lacnic 46
lacnog 2026
19 - 22 OCTUBRE / MENDOZA, ARGENTINA

BGP en 2026: amenazas, incidentes y soluciones

Erika Vega – evega@nog.lat
Álvaro Retana - aretana.ietf@gmail.com
Guillermo Cicileo - guillermo@lacnic.net

Qué vamos a ver hoy

Bloque	Tema
1	Amenazas e incidentes de ruteo
2	Buenas prácticas y validación de información
3	Route leaks y BGP Roles
4	RPKI: de la validación de origen a la operación
	Pausa
5	Más allá de ROV: ASPA
6	Mitigación y respuesta ante ataques
7	Qué hago mañana en mi red?
	Total (con margen y preguntas)

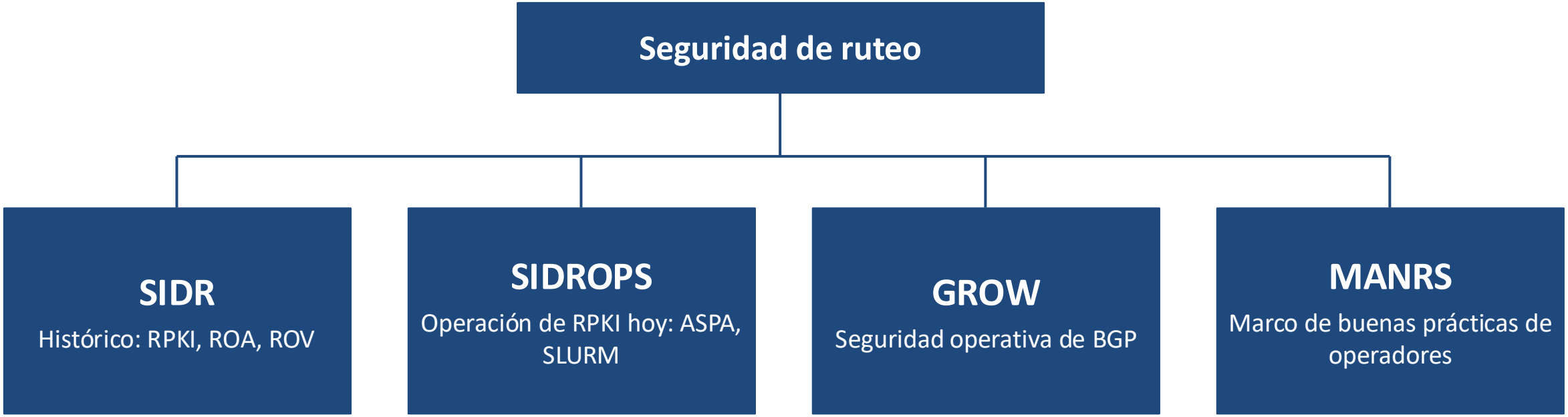
1. AMENAZAS E INCIDENTES DE RUTEO

Modelo de amenazas: ¿qué puede salir mal?

Amenaza	Ejemplo	Mitigación	Bloque
Secuestro de origen	Anunciar prefijos ajenos	ROAs + ROV	4
Manipulación del camino	AS_PATH falsificado con origen válido	ASPA (BGPsec: sin despliegue)	5
Route leak	Prefijos de un proveedor re-anunciados a otro	Filtros, BGP Roles / OTC, ASPA	2, 3, 5
Ataques a la sesión o a atributos	Sesiones eBGP abusadas, prefijos en exceso	TTL security (GTSM), TCP-AO, max-prefix	2
Agotamiento de recursos / DDoS	Tráfico volumétrico hacia un destino	RTBH, BLACKHOLE, Flowspec	6

Varias amenazas no tienen solución criptográfica hoy

¿Dónde se define y se discute todo esto?



IETF
Estándares (RFC). Aquí nace ASPA

MANRS
Iniciativa de operadores

RFC 4272
Catálogo canónico de vulnerabilidades de BGP

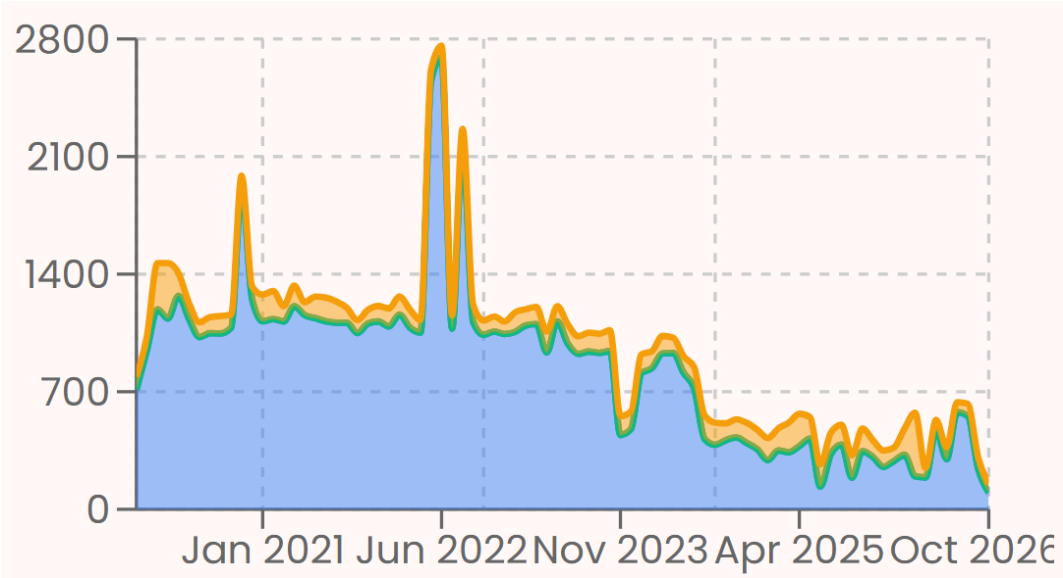
Cuatro grupos para ordenar el día

Amenazas	Prevención y validación	Mitigación y respuesta	Operación y gobernanza
• Hijacks • Leaks • Bogons • DDoS	• Filtros e IRR • ROA / ROV • BGP Roles / OTC • ASPA	• RTBH • BLACKHOLE • Flowspec	• MANRS • Validadores al día • SIDROPS / GROW

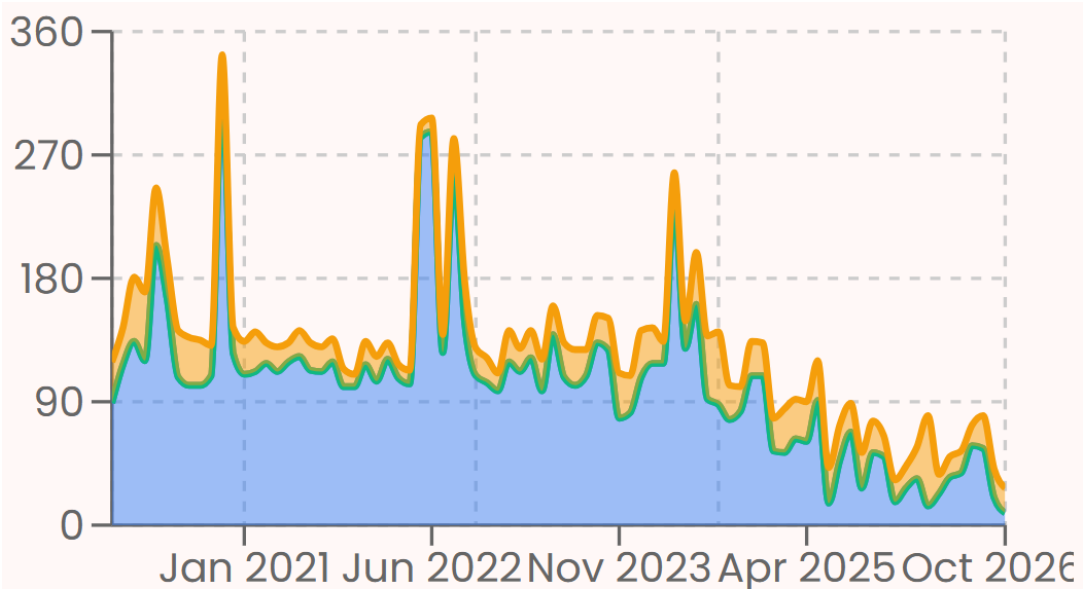
INCIDENTES DE RUTEO

Principales incidentes de seguridad

GLOBAL



LAC



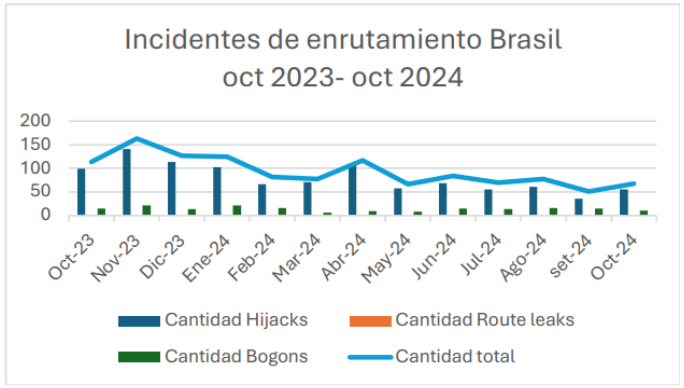
- Route misoriginations
- Route leaks
- Bogon announcements

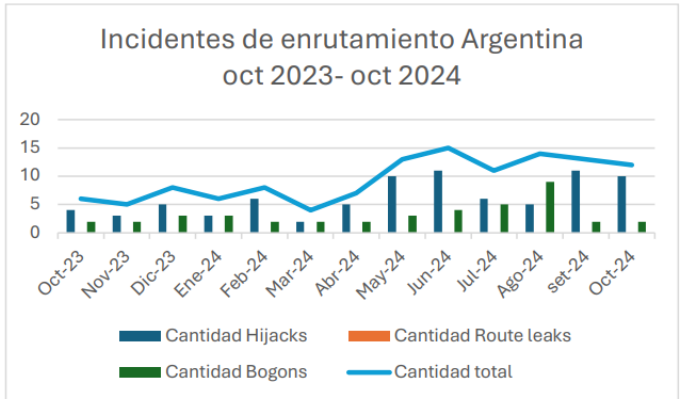
Fuentes:

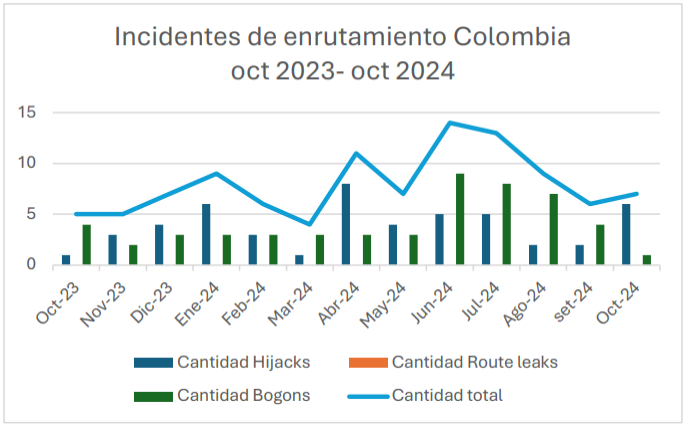
MANRS: https://observatory.manrs.org/history

TOP 5 incidentes en LAC





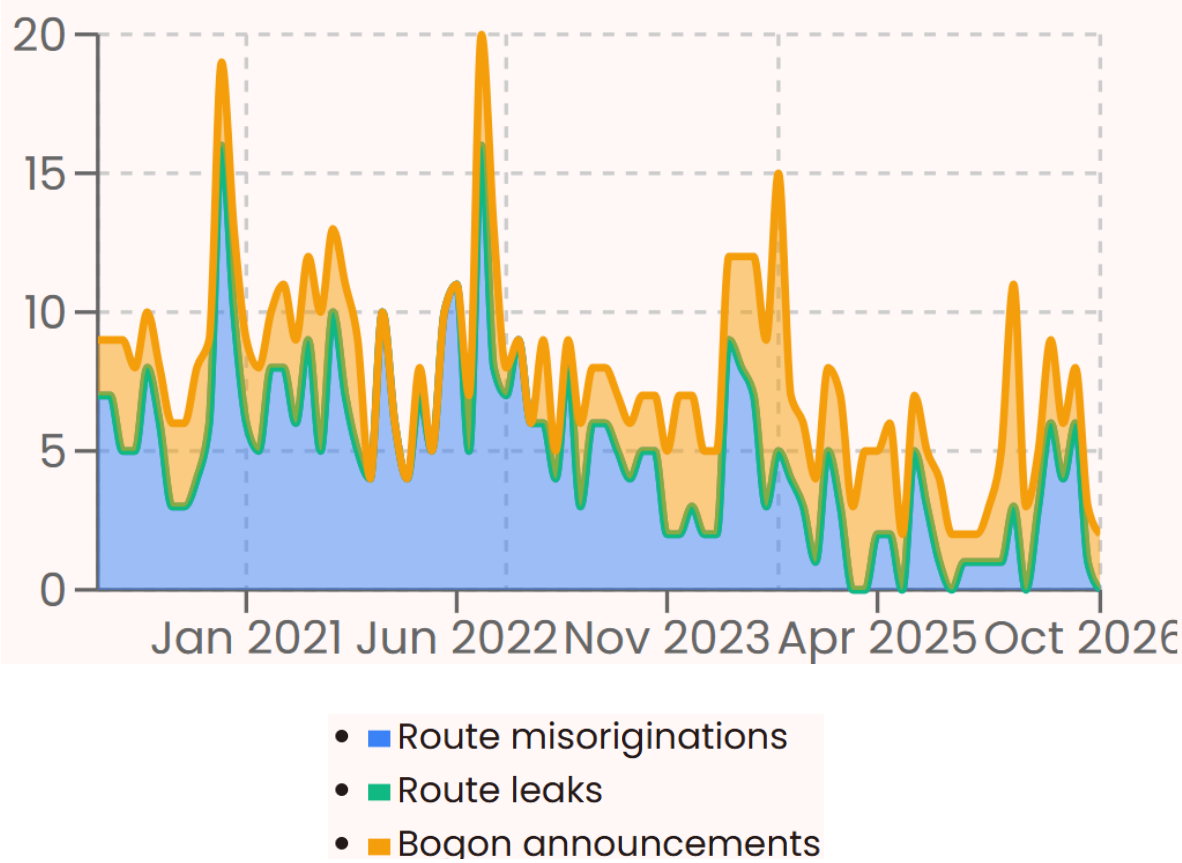




Fuente:

https://imasd.lacnic.net/reportes/interconexion/lacnic-analisis-incidentes-enrutamiento-lac-es.pdf

