

Tutorial de enrutamiento seguro

Guillermo Cicileo - guillermo@lacnic.net

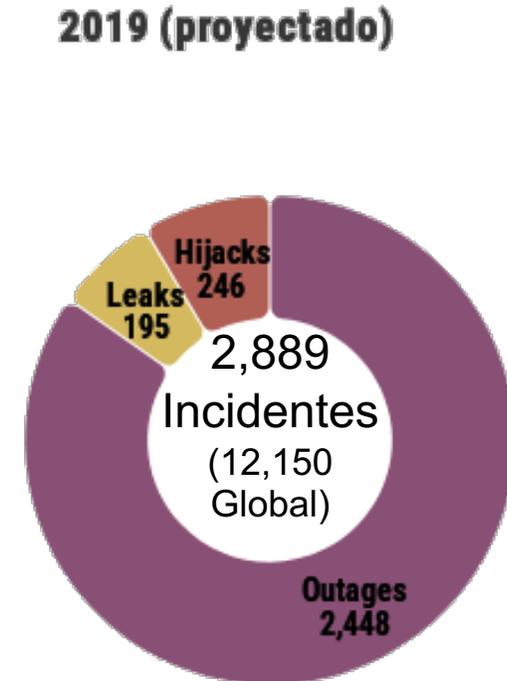
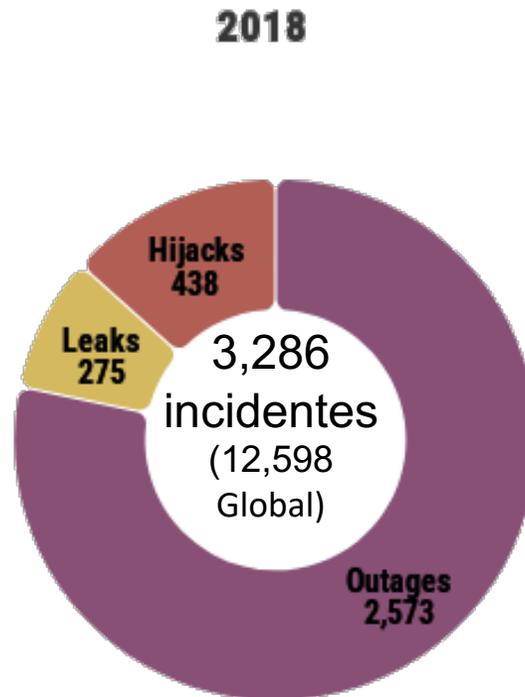
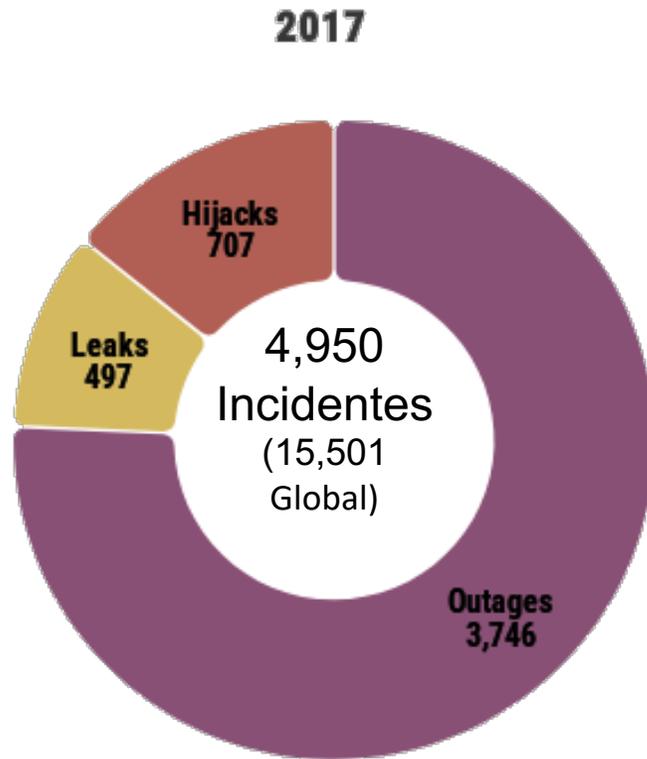


