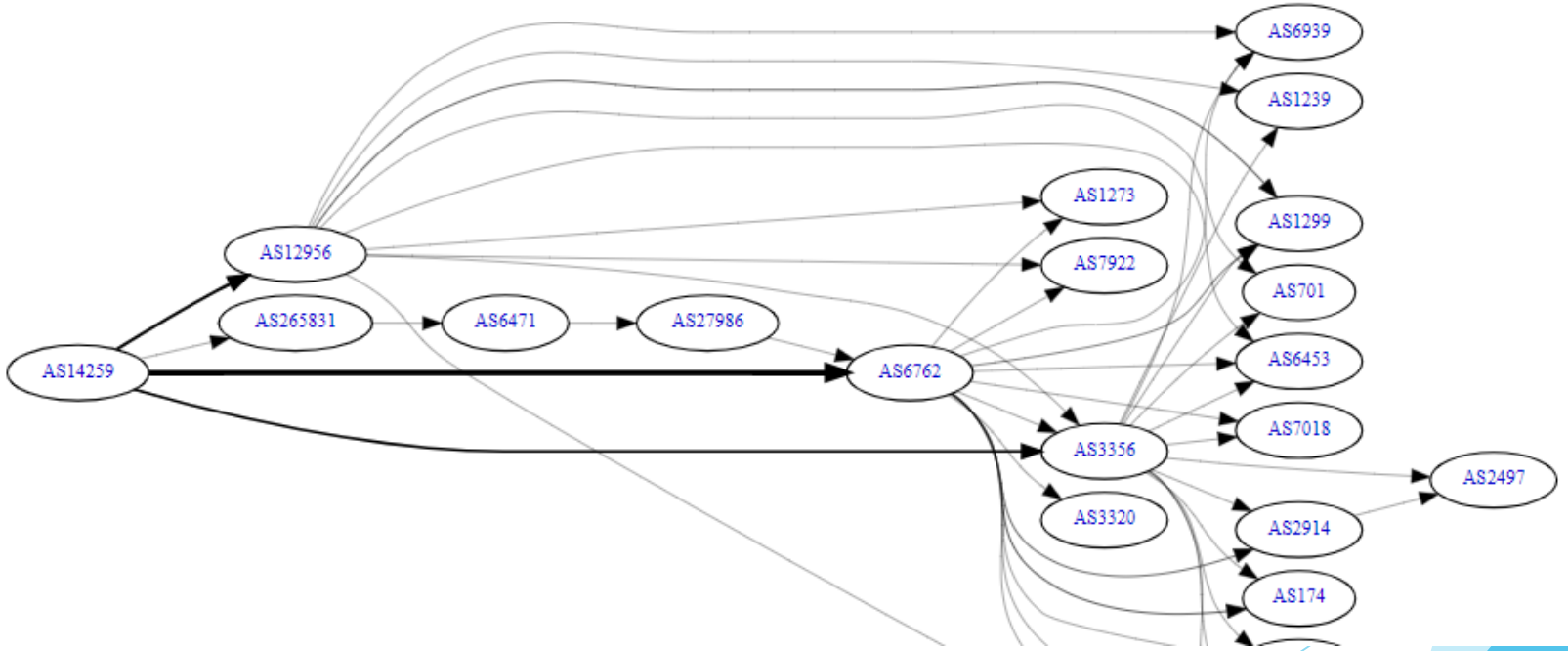
AS14259 Gtd Internet S.A.