Incidentes de enrutamiento en Argentina



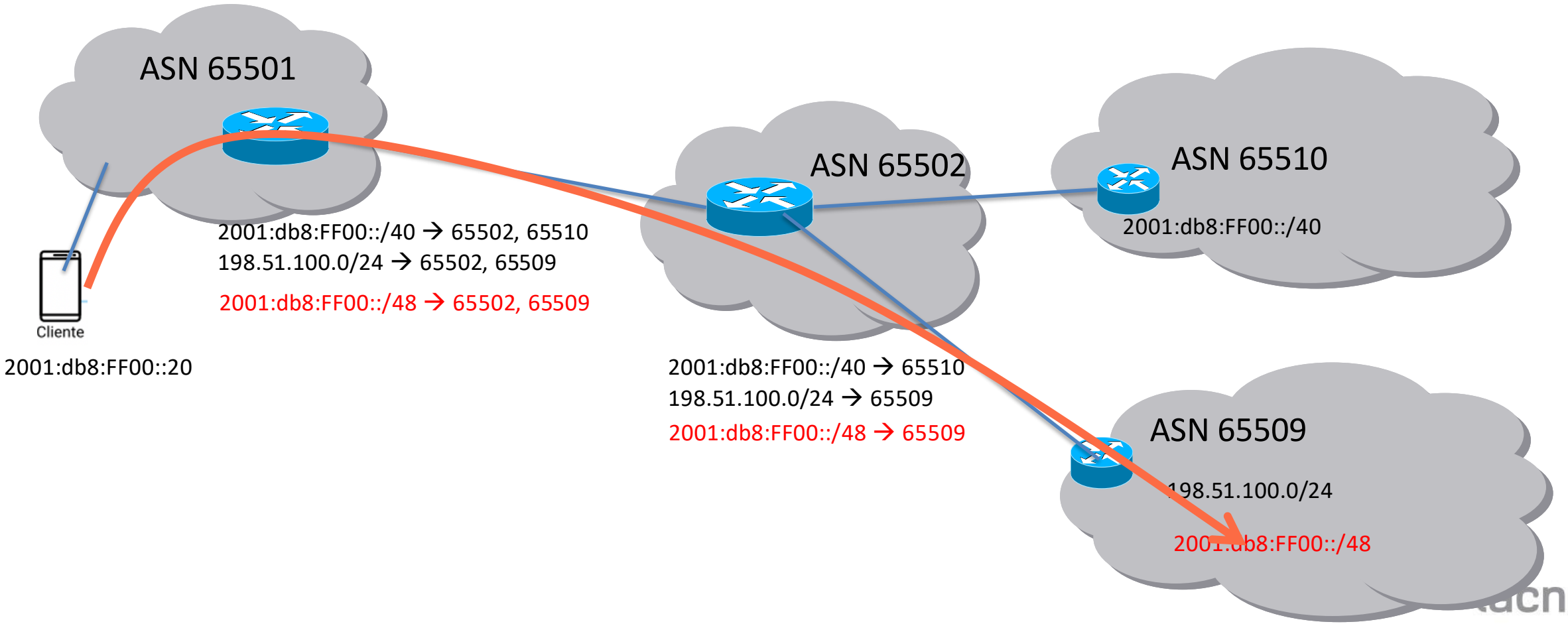
Date	Route misoriginatio	Route leaks	Bogon announceme
Jan 2026	1	0	2
Feb 2026	1	0	4
Mar 2026	3	0	8
Apr 2026	0	0	3
May 2026	3	0	2
Jun 2026	6	0	3
Jul 2026	4	0	2
Aug 2026	6	0	2
Sep 2026	1	0	2
Oct 2026	0	0	2

Fuente: https://observatory.manrs.org/#/history

Secuestro de rutas

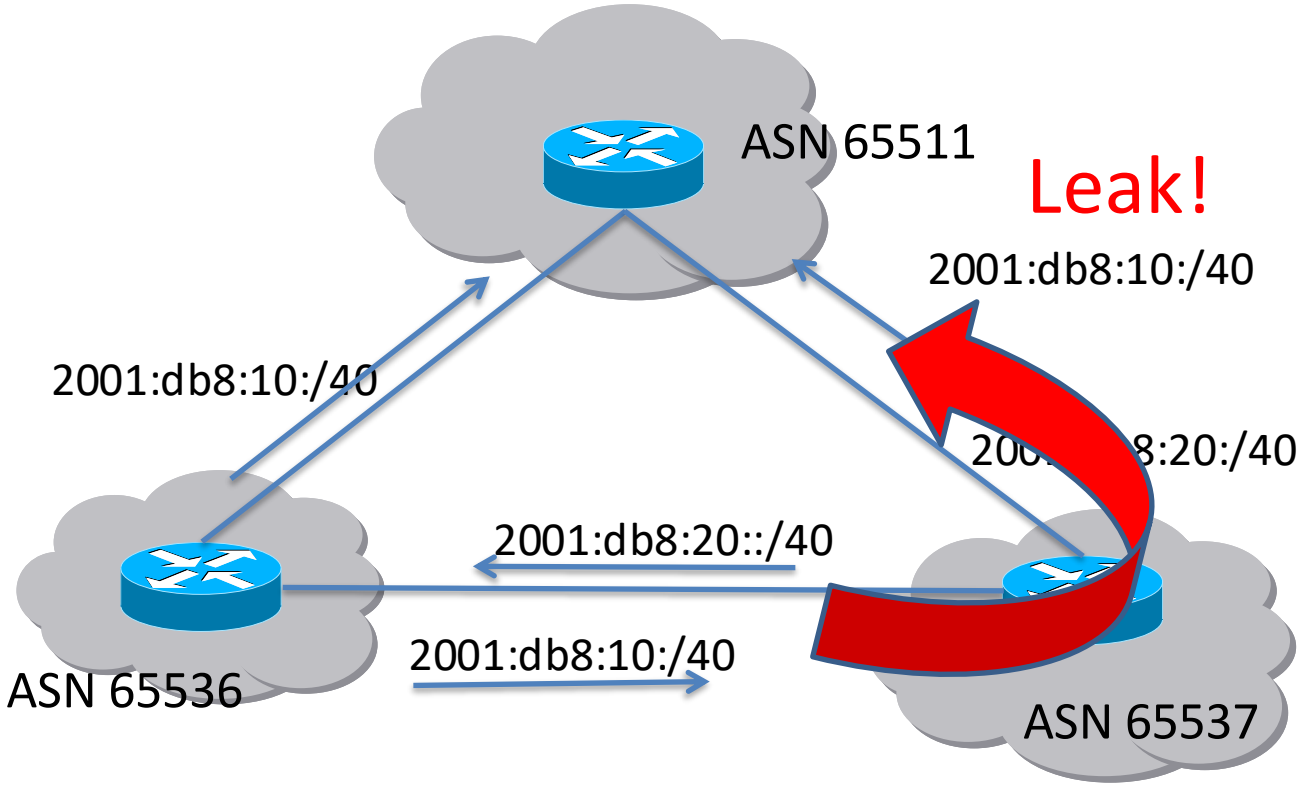
Secuestro de rutas:
Acción de anunciar
prefijos NO autorizados

- Intencional.
- Por error en la operación.



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

Bogons

Un “Bogon” (plural: “bogons”) es un paquete cuya dirección IP de origen pertenece a un bloque de direcciones que aún no ha sido asignado por la Internet Assigned Numbers Authority-IANA o por los Registros Regionales de Internet-RIR así como también todas las direcciones reservadas para uso privado o especial definidas en RFCs. RFC3330 y RFC1918.

Bogons = Marcianos + Espacio de direcciones no asignado en IANA y RIR/NIR

Fuente: RFC 3871_ septiembre 2004

lacnic

2. BUENAS PRÁCTICAS Y VALIDACIÓN DE INFORMACIÓN

MANRS

Normas acordadas para la seguridad de enrutamiento.

- Dar soluciones a tres clases de problemas:
  - Relativos a información de ruteo incorrecta
  - Relativos a tráfico con IP de origen spoofed
  - Relativos a la coordinación y colaboración entre operadores de red

- Busca una solución adoptada y coordinada por los propios operadores y no impuesta por alguna regulación

Programas MANRS

- MANRS para Operadores de Red
- MANRS para IXPs
- MANRS para CDNs y Proveedores de Nube
- MANRS para fabricantes

lacnic

MANRS – Para operadores de red

Filtering

Asegure la exactitud de sus propios anuncios y anuncios de sus clientes a redes adyacentes con prefijo y granularidad AS-path.

Anti-spoofing

Habilite la validación de la dirección de origen para al menos una red del cliente que tiene un único punto de entrada y salida, sus propios usuarios finales e infraestructura

Coordination

Mantener la información de contacto actualizada y accesible a nivel mundial en bases de datos de enrutamiento comunes

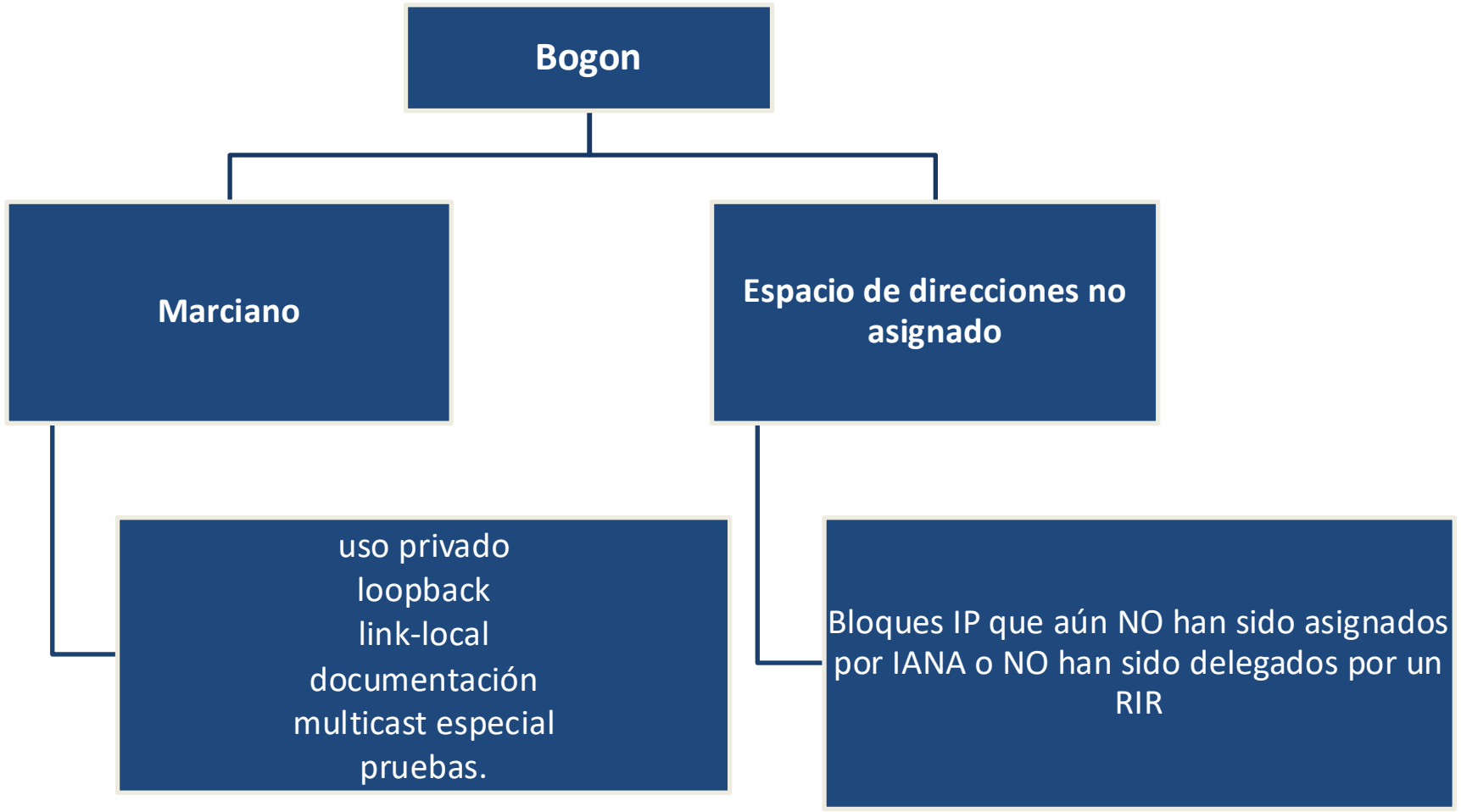
Global Validation

Publique sus datos para que otros puedan validar.

lacnic

FILTRADO

Tipos de Bogons por prefijos



Ejemplos

10.0.0.0/8, 192.168.0.0/16, 169.254.0.0/16, 100.64.0.0/10

Origen

Configuraciones erróneas accidentales o intenciones maliciosas.