Cantidad de incidentes en LAC

Fuente: Informe sobre seguridad en el ruteo de LAC – Augusto Mathurín, 2019

<https://www.lacnic.net/innovaportal/file/4297/1/fort-informe-seguridad-ruteo-es.pdf>

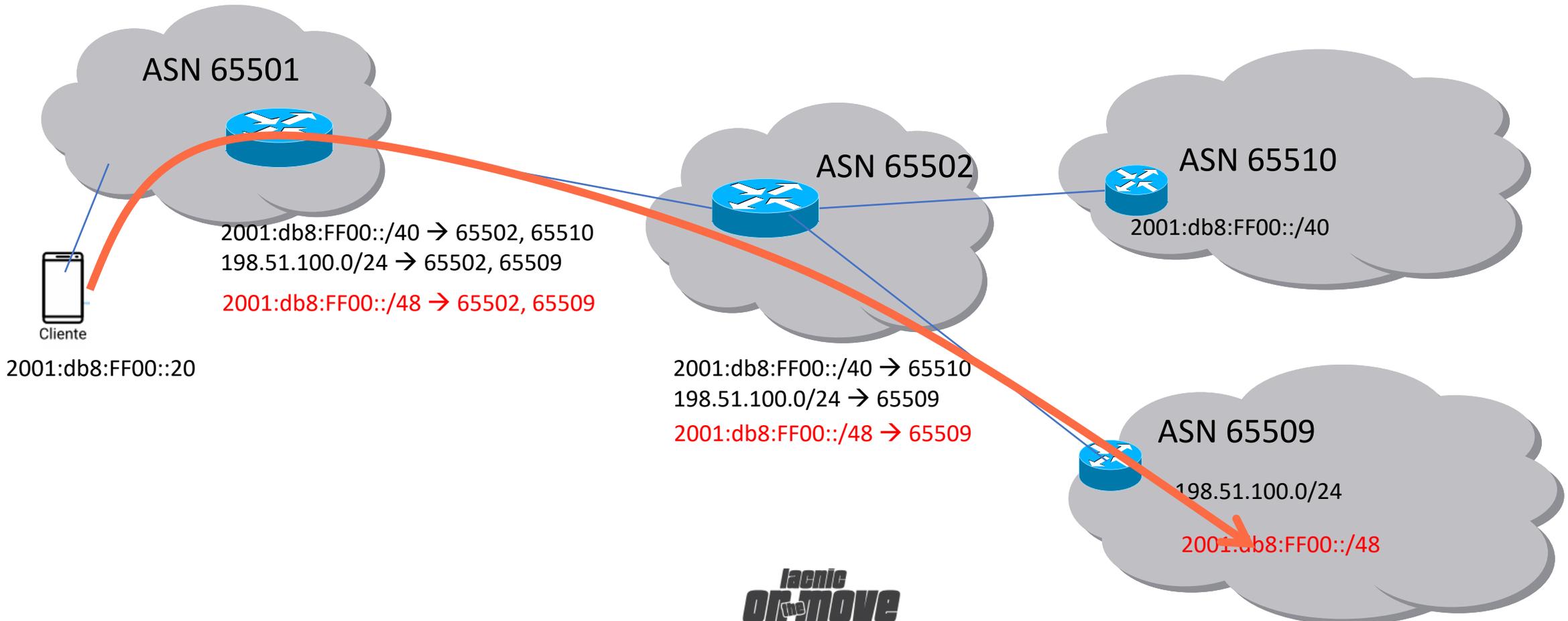
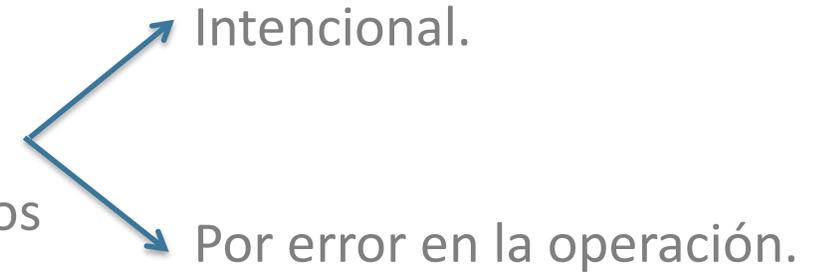
■ Outages ■ Leaks ■ Hijacks