Quick Links

- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

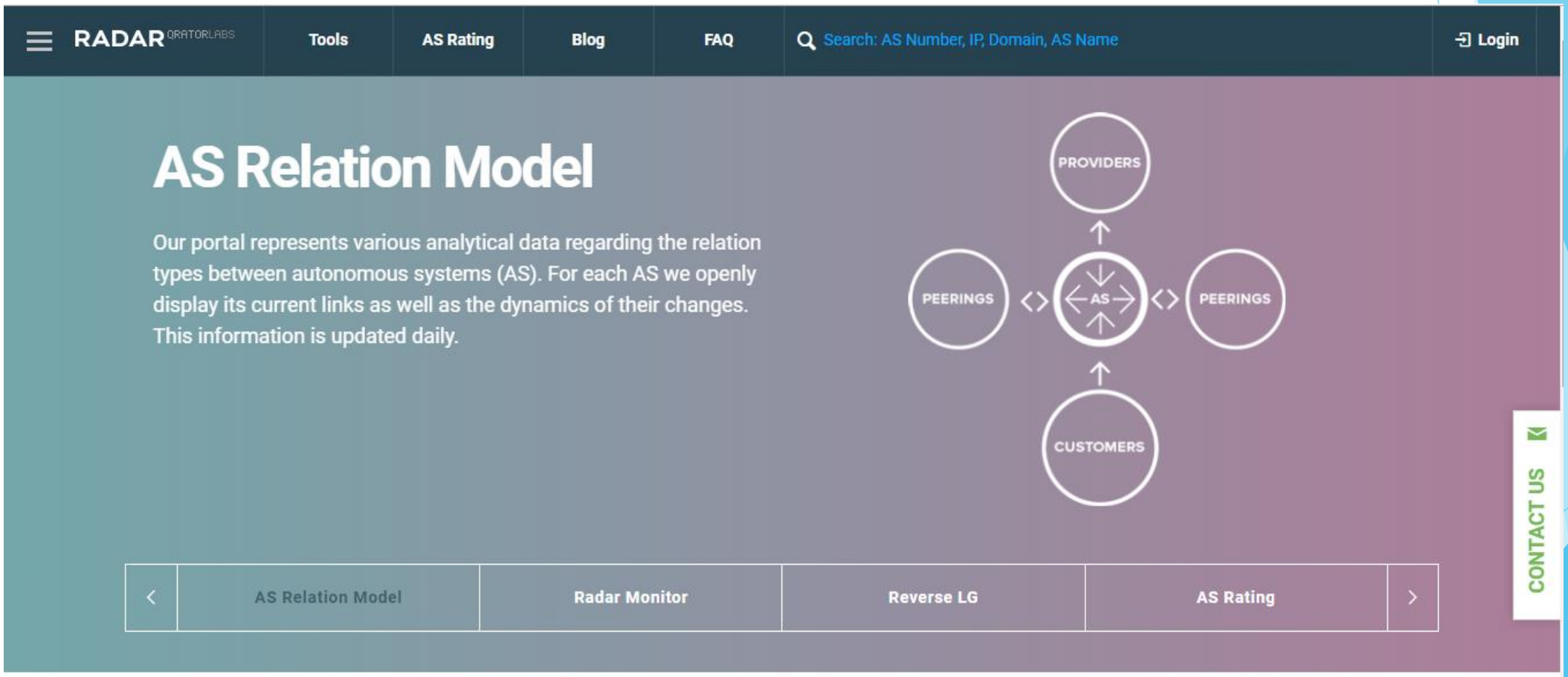
AS Info | Graph v4 | Graph v6 | Prefixes v4 | Prefixes v6 | Peers v4 | Peers v6 | Whois | IRR

AS14259 IPv4 Route Propagation



Más en: http://lg.softlayer.com/

Herramienta “Radar by Qrator”

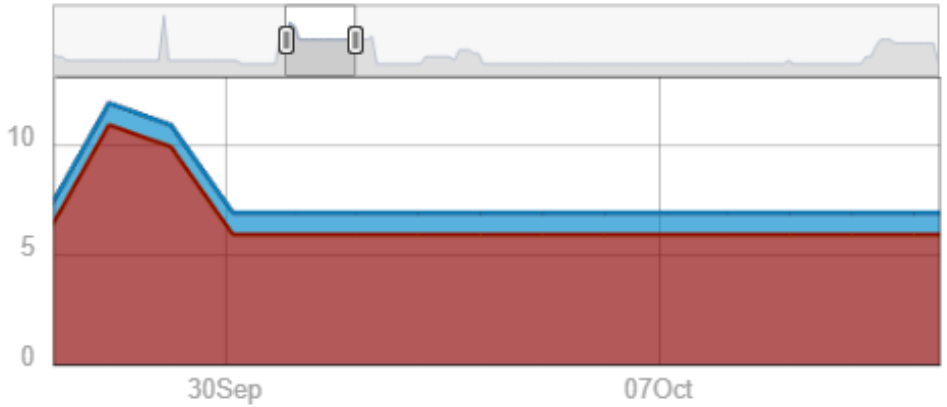


Más en: https://radar.qrator.net/

Herramienta “Radar by Qrator”