Impacto

Ataques DDoS, suplantación de IP y tráfico malicioso.

Fuente: RFC 1918 , RFC 5735 , RFC 6598 y RFC 6598 Definiciones de Marcianos: RFC1208 y RFC3871

lacnic

Tipos de Bogons por prefijos IPv6



Documentación — RFC 3849

`2001:db8::/32` — Solo para ejemplos y documentación.

ULA Privados — RFC 4193

`fc00::/7` — Direcciones únicas locales, no enrutables globalmente.

Enlace-Local — RFC 4291

`fe80::/10` — Válidas solo en el segmento local.

Deprecados

`3ffe::/16` (6bone) y `fec0::/10` (Site-Local) — ya no en uso.

Fuente: RFC 3849 , RFC 4193 y RFC 4291

lacnic

¿Qué pasa con los ASN bogon?

Un ASN se considera bogon si se cumple alguna de las siguientes condiciones:

- Está reservado para uso especial por un RFC
- No forma parte del bloque asignado a un RIR por IANA
- No está asignado a un LIR por ningún RIR.

Número/Rango AS	Estado	Referencia RFC
0	Reservado (no se puede usar en BGP)	RFC7607
23456	AS_TRANS	RFC6793
64496-64511	Reservado para su uso en documentación y código.	RFC5398
64512-65534	Reservado para uso privado.	RFC6996
65535	Reservado	RFC7300
65536-65551	Reservado para su uso en documentación y código.	RFC5398
65552-131071	Reservado	Por IANA
4200000000-4294967294	Reservado para uso privado.	RFC6996
4294967295	Reservado	RFC7300

lacnic

Como filtrar los bogons

Filtrar rutas recibidas desde:

- peers
- upstreams
- Customers(BCP 38-BCP 84- URPF)

Evitar anunciar:

- Diferentes RFCs mencionados anteriormente
- loopback
- link-local
- unallocated space

Ejemplo de filtros por prefijos

Creación de Prefix-list

```
ip prefix-list BOGONS seq 10 deny 10.0.0.0/8 le 32
ip prefix-list BOGONS seq 20 deny 172.16.0.0/12 le 32
ip prefix-list BOGONS seq 30 deny 192.168.0.0/16 le 32
ip prefix-list BOGONS seq 40 deny 127.0.0.0/8 le 32
ip prefix-list BOGONS seq 50 deny 169.254.0.0/16 le 32
ip prefix-list BOGONS seq 100 permit 0.0.0.0/0 le 32
```

Aplicación de route-map

```
route-map FILTER-BOGONS deny 10
 match ip address prefix-list BOGONS

route-map FILTER-BOGONS permit 20
```

Aplicación en el vecino BGP

```
router bgp 65001
 neighbor 203.0.113.1 route-map FILTER-BOGONS in
```

lacnic

Ejemplo de filtros por ASN

Creación de Access-list

```
ip as-path access-list 10 deny _0_
ip as-path access-list 10 deny _23456_
ip as-path access-list 10 deny _6451[2-9]_
ip as-path access-list 10 deny _645[2-9][0-9]_
ip as-path access-list 10 deny _64[6-9][0-9][0-9]_
ip as-path access-list 10 permit .*
```

Aplicación de route-map

```
route-map FILTER-ASN-BOGONS deny 10
 match as-path 10

route-map FILTER-ASN-BOGONS permit 20
```

Aplicación en el vecino BGP

```
router bgp 65001
 neighbor 203.0.113.1 route-map FILTER-ASN-
BOGONS in
```

lacnic

El problema de las listas estáticas

Un prefijo o un ASN:

- hoy puede ser Bogon
- mañana puede ser asignado por IANA

Mejor práctica operacional

- NO mantener listas manuales gigantes
- Usar:feeds automáticos

Team Cymru Bogon feeds

Ejemplo Team Cymru Bogon Feed

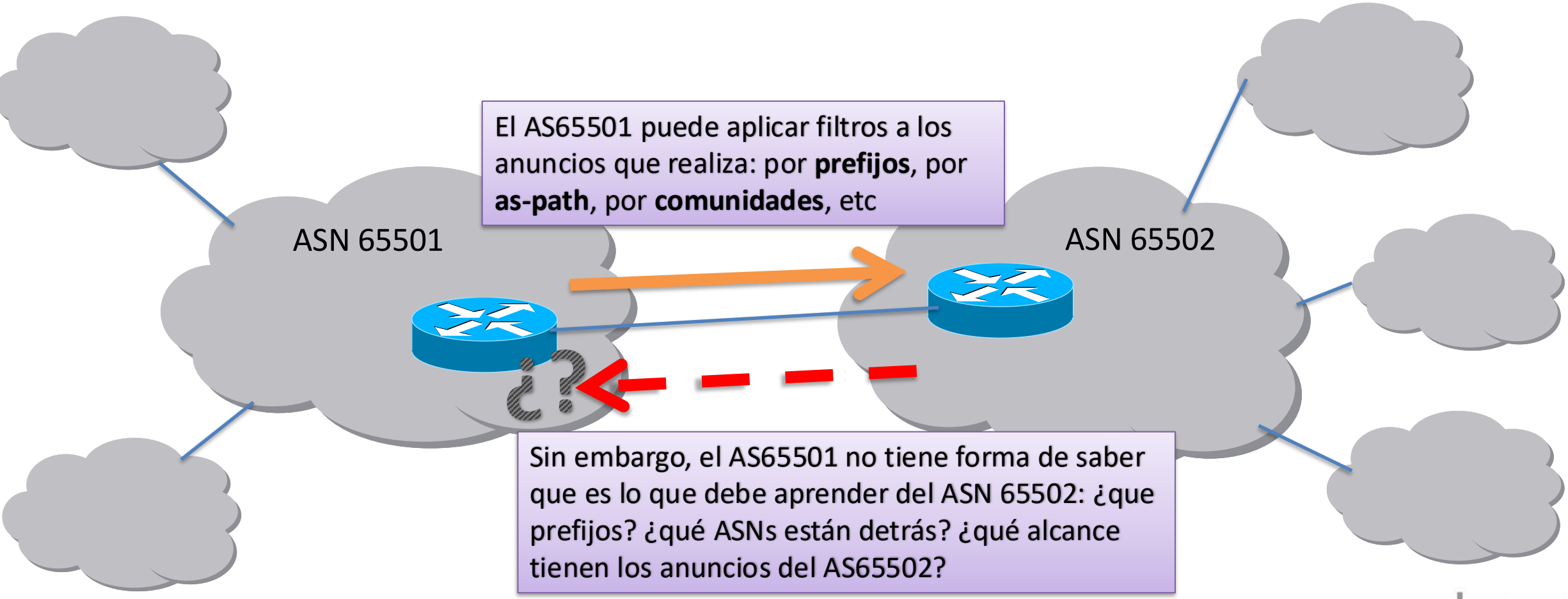
Funcionamiento

El operador establece una sesión BGP con;Team Cymru Bogon Project y recibe automáticamente:

- prefijos bogon
- updates dinámico

¿CÓMO OBTENER INFORMACIÓN MÁS ALLÁ DE NUESTRO SISTEMA AUTÓNOMO?

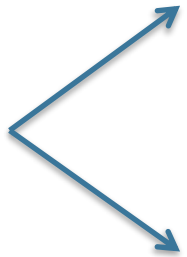
BGP: filtros de salida y entrada



Peering con otros ASN

- ¿Qué necesitamos informar a nuestros peers?
  - Es común que nos pidan información acerca de los prefijos y sistemas autónomos que vamos a anunciar
    - Por medios informales como un email o una LOA (Letter of Authorization)

Proveedores/peers: verifican derecho de uso



Whois RIRs: Información no firmada, no utilizable directamente para ruteo

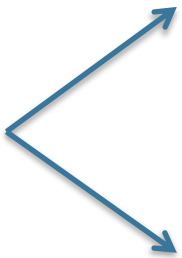
Whois IRR: Información no firmada, pocos mecanismos para autentificación de derecho de uso

- La verificación no siempre es todo lo meticulosa que debería ser
- La integridad del sistema depende de la **confianza entre peers**

lacnic

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

lacnic

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.

https://irr.net/registry/



AFRINIC
ALTDB
APNIC
ARIN
BELL
BBOI
CANARIE
IDNIC
JPIRR
LACNIC
LEVEL3
NESTEGG
NTTCOM
PANIX
RADB
REACH
RIPE
TC

lacnic

Ejemplos de registros

```
whois -h irr.lacnic.net '!oMNT-UY-NICO1-LACNIC'

route6:          2803:9910:8000::/34
descr:           LACNIC generated route6 for Ni Co
origin:          AS64135
remarks:         LACNIC generated route6 for Ni Co
remarks:         maxLength 48
mnt-by:          MNT-UY-NICO1-LACNIC
changed:         20220908
source:          LACNIC
remarks:         ************************************************
remarks:         This object may have been modified
remarks:         For more information, please query whois.lacnic.net
remarks:         ************************************************
last-modified:   2022-09-08T22:45:05Z

aut-num:         AS64136
descr:           LACNIC generated autnum for Ni Co
as-name:         AS64136
tech-c:          NIA14
remarks:         LACNIC generated autnum for UY-NICO1-LACNIC
mnt-by:          MNT-UY-NICO1-LACNIC
changed:         20220414
source:          LACNIC
remarks:         ************************************************
remarks:         This object may have been modified
remarks:         For more information, please query whois.lacnic.net
remarks:         ************************************************
last-modified:   2022-04-14T23:05:04Z
```

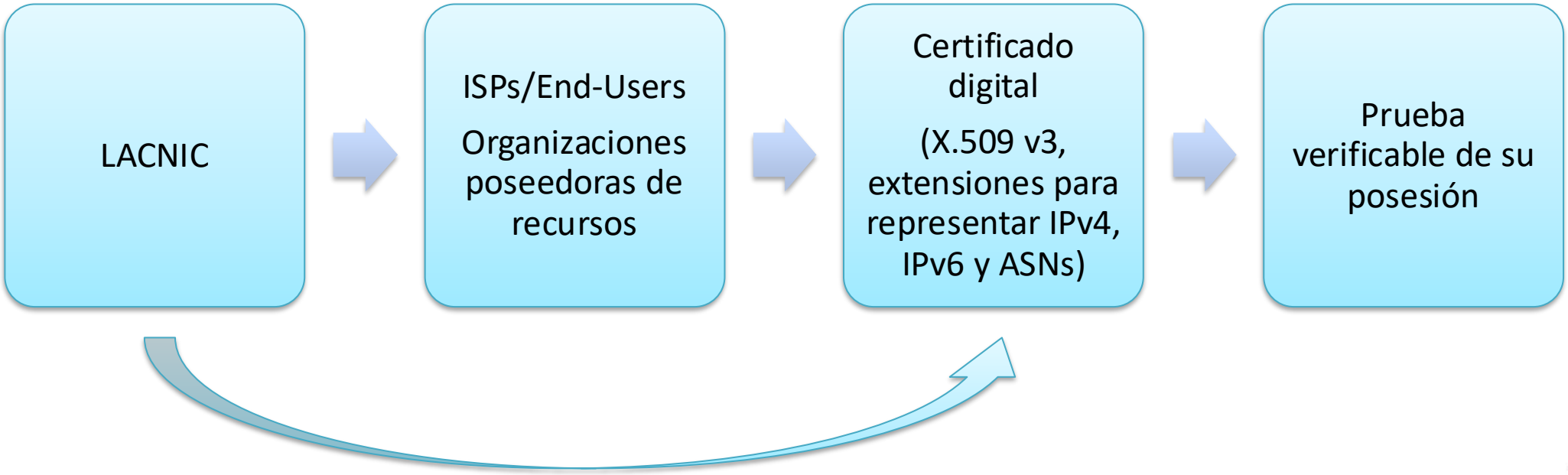
¿Por qué los IRR (Internet Routing Registry) no son suficiente?

Datos No Fiables	Información Desactualizada	Modelo de autenticación/autorización débil
• Los IRR almacenan información sobre qué AS debe originar qué prefijos, pero dependen de la precisión de los usuarios para mantener actualizada la información	• Múltiples fuentes de datos sin control centralizado generan inconsistencias. Errores tipográficos y configuraciones obsoletas son comunes en los registros	• Falta de mecanismos para validar automáticamente la autenticidad de las declaraciones de enrutamiento

lacnic

RPKI

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



Repaso de lo visto hasta ahora

- Modelo de amenazas
- Incidentes de ruteo: secuestros, leaks y bogons
- Mejores prácticas y MANRS
- Mecanismos para obtener información sobre otros sistemas autónomos:
  - IRR
  - RPKI



3. ROUTE LEAKS Y ROLES EN BGP

Clasificación de route leaks RFC 7908

¡¡¡Recordemos!!!

Es la propagación de anuncios de enrutamiento más allá de su alcance previsto. Es decir, un anuncio de un Sistema Autónomo (AS) de una ruta aprendida por BGP hacia otro AS, que viola las políticas previstas del receptor, el remitente y/o uno de los ASes a lo largo del camino.