Principales tipos de incidentes de ruteo

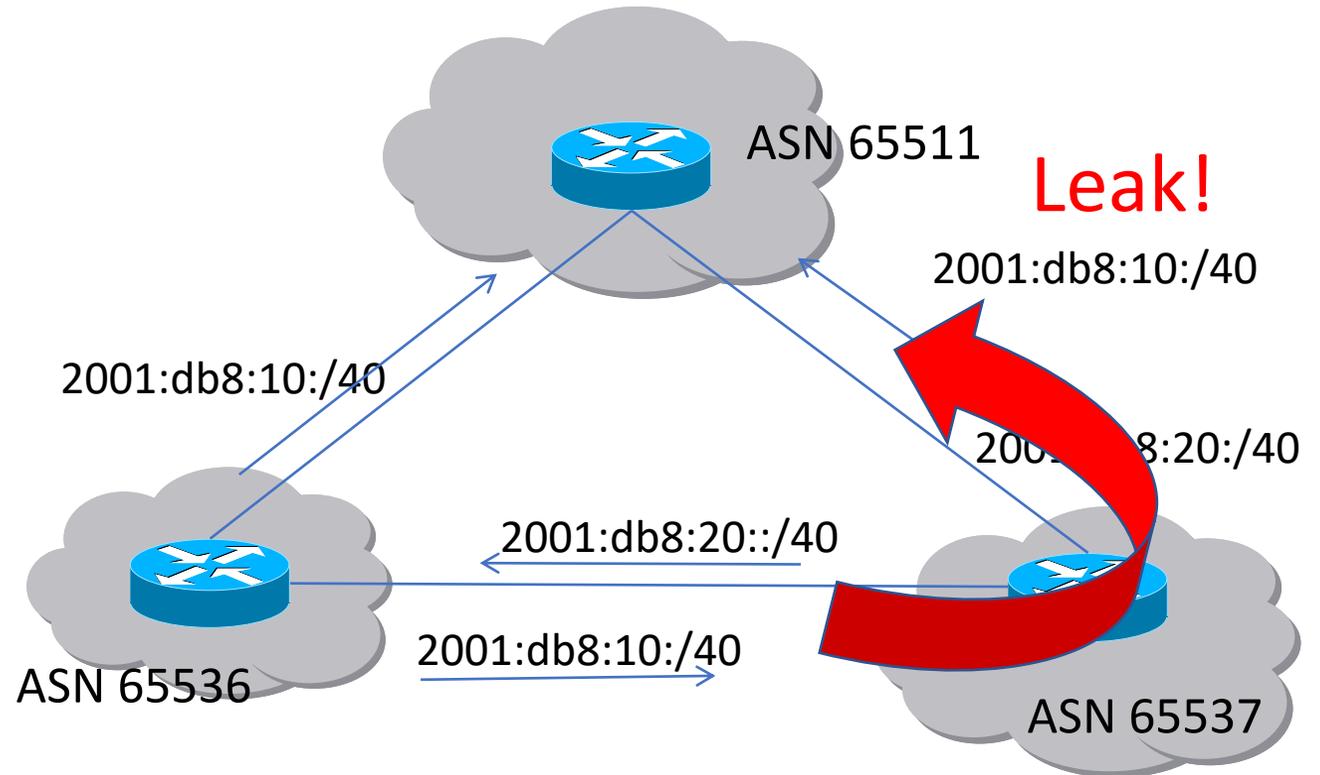
Secuestro de rutas

Secuestro de rutas:
Acción de anunciar
prefijos NO autorizados



Route leaks – fuga de rutas

- Prefijos aprendidos del **proveedor** no deben anunciarse a otro **peer** o a otro **proveedor**
- Prefijos aprendidos de un **peer** tampoco se anuncian a otros **peers** ni al **proveedor**
- Esos prefijos solo deberían anunciarse a **clientes**



Si no hay filtros configurados, esto trae problemas

¿Qué podemos hacer para mitigar los incidentes?