DDoS Amplifiers

2018-09-27 — 2018-10-12



DDoS amplifiers are vulnerabilities which can be used by attackers to produce large amounts of network traffic. The most important examples are ICMP, DNS and NTP amplifiers. Combined with IP spoofing, DDoS amplifiers can be used for bandwidth

Check out Server IP

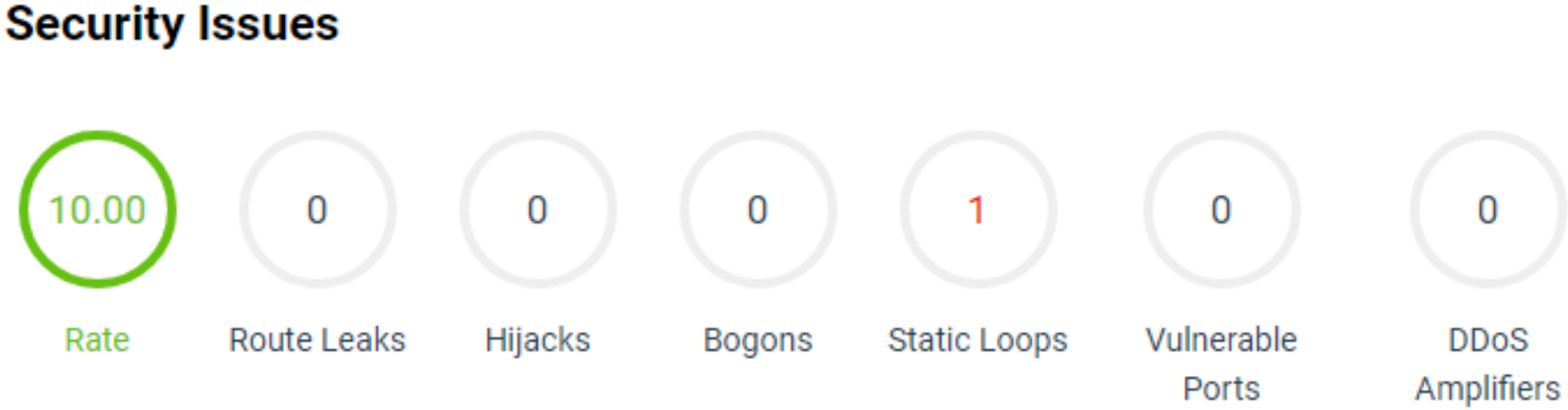
EXPORT

ALL (7) ICMP (0) DNS (6) NTP (0) SNMP (1) SSDP (0) CHARGEN (0) QOTD (0) NETBIOS (0) RIPv1 (0) PORTMAP (0) MEMCACHED (0)

Type	Server IP	Coefficient	First seen	Last seen	Status
SNMP	17[redacted]	40.15	2018-09-26 12:33:30	2018-10-15 18:23:43	Active