Clasificación de route leaks RFC 7908

RFC aprobado y publicado con fines informativos en Junio del 2016.

Describe y enumera diferentes tipos de fuga de rutas, basándose en eventos ya presentados en el enrutamiento de Internet

Clasificación de route leaks RFC 7908

Tipo 1: Fuga de proveedor de tránsito a otro proveedor de tránsito

Tipo 2: Fuga lateral de peer a otro peer

Tipo 3: Fuga de prefijos de proveedor de tránsito hacia un peer

Tipo 4: Fuga de prefijos de un peer hacia proveedor de tránsito

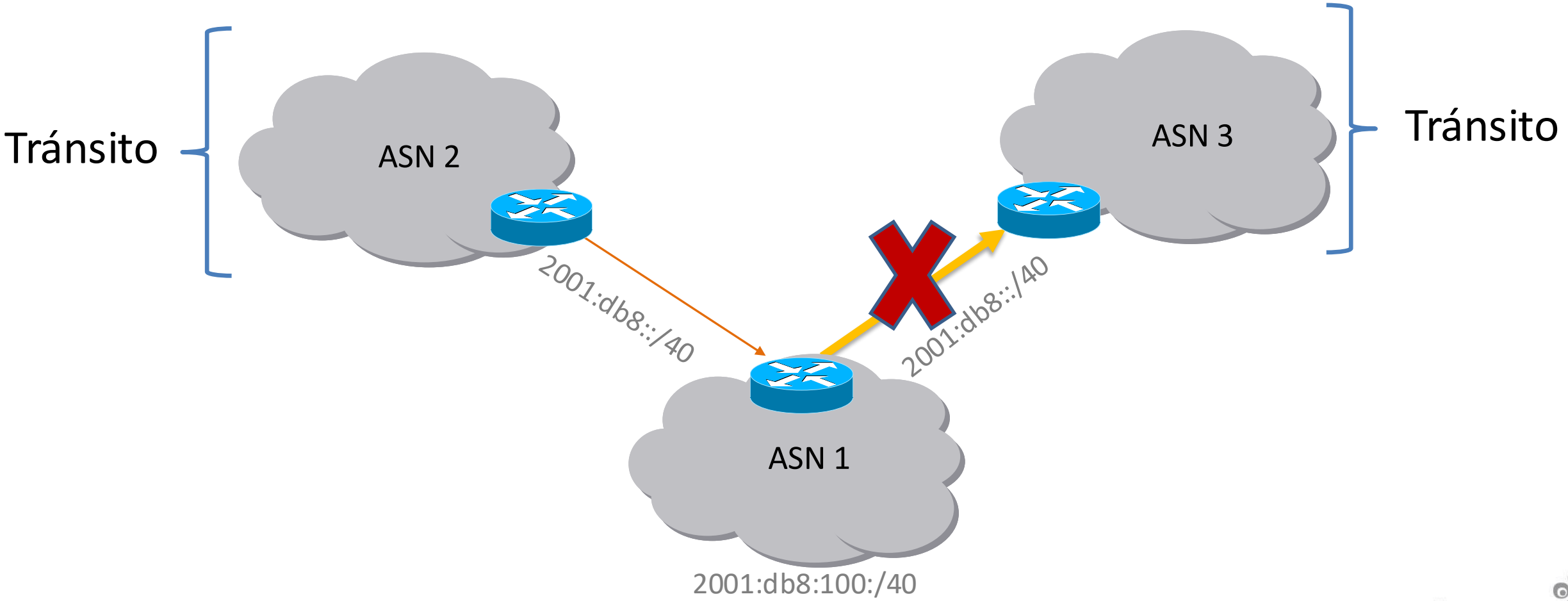
Tipo 5: Prefijo re originado cambiando el AS de origen

Tipo 6: Fuga accidental de prefijos internos y prefijos más específicos.

lacnic

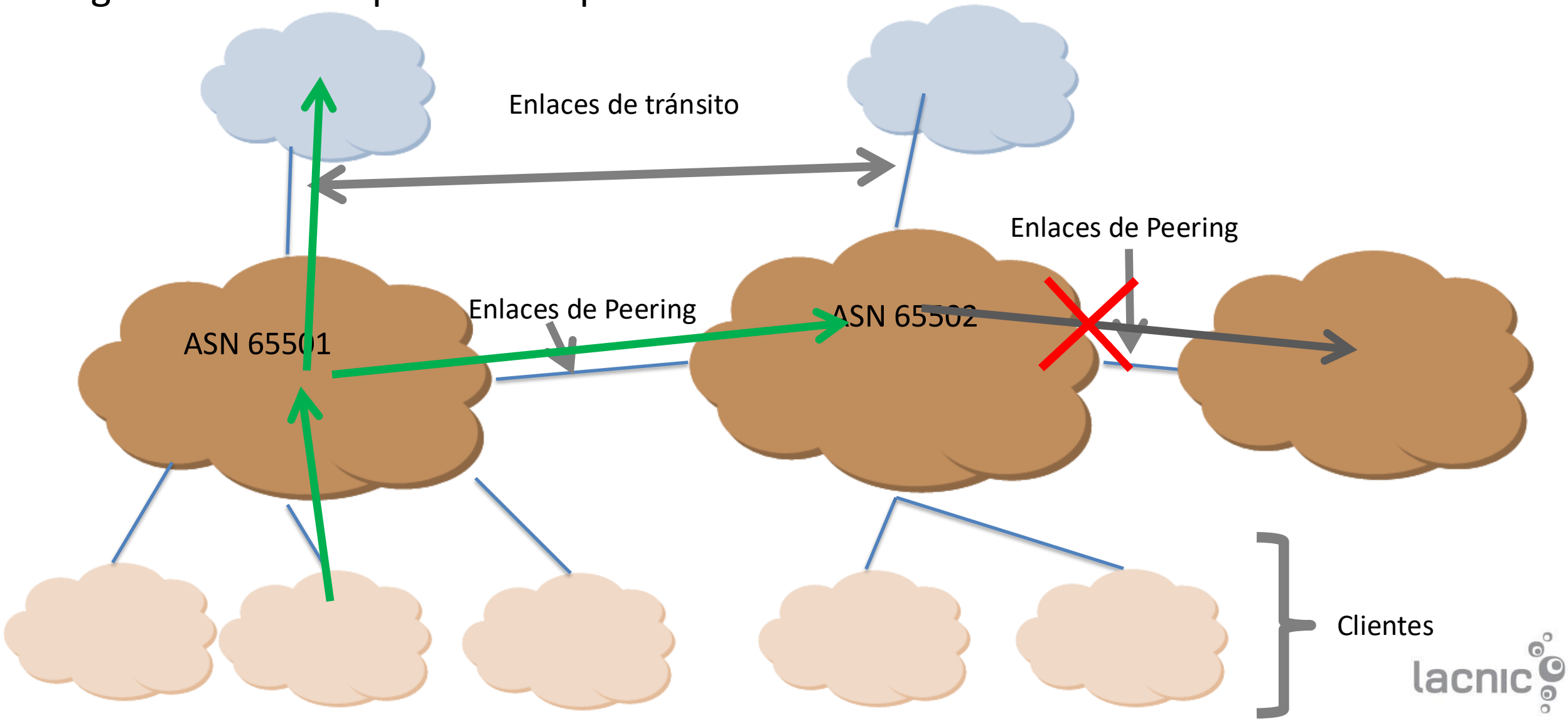
Ejemplos de tipos de fuga de rutas

Fuga de proveedor de tránsito a otro proveedor de tránsito



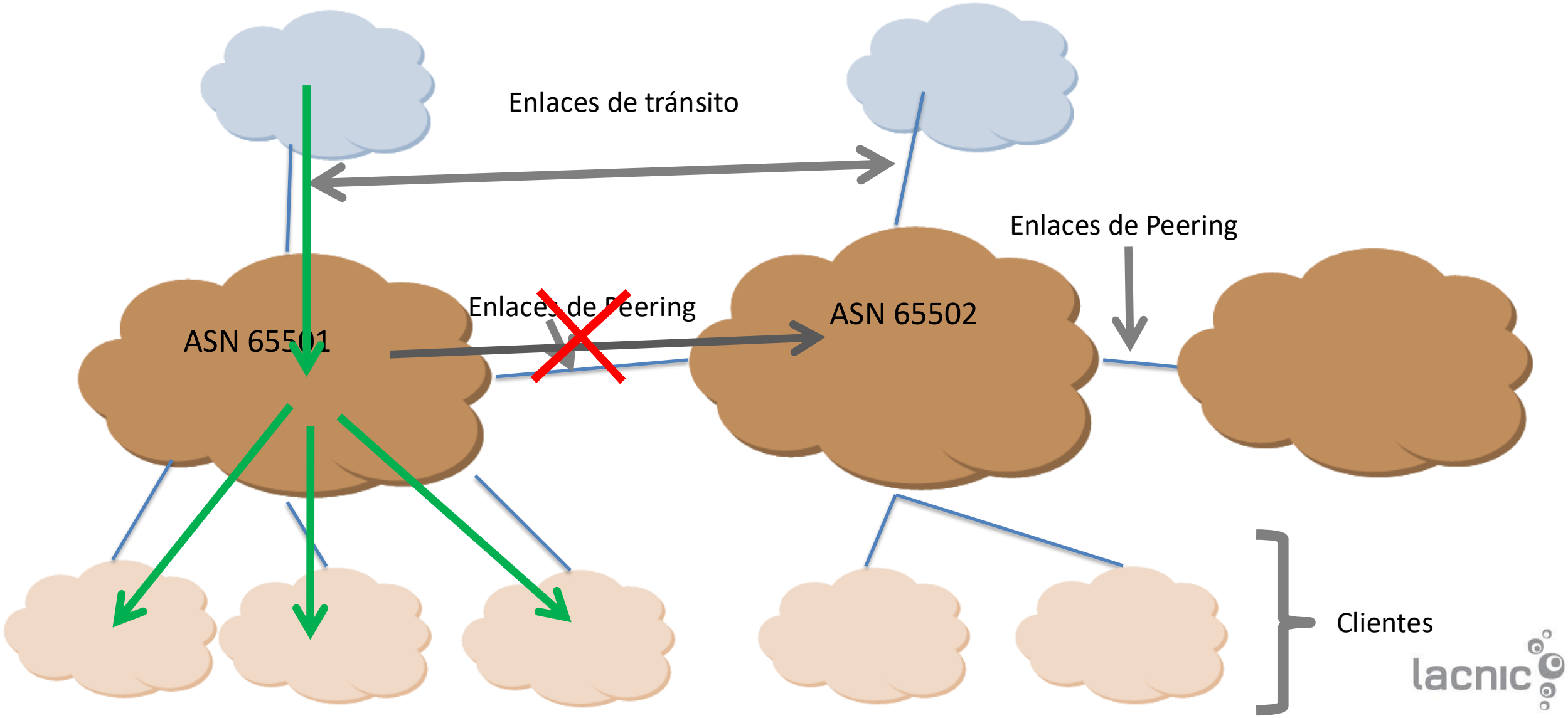
Ejemplos de tipos de fuga de rutas

Fuga lateral de un peer a otro peer



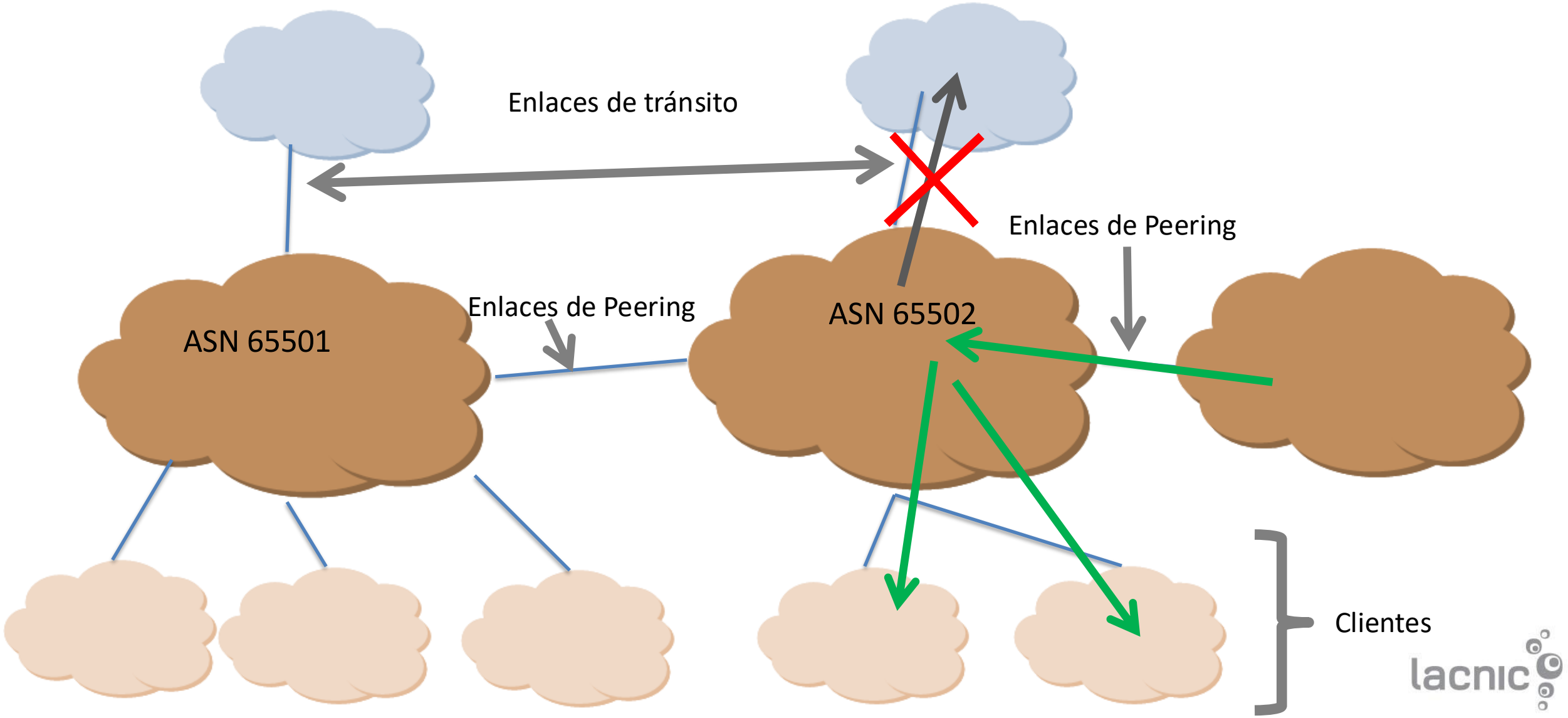
Ejemplos de tipos de fuga de rutas

Fuga de prefijos desde un proveedor de tránsito hacia un peer



Ejemplos de tipos de fuga de rutas

Fuga de prefijos de un peer hacia proveedor de tránsito



Roles en BGP para prevenir route leaks RFC9234

El RFC 9234 es una propuesta de estándar realizada en mayo de 2022.