Acciones acordadas para promover la seguridad del ruteo

MANRS – Mejores prácticas

MANRS es un conjunto de "Normas Mutuamente Acordadas para la Seguridad del Enrutamiento"

Acciones propuestas por MANRS para **operadores**:

- Filtrado
- Anti-spoofing
- Coordinación
- Validación global

Veremos estas acciones en más detalle a continuación



Hay también un programa específico para **IXPs** y para **CDNs**

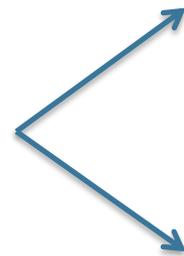
<https://www.manrs.org>

Seguridad en BGP

Tecnologías que facilitan la prevención de incidentes de seguridad

IRRs vs RPKI

- Cómo chequear que la información que recibimos por BGP es correcta?
 - BGP no tiene mecanismos intrínsecos que permitan verificar esto
 - Se deben contrastar los anuncios recibidos por BGP contra fuentes externas
- Existen dos formas:



IRR: Internet Routing Registries

RPKI: Resource Public Key
Infrastructure

IRR – Internet Routing Registries

- Existe una gran cantidad de IRRs
 - El más conocido es RADB
 - RADB replica todos los demas IRRs
- Las organizaciones definen sus políticas de ruteo en un IRR
- Los operadores (ISP) utilizan esa información para generar filtros para BGP, muchas veces en forma automática
- Existen herramientas para utilizar esa información y configurar los routers: bgpq3/bgpq4, etc.

- AFRINIC
- ALTDB
- AOLTW
- APNIC
- ARIN
- BELL
- BBOI
- CANARIE
- EASYNET
- EPOCH
- GT
- HOST
- JPIRR
- LEVEL3
- NESTEGG
- NTTCOM
- OPENFACE
- OTTIX
- PANIX
- RADB
- REACH
- RGNET
- RIPE
- RISQ
- ROGERS
- TC

- Ahora también LACNIC

Ejemplos de registros

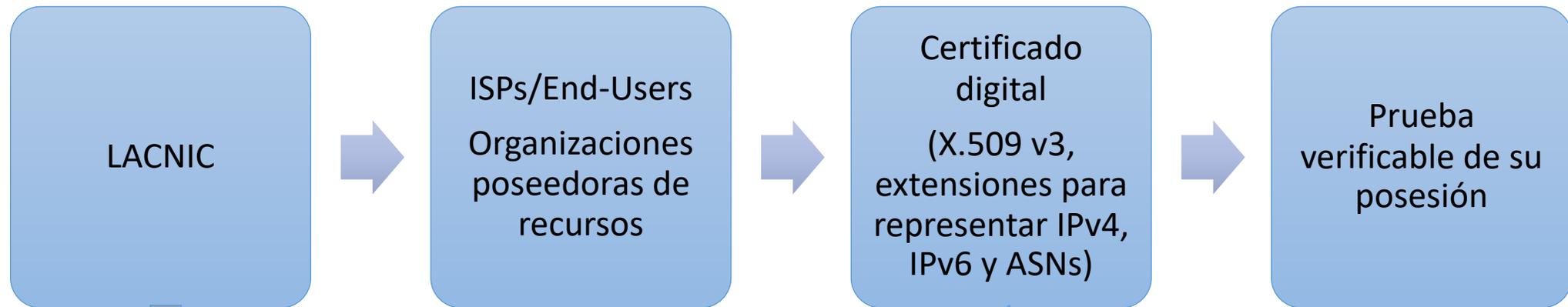
```
whois -h whois.radb.net -- '-s radb -i mnt-by MAINT-AS6057'
```

```
route:      201.221.32.0/19
descr:      ANTEL
origin:     AS6057
notify:     noc@antel.net.uy
mnt-by:     MAINT-AS6057
changed:    nantoniello@antel.net.uy 20080903
changed:    nantoniello@antel.net.uy 20080903 #19:20:32Z
source:     RADB
```

```
route:      201.217.128.0/18
descr:      ANTEL
origin:     AS6057
notify:     noc@antel.net.uy
mnt-by:     MAINT-AS6057
changed:    nantoniello@antel.net.uy 20080903
changed:    nantoniello@antel.net.uy 20080903 #19:21:34Z
source:     RADB
```

RPKI

- Define una infraestructura de clave pública especializada para ser aplicada al enrutamiento
 - En particular, para BGP