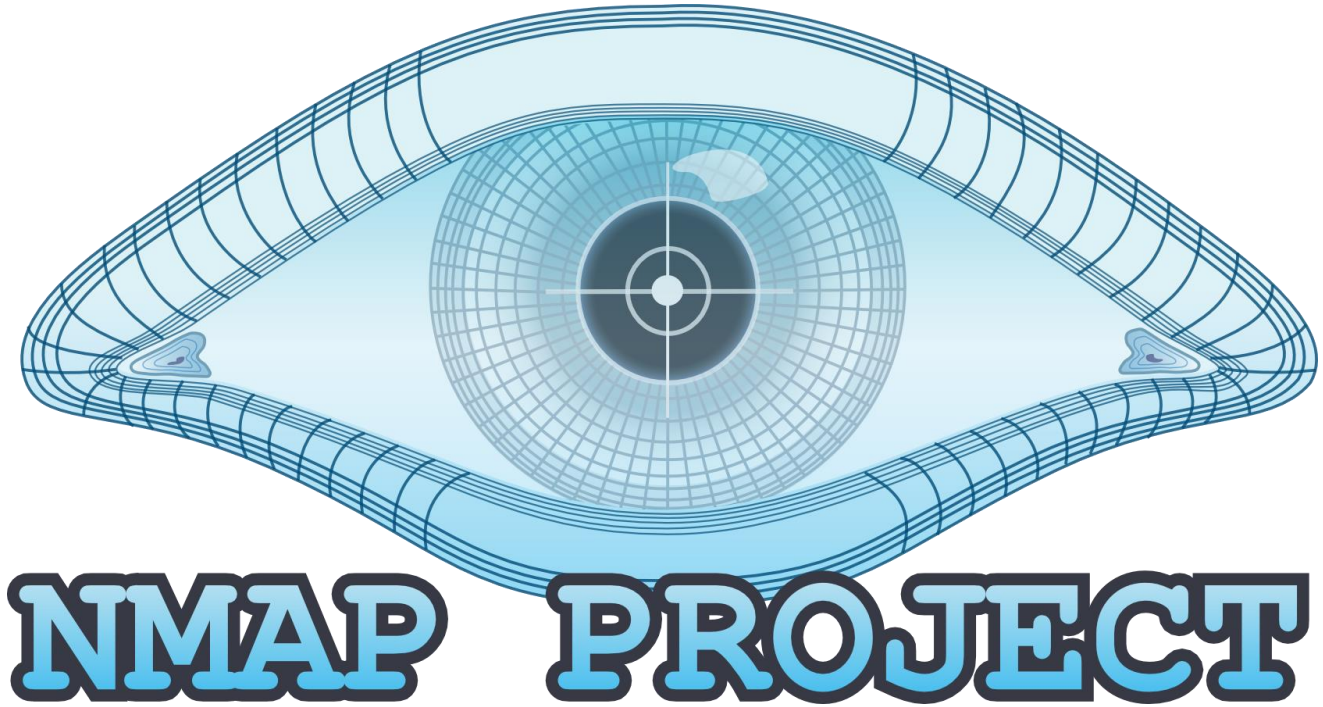
Más en: https://radar.qrator.net/

Herramienta “Radar by Qrator”