Describe un método para prevenir y detectar fugas de rutas en el enrutamiento de redes utilizando roles en los mensajes UPDATE y OPEN de BGP.

Roles en BGP para prevenir route leaks RFC9234

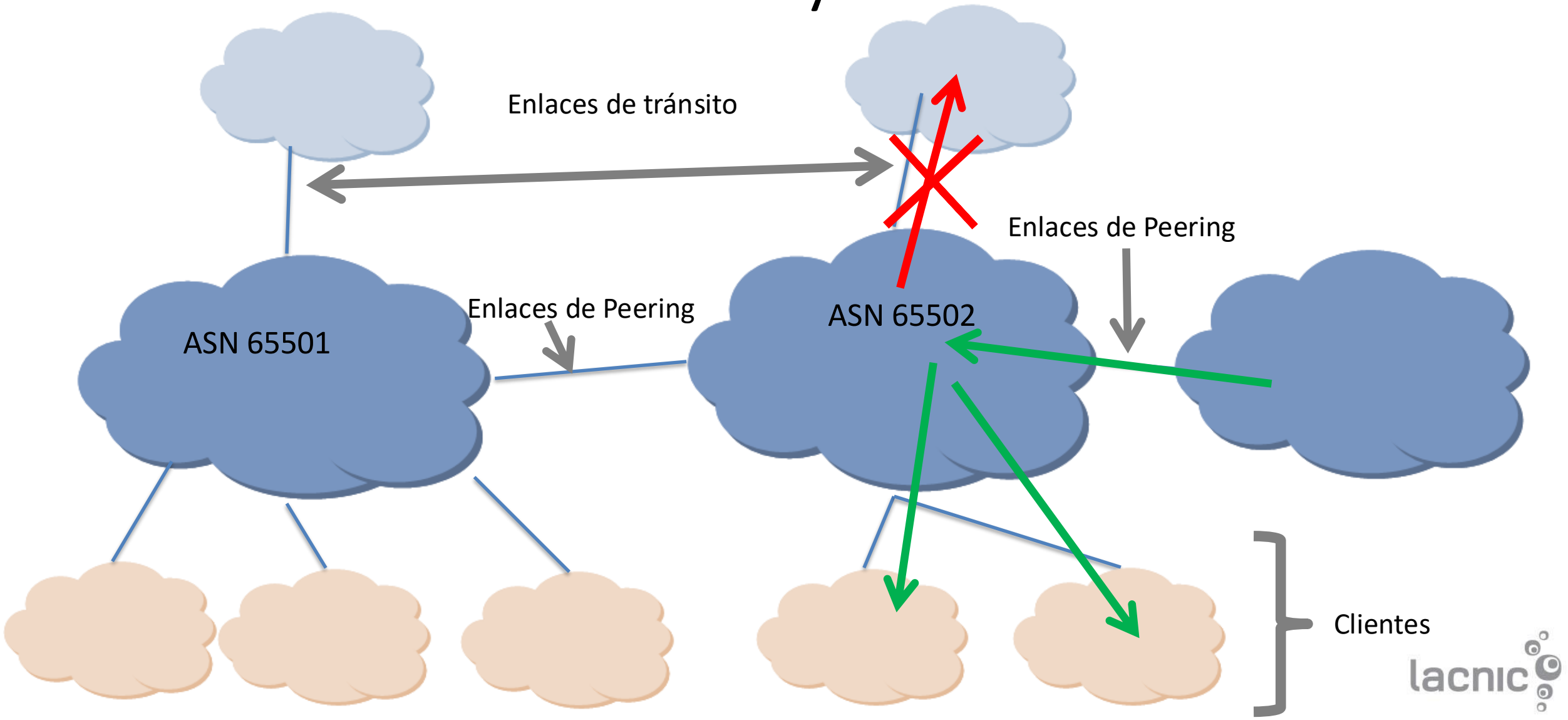
Este método propuesto en el RFC establece roles específicos para los sistemas autónomos (AS) dentro del BGP. Los roles asignados son los siguientes:

- **Proveedor:** El remitente es un proveedor de tránsito para el vecino
- **Cliente:** El remitente es un cliente de tránsito del vecino
- **Route Server:** El remitente es un Route Server usualmente usados en un IXP
- **Route Server-cliente:** Cliente conectado al RS
- **Peer:** El remitente y el vecino son peers

lacnic

Roles en BGP para prevenir route leaks RFC 9234

Atributo nuevo!!! OTC : Only To Customer



Prevención de fugas de rutas en AS locales

- RFC 9234: Atributo Solo a Cliente (OTC-only to customer)
- Se agrega el atributo OTC en la entrada eBGP (si no está ya presente) cuando se recibe una ruta desde un proveedor, un servidor de rutas de un IXP o un peer lateral
- Si el atributo OTC está presente, no se propagará la ruta hacia un proveedor, un servidor de rutas de un IXP o un peer lateral en la salida eBGP
- Si el atributo OTC no está presente, la ruta puede propagarse hacia cualquier tipo de peer en la salida eBGP



Roles en BGP para prevenir route leaks

- https://datatracker.ietf.org/doc/rfc9234/
- Ver video y articulo de Alejandro Acosta:
  - https://www.lacnic.net/innovaportal/file/6405/1/bgp-roles-lacnic-38-alejandro-acosta.pdf
  - https://www.youtube.com/watch?v=w0WDg4TO0ug

4. RPKI: DE LA VALIDACIÓN DE ORIGEN A LA OPERACIÓN

Jerarquía RPKI: 5 Trust Anchors

ARIN | **RIPE NCC** | **APNIC** | **LACNIC** | **AFRINIC**

LIRs / Miembros del RIR (ISPs, Empresas, Universidades)

ISP Grande	**ISP Mediano**	**Empresa**	**CDN/Cloud**	**Universidad**
Cert. de recurso	Cert. de recurso	Cert. de recurso	Cert. de recurso	Cert. de recurso

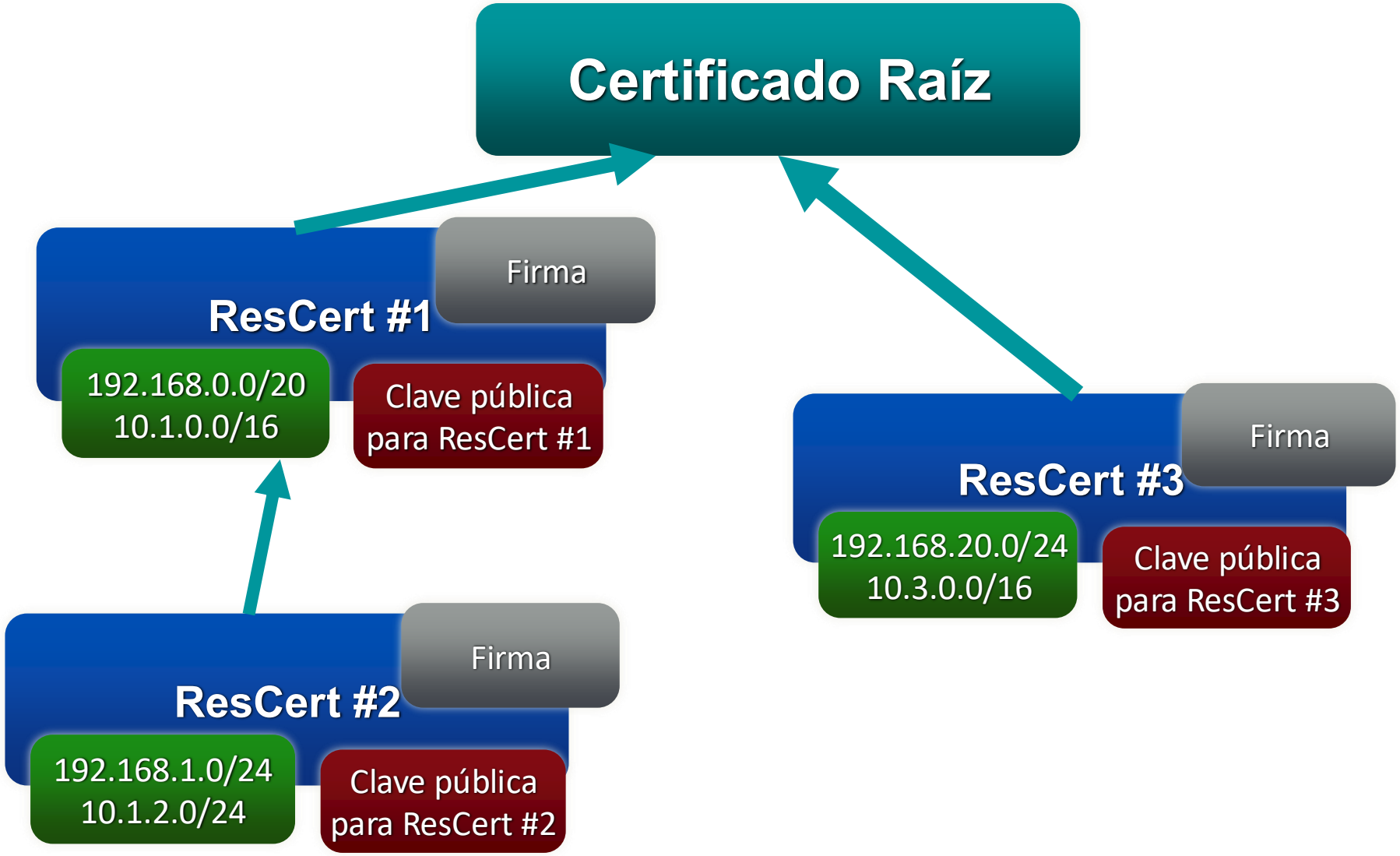
ROA — Route Origin Authorization (hoja del árbol, firmada por el LIR)

ROA: origin=AS64496 **pfx=203.0.113.0/24** **maxLength=24**	**ROA: origin=AS64512** **pfx=198.51.100.0/22** **maxLength=24**	**ROA: origin=AS65000** **pfx=192.0.2.0/24** **maxLength=24**

Cada certificado hereda solo los recursos que su padre tiene asignados — la jerarquía impone el alcance de lo que puede certificarse.

lacnic

PKI de Recursos



¿Qué compone la solución RPKI?