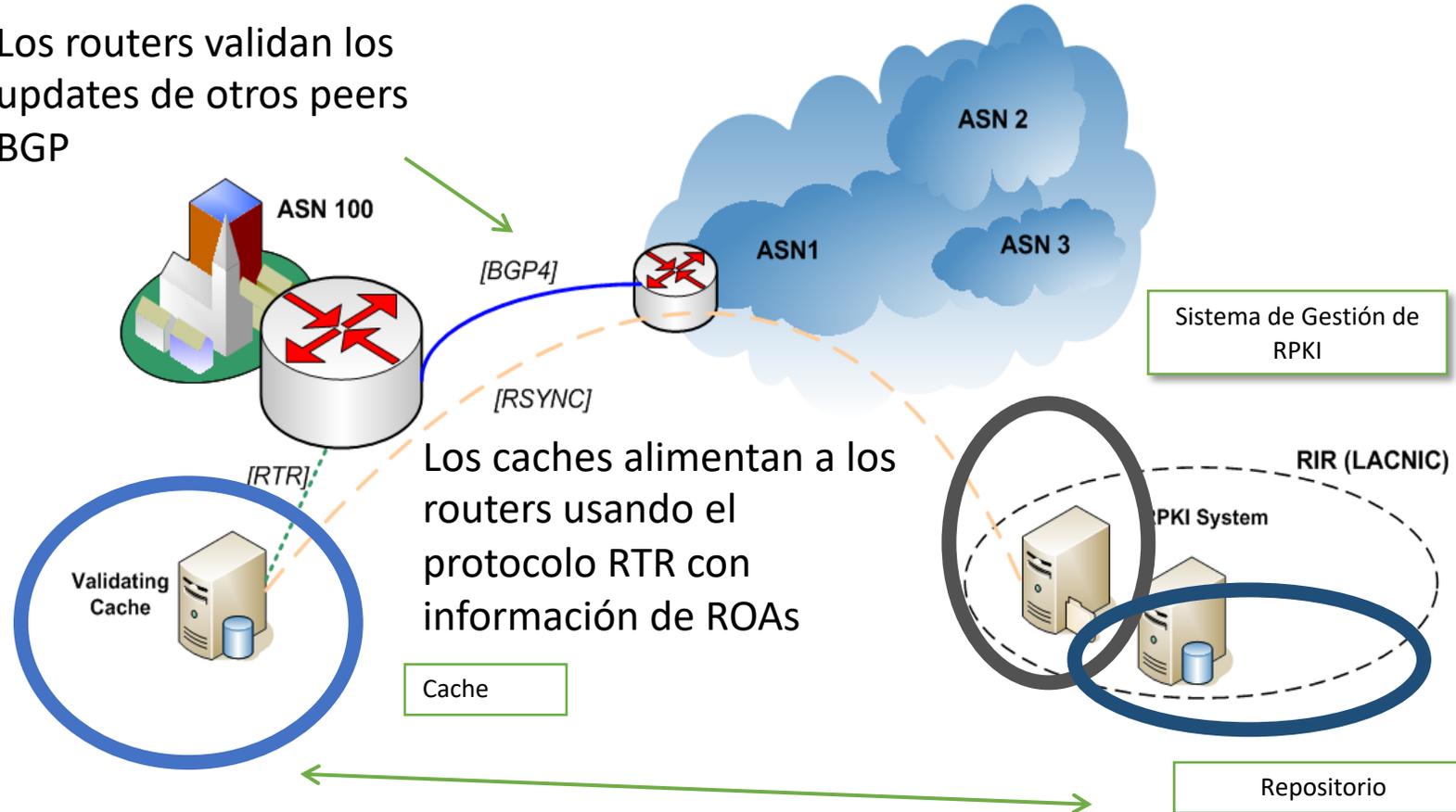
¿Qué compone la solución RPKI?