Más en: https://radar.qrator.net/

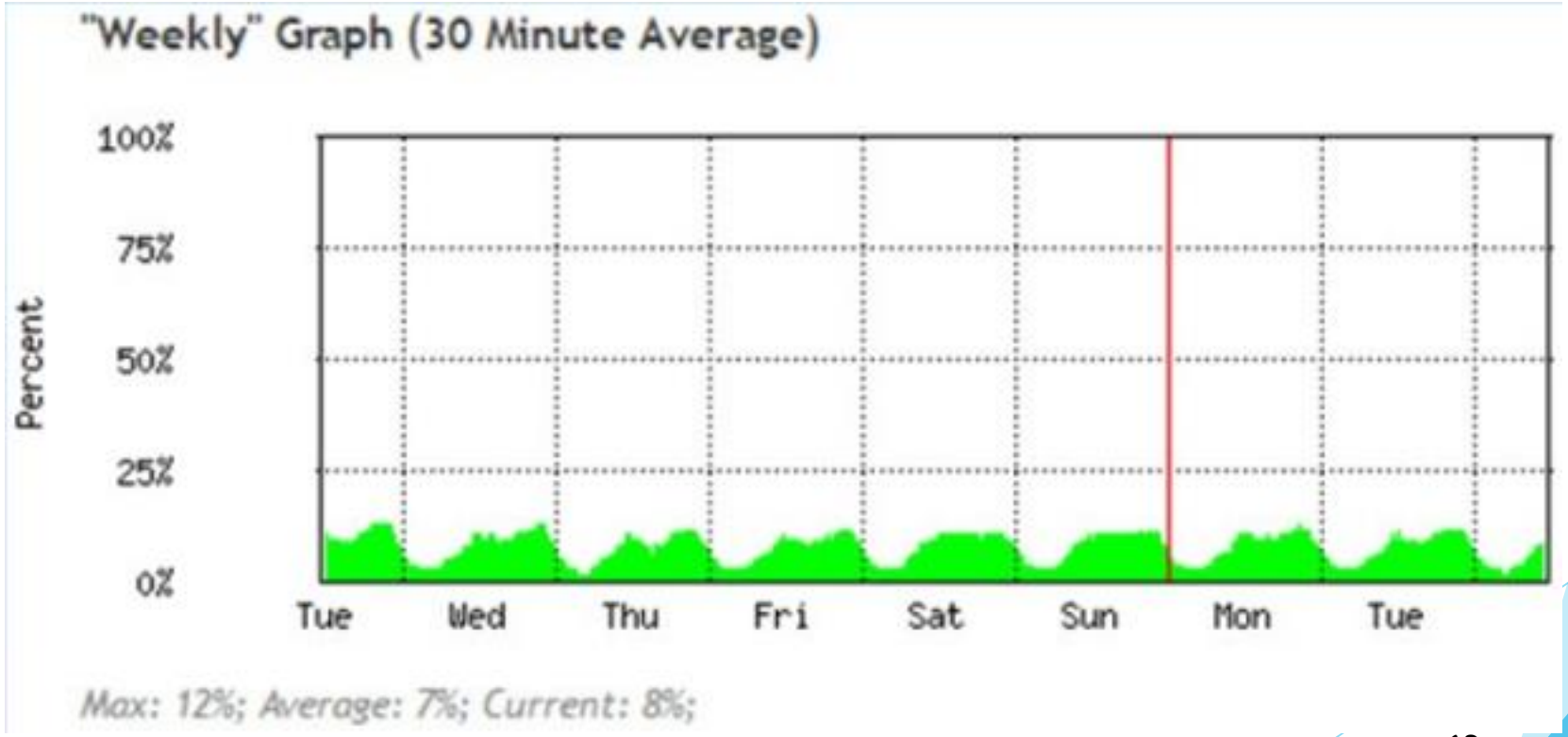
Herramienta “NMAP”



Más en: https://radar.qrator.net/

¿Qué esperar?

- Más estabilidad de su enrutador de borde



Referencias bibliográficas

- http://nic.br
- https://tools.ietf.org/html/bcp194
- https://wiki.mikrotik.com
- https://cert.br
- http://www.team-cymru.com
- Artículo: *"Boas Práticas em roteamento de borda para Sistemas autônomos provedores de acesso à internet Em processo de Dual Stack"* João Alberto B. Oliveira, 2016

Artículo

BOAS PRÁTICAS EM ROTEAMENTO DE BORDA PARA SISTEMAS AUTONOMOS PROVEDORES DE ACESSO À INTERNET EM PROCESSO DE DUAL STACK

JOÃO ALBERTO BARBOSA DE OLIVEIRA
Especialista em Gestão e Segurança em Redes de Computadores, Universidade Estadual de Goiás (UEG), Campus de Trindade

FÁBIO BARBOSA RODRIGUES
Mestre e doutorando em Engenharia Elétrica e de Computação pela UFG - Universidade Federal de Goiás (Goiânia / GO) e docente da UEG - Universidade Estadual de Goiás (UEG), Campus de Trindade

Palavras-chave: Roteador de borda, Sistemas Autônomos, Provedor de Acesso, Boas práticas.

Resumo

Considerando que o número de novos Sistemas Autônomos (SA) tem crescido em to

Más en http://www.revista.ueg.br/index.php/mirante/article/view/7607

¿Dudas?

- También estoy em el stand de Mikrotik Xperts Chile!

mikrotik xperts

¡Gracias!