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

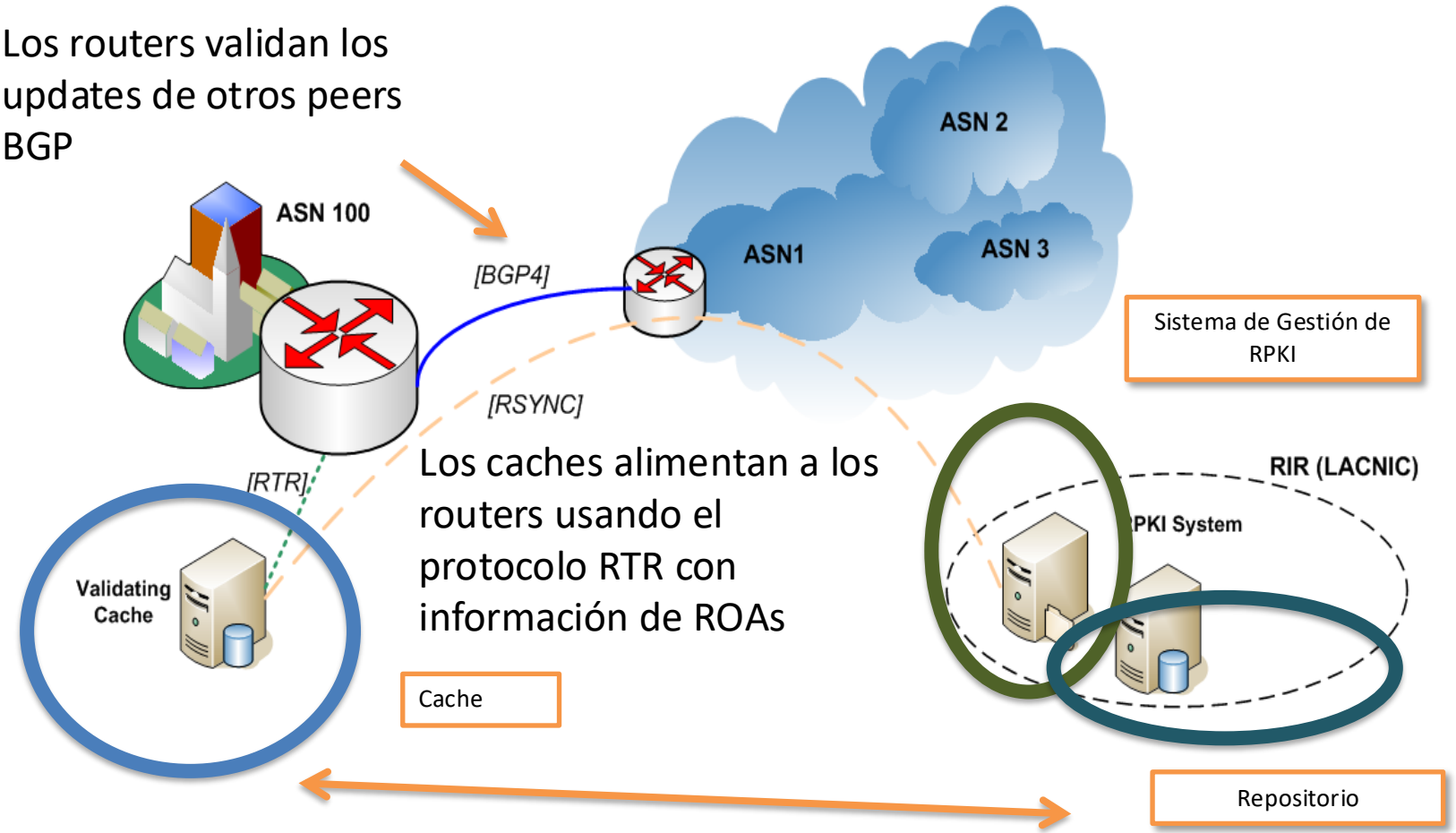
- Un **mecanismo de validación** de prefijos
  - Validación de origen (**ROV** – Route Origin Validation)

lacnic

VALIDACIÓN DE ORIGEN (ROV)

RPKI en acción

Los routers validan los updates de otros peers BGP



Los caches traen y validan criptográficamente los certificados y ROAs de los repositorios

1 **Descarga**

RPKI Validator descarga objetos RPKI de repositorios

2 **Validación**

Valida certificados y ROAs mediante criptografía

3 **Comparación**

Compara anuncios BGP con ROAs validados (VRP)

Validación de Origen – **ROV**

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

Prefix	Length	Max length	Origin-AS
200.0.112.0	22	24	65501
2001:db8:2200::	48	48	65502
…	…	…	…
2001:db8::	32	48	65500

- Con esto es posible asignar un ***estado de validez*** a cada UPDATE de BGP

Válido
El anuncio BGP coincide con un ROA: AS de origen coincide y el anuncio está dentro del Largo Máximo (no es más específico)

Inválido
El anuncio BGP no coincide con ningún ROA válido (prefijo o ASN incorrecto).

Desconocido
No hay información RPKI disponible para el prefijo anunciado.

lacnic

Validación de Origen – **ROV**

Tabla de ROAs

Prefijo (long, max long)	Max Length	ASN
2001:db8:0::/48	48	100
2001:db8:100:/40	48	200
2001:db8::/32	36	300
200.0.113.0/24	24	400
198.51.100.0/22	24	150

BGP
UPDATE 2001:db8::/48
ORIGIN-AS 100

Válido

2001:db8::/48 matchea la 1ra entrada
AS 100 coincide

lacnic

Validación de Origen – **ROV**

Tabla de ROAs

Prefijo (long, max long)	Max Length	ASN
2001:db8:0::/48	48	100
2001:db8:100:/40	48	200
2001:db8::/32	36	300
200.0.113.0/24	24	400
198.51.100.0/22	24	150

BGP
UPDATE 2001:db8:100::/44
ORIGIN-AS 200

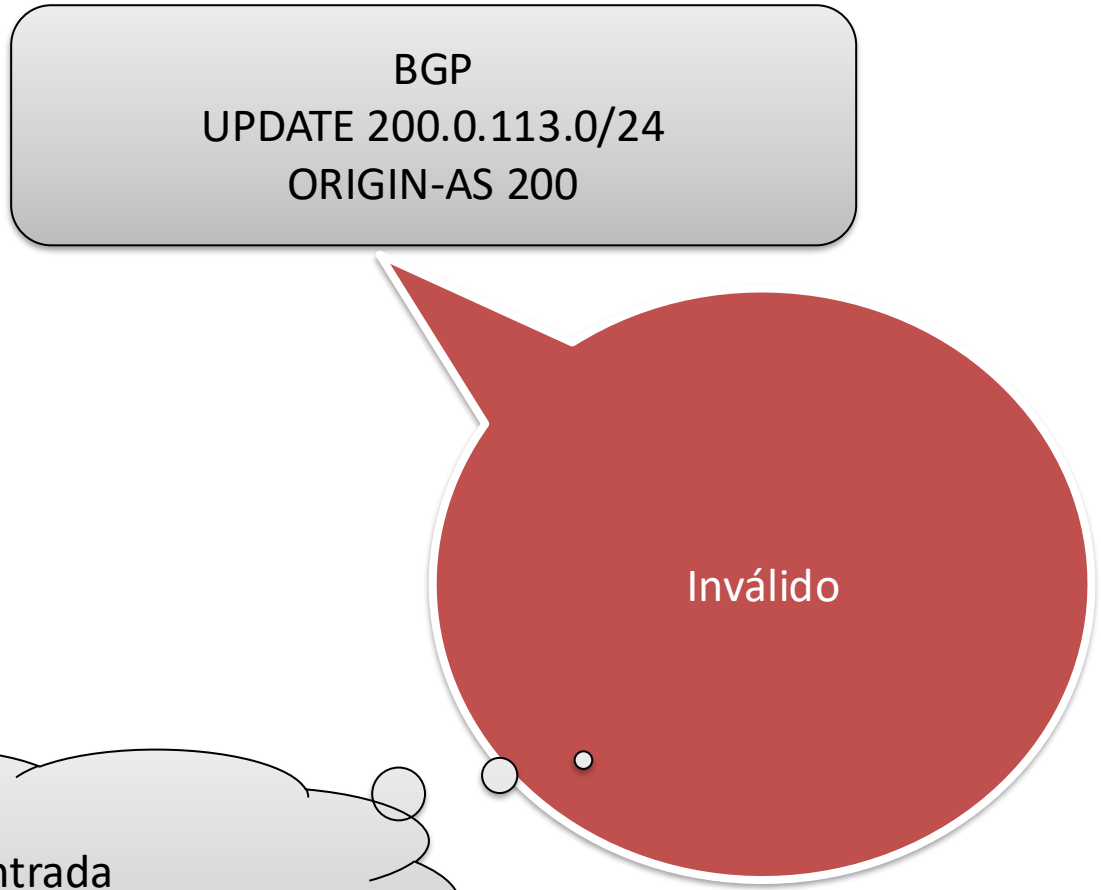
Válido

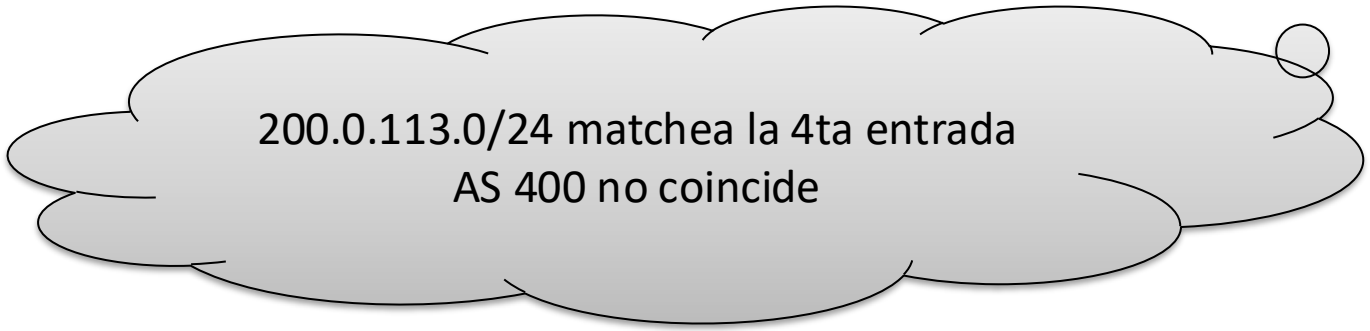
2001:db8:100::/44 matchea la 2da entrada
AS 200 coincide
Max length es menor a 48

Validación de Origen – **ROV**

Tabla de ROAs

Prefijo (long, max long)	Max Length	ASN
2001:db8:0::/48	48	100
2001:db8:100:/40	48	200
2001:db8::/32	36	300
200.0.113.0/24	24	400
198.51.100.0/22	24	150





Validación de Origen – **ROV**

Tabla de ROAs

Prefijo (long, max long)	Max Length	ASN
2001:db8:0::/48	48	100
2001:db8:100:/40	48	200
2001:db8::/32	36	300
200.0.113.0/24	24	400
198.51.100.0/22	24	150

BGP
UPDATE 200.0.115.0/24
ORIGIN-AS 400

Not found

200.0.115.0/24 no matchea con
ninguna entrada
No hay ROA creado

lacnic

Validación de Origen – **ROV**

Tabla de ROAs

Prefijo (long, max long)	Max Length	ASN
2001:db8:0::/48	48	100
2001:db8:100:/40	48	200
2001:db8::/32	36	300
200.0.113.0/24	24	400
198.51.100.0/22	24	150

BGP
UPDATE 2001:db8:abcd::/40
ORIGIN-AS 300

Inválido

2001:db8:abcd::/40 matchea la 3ra entrada
AS 300 coincide
Max length es mayor a 36 (más específico)

lacnic

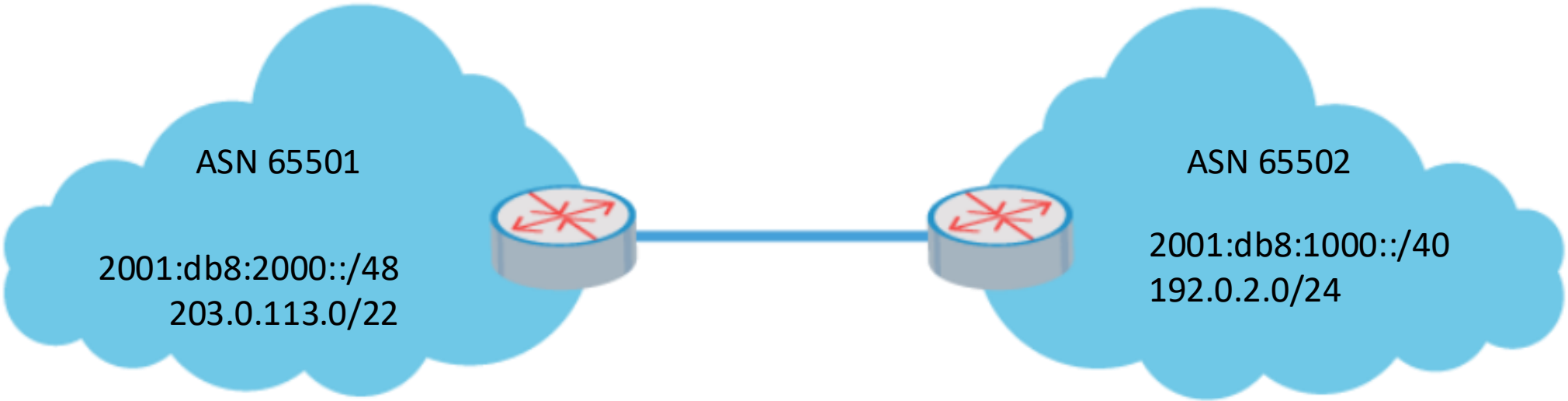
¿Cómo definir los ROA?