- **ROA:** Objetos firmados digitalmente para soportar seguridad del enrutamiento
 - Equivalentes a route o route6 objects de un IRR
 - Los ISPs u organizaciones pueden ***definir y certificar los anuncios de rutas que autorizan*** realizar
 - Los **ROAs** permiten definir el AS de origen para nuestros prefijos
 - **Firmados** con la clave privada del certificado
 - Toda la información es copiada en un **repositorio públicamente accesible**
- Un **mecanismo de validación** de prefijos
 - Validación de origen

Validación de Origen

RPKI en acción

Los routers validan los updates de otros peers BGP



Validación de Origen

- Una vez que los routers reciben la información de los caches, tendrán una tabla con:

Prefix	Length	Max length	Origin-AS
200.0.112.0	22	24	65501

- Con esto es posible asignar un ***estado de validez*** a cada UPDATE de BGP
- El estado de validez puede ser:
 - Válido: El AS de origen y el Largo Máximo coinciden con la información del ROA
 - Inválido: La información del ROA no coincide
 - No encontrado: No hay un ROA para el prefijo dado

Validador FORT

El validador FORT es un validador RPKI de código abierto

- Es parte del Proyecto FORT, iniciativa conjunta entre **LACNIC** y **NIC.MX**

Objetivos:

- Contribuir al despliegue de RPKI para aumentar la seguridad y la resiliencia de los sistemas de enrutamiento.
- Desarrollar una herramienta de monitoreo para estudiar incidentes de enrutamiento en la región y exponer secuestros intencionales.

Documentación

- Documentación general: <https://nicmx.github.io/FORT-validator/>
- Descargar el validador: <https://github.com/NICMx/FORT-validator/releases>

¿Preguntas hasta acá?



RPKI en la práctica

¿Cómo definir los ROA?

- Quienes tienen recursos IPv4, IPv6, ASN:
 - Pueden hacerlo desde el sistema de administración de recursos de LACNIC (MiLACNIC)
 - Se necesita para eso los datos de usuario y contraseña de administración de recursos
- Quienes no tienen recursos propios, dependerán del ISP
- Puede haber organizaciones con recursos IP pero no ASN
 - Deben crear los ROA permitiendo a cada ASN (upstream) anunciar los prefijos
 - La creación la realiza quien posee los recursos (diferente modelo que en el IRR en el que lo hace el que posee el ASN)

¿Qué tener en cuenta?

- Verificar cómo estamos realizando los anuncios
- Ejemplo: red 203.0.112.0/22
 - La estamos publicando sumariada?
 - La estamos publicando desagregada?
 - En bloques de qué tamaño? /23? /24?
 - Con qué sistema autónomo se originan las publicaciones?
 - Siempre es el mismos ASN?
 - Los distintos bloques se anuncian siempre con un mismo ASN?
- Importante: los ROA que creamos deben respetar esta política
- De lo contrario, estaremos invalidando nuestras publicaciones

Ejemplo de peering



ROAs que se necesita crear

Ejemplo Peering

ASN 65501

203.0.113.0/22

203.0.113.0/24

2001:db8:20::/48

Nombre:	ROA Peering ASN 65502	ASN	65501
Válido desde:	 07/05/2020	Válido hasta:	 07/05/2022
<input checked="" type="checkbox"/> ¿Extender la validez del ROA automáticamente?			
<input type="text" value="203.0.113.0/22"/>			
<input type="button" value="Guardar"/>			

ROAs que se necesita crear

Nombre:
ROA Peering ASN 65502

ASN
65501

Válido desde:
07/05/2020

Válido hasta:
07/05/2022

¿Extender la validez del ROA automáticamente?

203.0.113.0/22-24

Nombre:
ROA Peering ASN 65502

ASN
65501

Válido desde:
07/05/2020

Válido hasta:
07/05/2022

¿Extender la validez del ROA automáticamente?

2001:db8:20::/48

Guardar

ROAs que se necesita crear

ASN 65502

192.0.2.0/22

192.0.2.0/24

2001:db8:10::/48

Nombre:	<input type="text" value="ROA Peering ASN 65502"/>	ASN	<input type="text" value="65502"/>
Válido desde:	<input type="text" value="07/05/2020"/>	Válido hasta:	<input type="text" value="07/05/2022"/>
<input checked="" type="checkbox"/> ¿Extender la validez del ROA automáticamente?			
<input type="text" value="192.0.2.0/22"/>			
<input type="button" value="Guardar"/>			

ROAs que se necesita crear

Nombre:
ROA Peering ASN 65502

ASN
65502

Válido desde:
07/05/2020

Válido hasta:
07/05/2022

¿Extender la validez del ROA automáticamente?