- 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
- 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
  - **A partir de Abril de 2023 quienes tienen subasignaciones sí pueden crear ROAs (respondiendo a la política LAC-2020-10)**
- 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 sumarizada?
  - ¿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 y ROAs a crear



ASN 65501
203.0.113.0/22
203.0.113.0/22-24 ???
2001:db8:2000::/48

ASN 65502
192.0.2.0/24
2001:db8:1000::/40
2001:db8:1000::/40-48 ???

lacnic

Implementación Práctica para Operadores de Red

Configurar ROAs	Instalar un Validador RPKI	Configurar Routers	Monitoreo Continuo
• Crear autorizaciones para los prefijos que su organización origina, especificando ASNs autorizados y longitud máxima de prefijo	• Software como: • Routinator (NLnet Labs) • Validador FORT (LACNIC-NIC MX)	• Conectar los routers con el validador RPKI para realizar la validación de origen (ROV) y aplicar políticas de enrutamiento basadas en resultados	• Supervisar el estado de validación de las rutas, los logs del validador y los cambios en la cobertura RPKI de la red. Herramienta muy útil: Packetvis

lacnic

Herramientas útiles

- Mi LACNIC: https://milacnic.lacnic.net

- LACNIC Tools: https://tools.labs.lacnic.net/
  - Información de los repositorios de RPKI, consultas a RDAP, WHOIS y preguntas directas a servidores de nombres
- Monitoreo FORT: https://monitor.fortproject.net/
  - Cobertura de ROAs, validez de los updates BGP, anomalías en la información de ruteo, etc

- RIPE RIS: https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris
- BGP HE.NET https://bgp.he.net

- Cursos de Campus de LACNIC: https://campus.lacnic.net (BGP y RPKI)
- Documentación RPKI: https://rpki.readthedocs.io/en/latest/

lacnic

Repaso de lo visto hasta ahora

- Route leaks y Roles en BGP / Atributo OTC
- Validación de origen
  - Repositorios, ROAs, caches
  - Implementación en la práctica
- Qué información tener en cuenta para crear los ROA
- Pasos para desplegar RPKI
- Herramientas



lacnic

lacnic 46
lacnog 2026
19 - 22 OCTUBRE / MENDOZA, ARGENTINA

Kahoot de la mañana

MODULO 5: MAS ALLÁ DE LA VALIDACIÓN DE ORIGEN: ASPA

Limitaciones de ROV (Route Origin Validation)

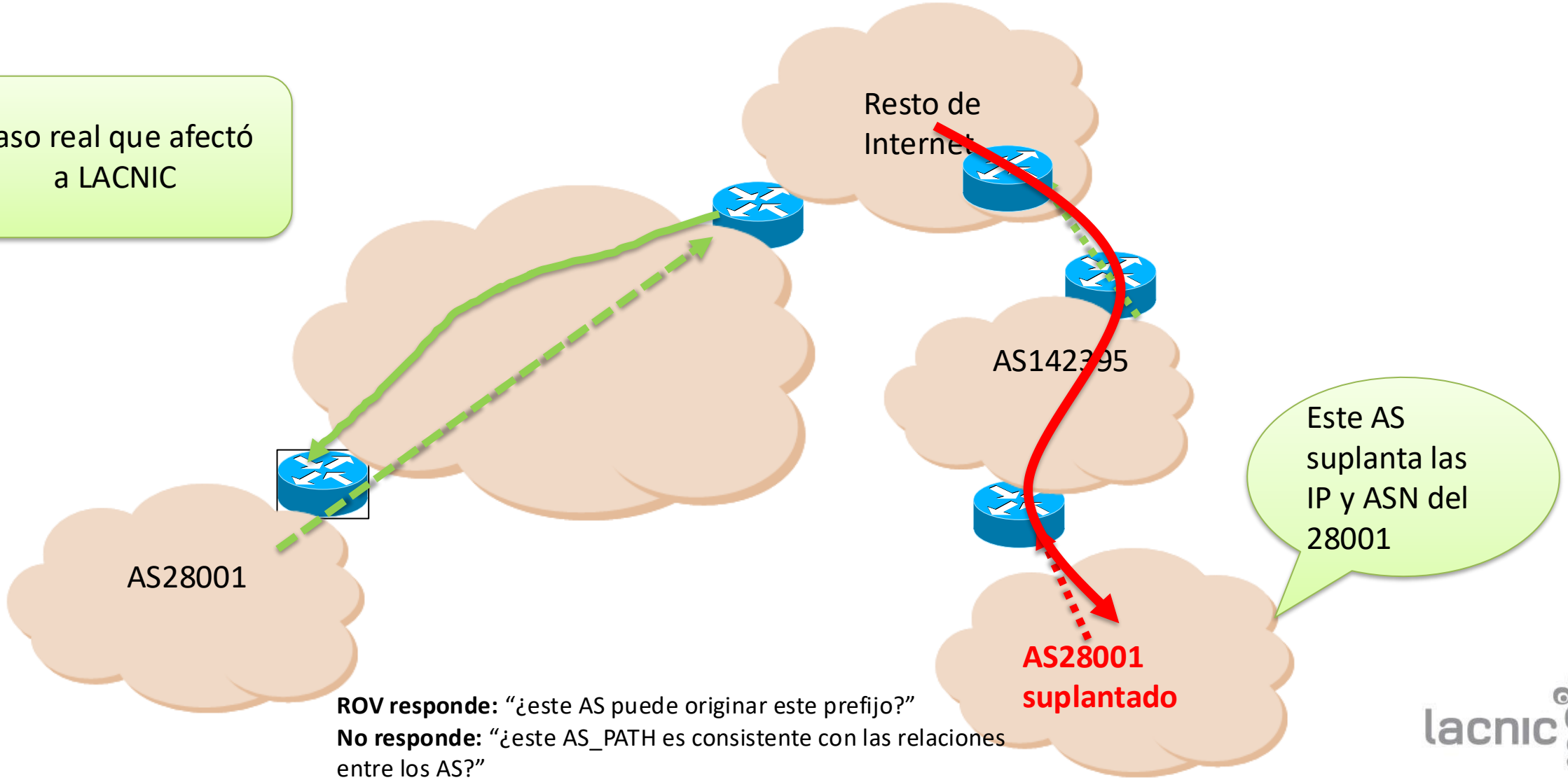
¡CUANDO TENIAMOS TODAS LAS RESPUESTAS NOS CAMBIARON LAS PREGUNTAS!

¿Cuál es el problema a resolver?

- ROV protege el origen, pero… ¿qué pasa con el AS_PATH?
- Necesitamos mecanismos para validar todo el camino de los anuncios BGP, no sólo el origen
  - Leaks: generalmente el ASN de origen se preserva, ROV no los evita
  - Es posible agregar el ASN de origen correcto en un AS-PATH falsificado
- En la IETF se propuso BGPSec como solución, pero no ha tenido mucha aceptación por parte de los operadores

Secuestro de rutas: suplantación de AS de origen

Caso real que afectó a LACNIC

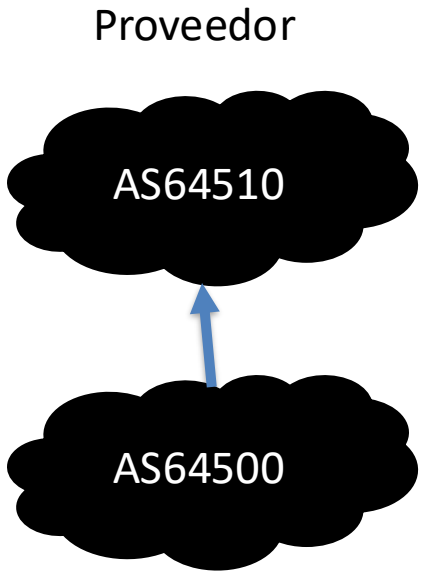


ROV responde: "¿este AS puede originar este prefijo?"
No responde: "¿este AS_PATH es consistente con las relaciones entre los AS?"

¿Qué es ASPA?
Autonomous System Provider Authorization

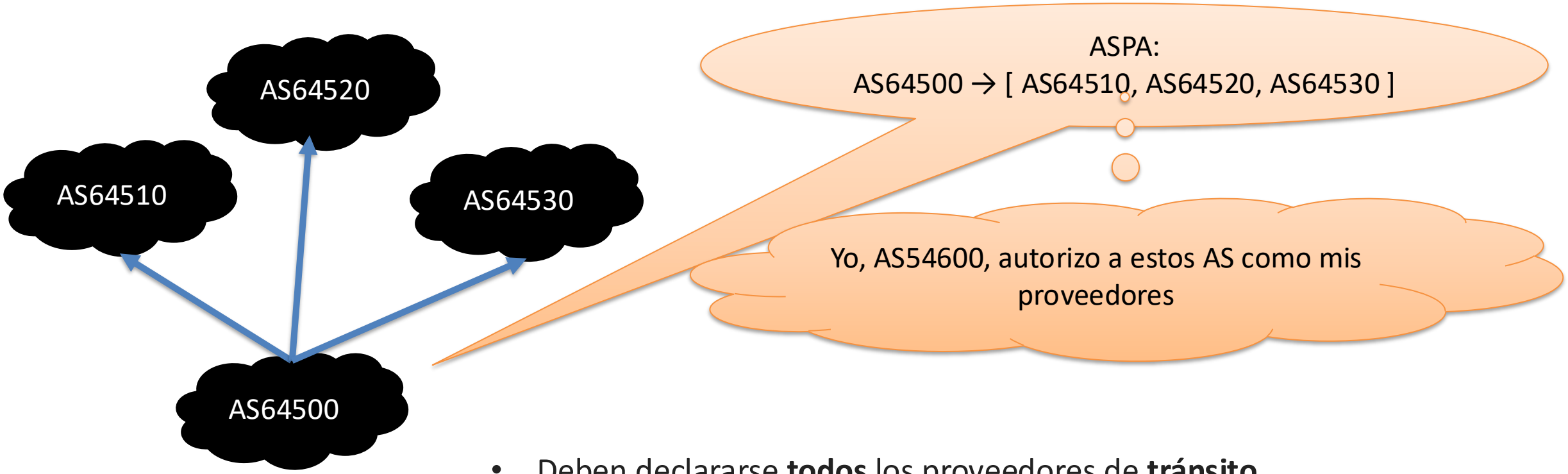
- Un nuevo objeto firmado dentro de RPKI mediante el cual un AS declara cuáles AS están autorizados a actuar como sus proveedores de tránsito
  - El **cliente autoriza a sus proveedores**
  - La información se publica y distribuye utilizando la infraestructura RPKI
  - Los validadores pueden usar esas autorizaciones para verificar propiedades del **AS_PATH**

draft-ietf-sidrops-aspa-profile
draft-ietf-sidrops-aspa-verification



ASPA de AS64500:
AS64500 → AS64510

El objeto ASPA visto por un operador



- Deben declararse **todos** los proveedores de **tránsito**.
- La misma lista se utiliza para IPv4 e IPv6.
- Si el AS no tiene proveedores de tránsito puede publicar **AS0 ASPA**.

¿Cómo se usa ASPA para validar un camino?

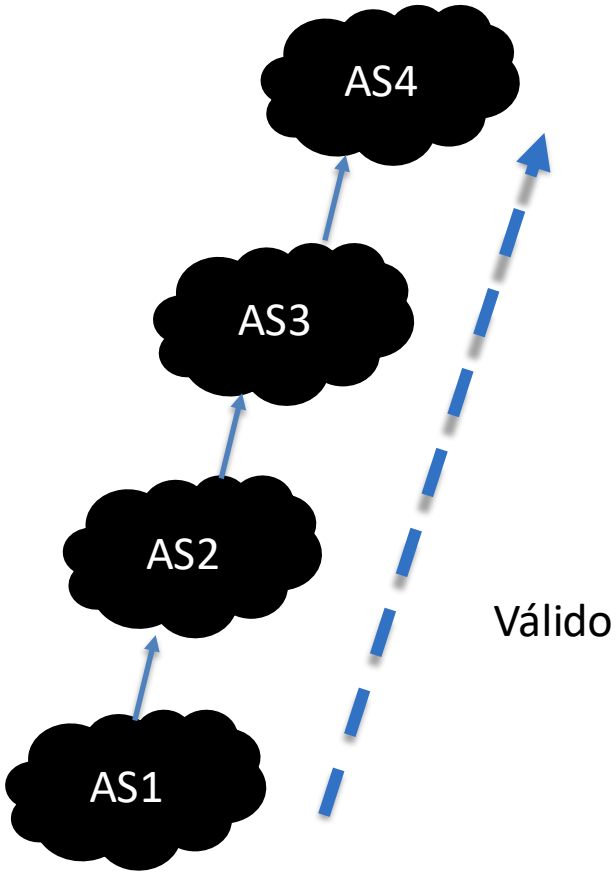
- ASPA publicados:

```
AS1 => AS2
AS2 => AS3
AS3 => AS4
```

- Camino recibido por AS4:

```
AS-PATH: AS3 AS2 AS1
```

- ASPA Valid: las relaciones necesarias para explicar el camino están autorizadas



¿Cómo se usa ASPA para validar un camino?

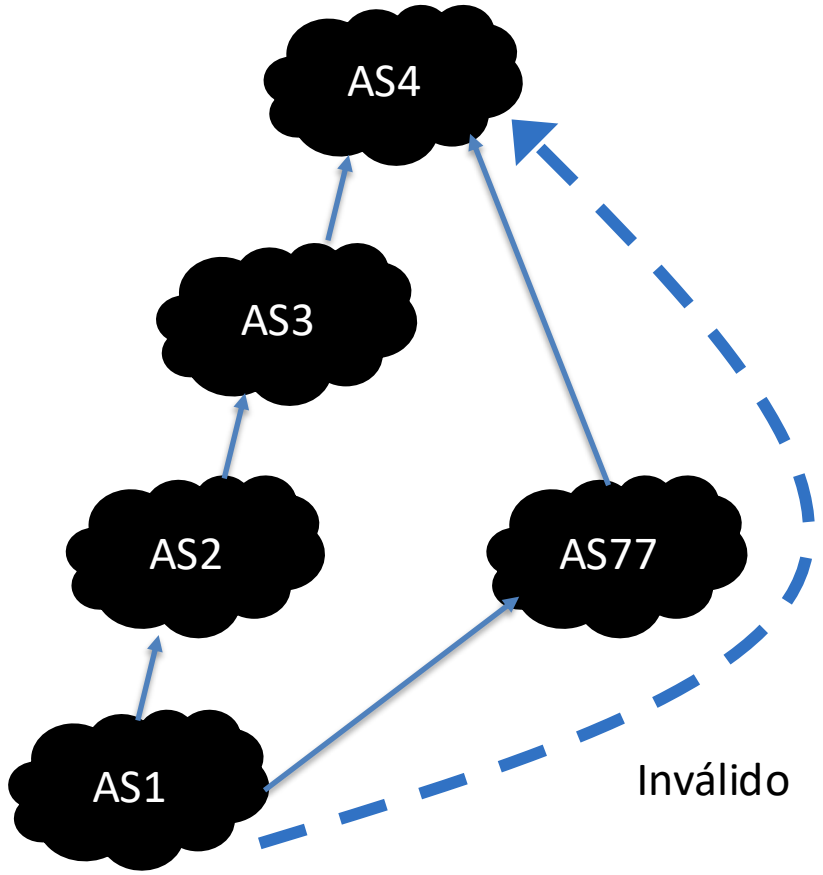
- ASPA publicados:

```
AS1 => AS2
AS2 => AS3
AS3 => AS4
```

- Camino recibido por AS4:

```
AS-PATH: AS77 AS1
```

- ASPA **Invalid**: AS77 no está autorizado como proveedor por AS1
- El origen puede seguir siendo ROV Valid
  - ASPA agrega información para evaluar el camino.