192.0.2.0/22-24

Nombre:
ROA Peering ASN 65502

ASN
65502

Válido desde:
07/05/2020

Válido hasta:
07/05/2022

¿Extender la validez del ROA automáticamente?

2001:db8:10::/48

Guardar

Herramientas útiles

- Mi LACNIC: <https://milacnic.lacnic.net>
- ROA Wizard: <https://tools.labs.lacnic.net/roa-wizard/>
- ROA Announcement: <https://tools.labs.lacnic.net/announcement/>
- RIPE RIS: <https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris>
- BGP HE.NET <https://bgp.he.net>
- Documentación RPKI: <https://rpki.readthedocs.io/en/latest/>

¿Preguntas hasta acá?



IRR de LACNIC

Algunas decisiones de diseño

- La mayoría de la información requerida ya existe en alguna base de datos de LACNIC
 - WHOIS, RPKI
- Reutiliza la información ya disponible:
 - route(6) generados a partir de RPKI
 - autnum y maintainers del whois
- No se hará una implementación completa de RPSL:
 - Los operadores utilizan solo una pequeña parte de las facilidades
 - Lo principal que estaría faltando en RPKI es el objeto AS-SET
 - AS-SET debe puede ser definido por el usuario

ROAs vs route(6)

- Un ROA es semánticamente equivalente a un route(6) object:
 - **Asocia un prefijo a un ASN de origen**
 - Con esta información es posible hacer chequeo de un anuncio BGP
- Los ROAs están firmados criptográficamente, los objetos en un IRR no
- Los ROAs no pueden ser alterados por un tercero
 - El repositorio es seguro
- RPKI sólo implementa un subconjunto de lo que un IRR puede definir

Cómo usar la información

Ejemplo de peering



Utilizar la información del IRR

- Obtenemos todos los prefijos IPv6 del ASN 65502:

```
$ whois -h irr.lacnic.net '!6AS65502'
```

A...

```
2001:db8:10::/48
```

C

- Obtenemos todos los prefijos IPv4 del ASN 65502:

```
$ whois -h irr.lacnic.net '!gAS65502'
```

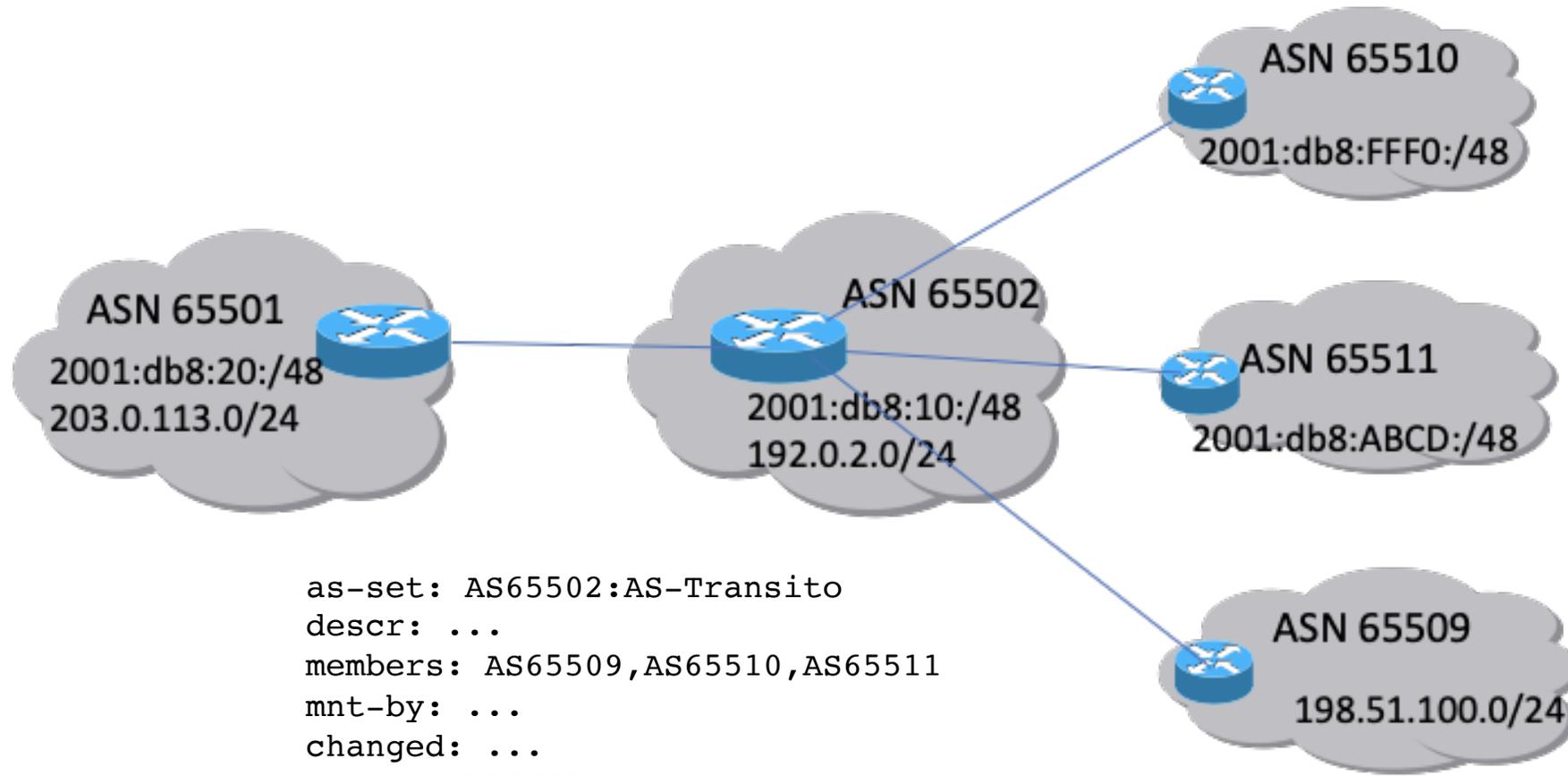
A...

```
192.0.2.0/24
```

C

- Más info en: <https://irrd4.readthedocs.io/en/master/users/queries.html>

Ejemplo de tránsito



```
as-set: AS65502:AS-Transito
descr: ...
members: AS65509,AS65510,AS65511
mnt-by: ...
changed: ...
source: LACNIC
```

Utilizando bgpq3/bgpq4

- En este caso, usamos el as-set:

- Prefijos IPv4

```
$ bgpq4 -h irr.lacnic.net -l clientes-as65502 AS65502:AS-Transito  
no ip prefix-list clientes-as65502  
ip prefix-list clientes-as65502 permit 198.51.100.0/24
```

- Prefijos IPv6

```
$ bgpq4 -h irr.lacnic.net -6 -l clientes-as65502 AS65502:AS-Transito  
no ipv6 prefix-list clientes-as65502  
ipv6 prefix-list clientes-as65502 permit 2001:db8:FFF0:/48  
ipv6 prefix-list clientes-as65502 permit 2001:db8:ABCD:/48
```

- Ver más información sobre bgpq4 en <https://github.com/bgp/bgpq4>

Referencias

- Cursos de Campus de LACNIC: <https://campus.lacnic.net> (BGP y RPKI)
- Tutorial de BGP y RPKI de LACNIC32: <https://www.lacnic.net/3900/52/evento/tutoriales>
- Webinar: Seguridad en el ruteo de América Latina y el Caribe (Augusto Mathurín)
<https://www.lacnic.net/4413/1/lacnic/>
- Webinar: Implementación de servicio UpDown de LACNIC y KRILL (Carlos Ortiz)
<https://www.lacnic.net/4350/1/lacnic>

- Documentación RPKI: <https://rpki.readthedocs.io/en/latest/>
- Proyecto FORT: www.fortproject.net
- IRR de LACNIC: <https://labs.lacnic.net/UsodeIRR-LACNIC/>
- Documentación Mi LACNIC:
 - General: <https://lacnic.zendesk.com/hc/es/categories/360002625214-Internet-Routing-Registry>
 - RPKI: <https://lacnic.zendesk.com/hc/es/sections/206490008-RPKI>
 - IRR: <https://lacnic.zendesk.com/hc/es/categories/203940327-Soporte-Mi-LACNIC>

¿Preguntas?



Muchas gracias!