¿Cómo se usa ASPA para validar un camino?

- El router toma el AS_PATH y lo contrasta con las autorizaciones ASPA disponibles
- Como en ROV tenemos 3 estados de validación: Valid, Invalid y Unknown
- Si falta información ASPA → el resultado puede ser Unknown; no significa Invalid

Beneficios de ASPA

- Detecta AS_PATHs falsificados (*forged-origin hijacks*)
- Mitiga la propagación global de route leaks
- Reuso Operativo: Aprovecha la arquitectura RPKI existente (validadores, repositorios y protocolo rpki-rtr)
- No agrega complejidad en los routers (criptografía por ejemplo)

6. MITIGACIÓN Y RESPUESTA ANTE ATAQUES

Validar no basta

- **RPKI, IRR y filtros:** previenen anuncios falsos
- **DDoS volumétrico:** tráfico legítimo en forma, malicioso en volumen
- **Sin firma que lo detenga:** se responde con ruteo
- **Tres herramientas:** RTBH, comunidad BLACKHOLE y Flowspec

Caja de herramientas de respuesta

RTBH

Descarte del tráfico al destino atacado, dentro de mi red

RFC 5635

Comunidad BLACKHOLE

Pedir al upstream o al IXP que descarte antes de mi enlace

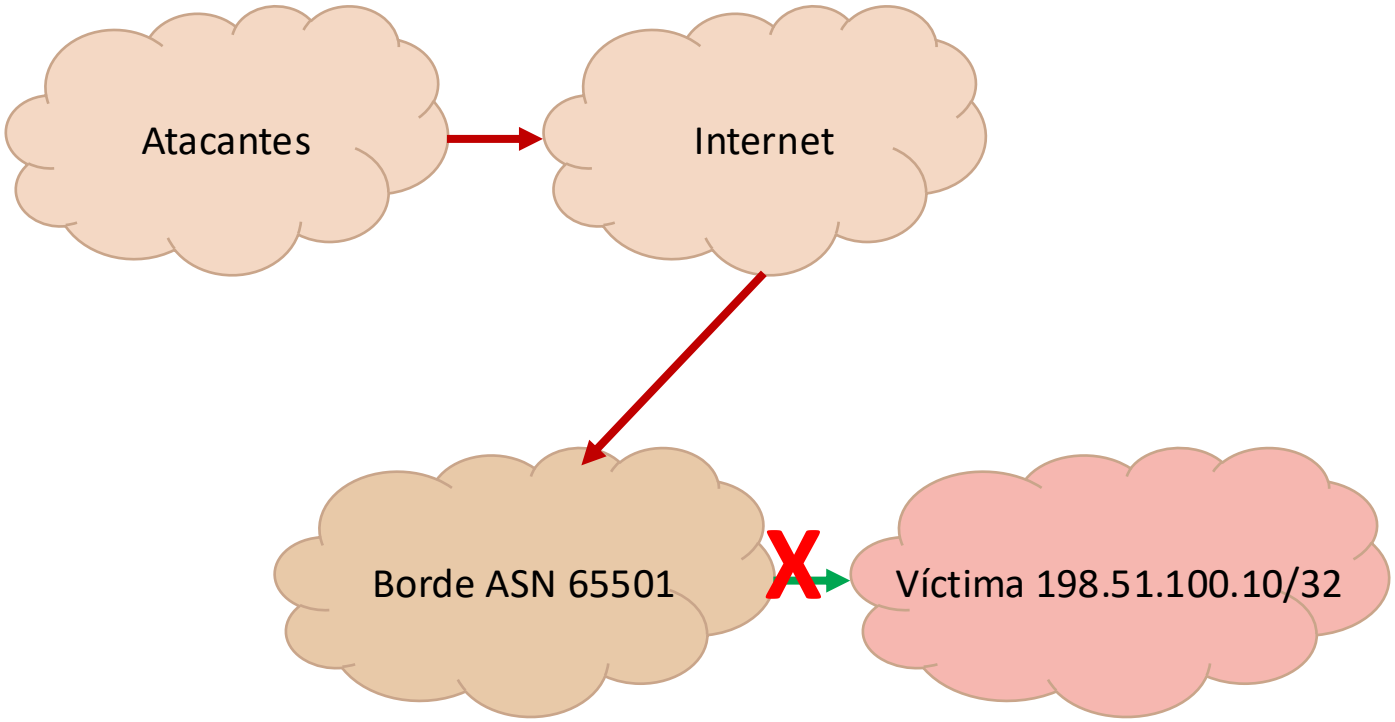
RFC 7999

BGP Flowspec

Filtrar, limitar, o redireccionar por protocolo, puerto y origen

RFC 8955 / 8956

Black hole: la idea básica



- **Se anuncia** solo la IP atacada (/32 o /128)
- **Next-hop** a un destino de descarte (Null0)
- **Costo:** esa IP queda inalcanzable
- **Beneficio:** el resto de la red sigue vivo

RTBH: cómo funciona

1. Preparar: ruta estática de descarte en todos los bordes

2. Disparar: el router trigger anuncia la IP víctima por iBGP

3. Descartar: los bordes resuelven el next-hop recursivamente hacia Null0

Ejemplo ilustrativo (estilo Cisco)

```
! 1) En TODOS los routers de borde
ip route 192.0.2.1 255.255.255.255 Null0

! 2) En el router trigger
ip route 198.51.100.10 255.255.255.255 Null0 tag 66
route-map RTBH-TRIGGER permit 10
 match tag 66
 set ip next-hop 192.0.2.1
 set community no-export
router bgp 65001
 redistribute static route-map RTBH-TRIGGER
```

RTBH por destino vs. por origen

Por destino (D/RTBH)	Por origen (S/RTBH)
• Descarta todo lo que va a la IP víctima	• Descarta tráfico desde los orígenes del ataque
• Simple y muy usado	• Requiere uRPF en modo loose
✗ La víctima queda inalcanzable	✓ La víctima sigue alcanzable
▲ El ataque "gana" para esa IP	▲ Los orígenes spoofed lo complican

No acepte S/RTBH de peers ni de clientes

Comunidad BLACKHOLE (RFC 7999)

- **Valor:** 65535:666 (well-known, 0xFFFF029A)
- **Qué hace:** pide al upstream o al IXP que descarte el prefijo
- **Longitud:** típicamente /32 IPv4 o /128 IPv6
- **Alcance:** agregar NO_EXPORT o NO_ADVERTISE
- **El proveedor verifica:** que el cliente está autorizado a anunciar ese prefijo

Pregunte hoy a su upstream si lo soporta y con qué longitud máxima

La trampa del /32 y los ROAs

- **Problema:** un /32 de blackhole no está cubierto por un ROA con maxLength /24, así que ROV lo marca inválido
- **Tentación:** ampliar maxLength a /32 "por si acaso”

✗ **No lo haga:** RFC 9319 desaconseja ROAs no mínimos para anunciar rutas de blackhole (RTDR)

✓ **Mejor:** el proveedor no debe exigir ROAs no mínimos para aceptar blackholes

▲ **Scrubbing:** RFC 9319 § 5.1 admite excepciones acotadas para servicios de mitigación DDoS

BGP Flowspec: filtrado granular

- **Qué es:** reglas de filtrado distribuidas por BGP
- **Dónde:** IPv4 (RFC 8955) e IPv6 (RFC 8956)
- **Cómo:** match en el NLRI y acción en una extended community

Match (NLRI)	Acción
Destino / origen	Descartar
Protocolo, puertos	Limitar
Flags TCP, largo de paquete	Redirigir
DSCP, fragmentos	Marcar DSCP

Flowspec: ejemplo de regla

Ejemplo ilustrativo (sintaxis ExaBGP): bloquear amplificación DNS hacia la víctima

```
flow {
  route block-dns-amp {
    match {
      destination 198.51.100.10/32;
      protocol udp;
      source-port=53;
    }
    then {
      rate-limit 0;
    }
  }
}
```

- **Ventaja:** el resto del tráfico hacia la IP sigue pasando
- **Validación:** RFC 8955 (revisada en RFC 9117) exige que el originador de la regla coincida con el de la ruta unicast

RTBH, BLACKHOLE o Flowspec

	RTBH	BLACKHOLE	Flowspec
Granularidad	Toda la IP	Toda la IP	Protocolo, puerto, origen
Daño colateral	Alto (IP caída)	Alto (IP caída)	Bajo
Dónde actúa	Mi red	Upstream o IXP	Mi red o upstream
Requisito	Preparar bordes	Soporte del upstream	Soporte en routers y acuerdo
Cuándo	Último recurso	Enlace saturado	Ataque identificable

Buenas prácticas antes del ataque

Preparar	Autorizar	Limitar	Probar
• Plan por escrito • Contactos NOC de upstreams • Next-hop de descarte listo	• Triggers solo de prefijos propios • Sin S/RTBH de peers o clientes	• max-prefix en sesiones con triggers • NO_EXPORT en blackholes • Retirar reglas al terminar	• Ejercicio periódico • Verificar que el upstream responde • Medir tiempo de reacción

¿Preguntas?

- ¿Mi upstream acepta 65535:666?
- ¿Quién puede disparar un blackhole en mi red?
- ¿Cuánto tarda mi NOC en reaccionar?



7. ¿QUÉ HAGO MAÑANA EN MI RED?

Hoy: lo que ya podemos desplegar

1. ROAs correctos	2. IRR actualizado	3. Filtros
ROAs mínimos, maxLength ajustado *Bloque 4*	Objetos route/route6 y AS-SET al día *Bloque 2*	Bogons, prefijos y AS-path; bgpq4 *Bloque 2*

4. ROV	5. BGP Roles / OTC	6. Respuesta DDoS
Validador + RTR; descartar inválidos *Bloque 4*	Roles en sesiones eBGP; atributo OTC *Bloque 3*	RTBH, BLACKHOLE y Flowspec listos *Bloque 6*

Lo que viene

ASPA

Validación de path y detección de leaks

Aún en discusión en el IETF

Validadores y routers al día

Parches y versiones con soporte RTRv2

Un validador sin parchear es un riesgo

Seguir SIDROPS / GROW

Los estándares aún se mueven

Ahí se publica lo siguiente

Hoy: planificar ASPA, no desplegarlo en producción

Cómo seguir

- **SIDROPS:** https://datatracker.ietf.org/wg/sidrops/
- **GROW:** https://datatracker.ietf.org/wg/grow/
- **MANRS:** https://manrs.org
- **MANRS Observatory:** https://observatory.manrs.org
- **LACNIC Campus (cursos de BGP y RPKI):** https://campus.lacnic.net
- **Documentación RPKI:** https://rpki.readthedocs.io/en/latest/

lacnic 46
lacnog 2026
19 - 22 OCTUBRE / MENDOZA, ARGENTINA

Kahoot del mediodía

¡MUCHAS GRACIAS!

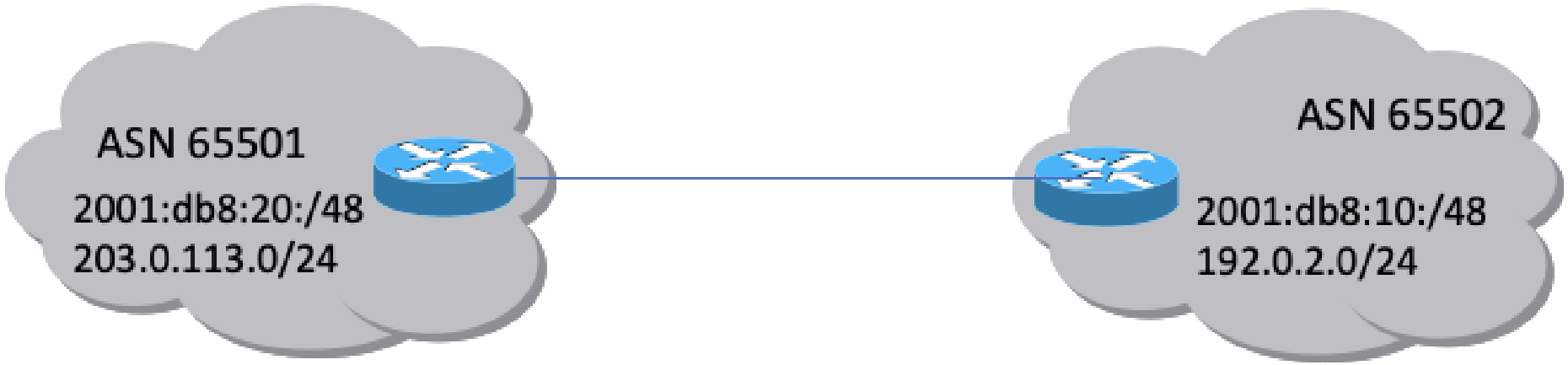
¿Preguntas?



MATERIAL EXTRA

IRR: 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

lacnic

Peering con otros ASN

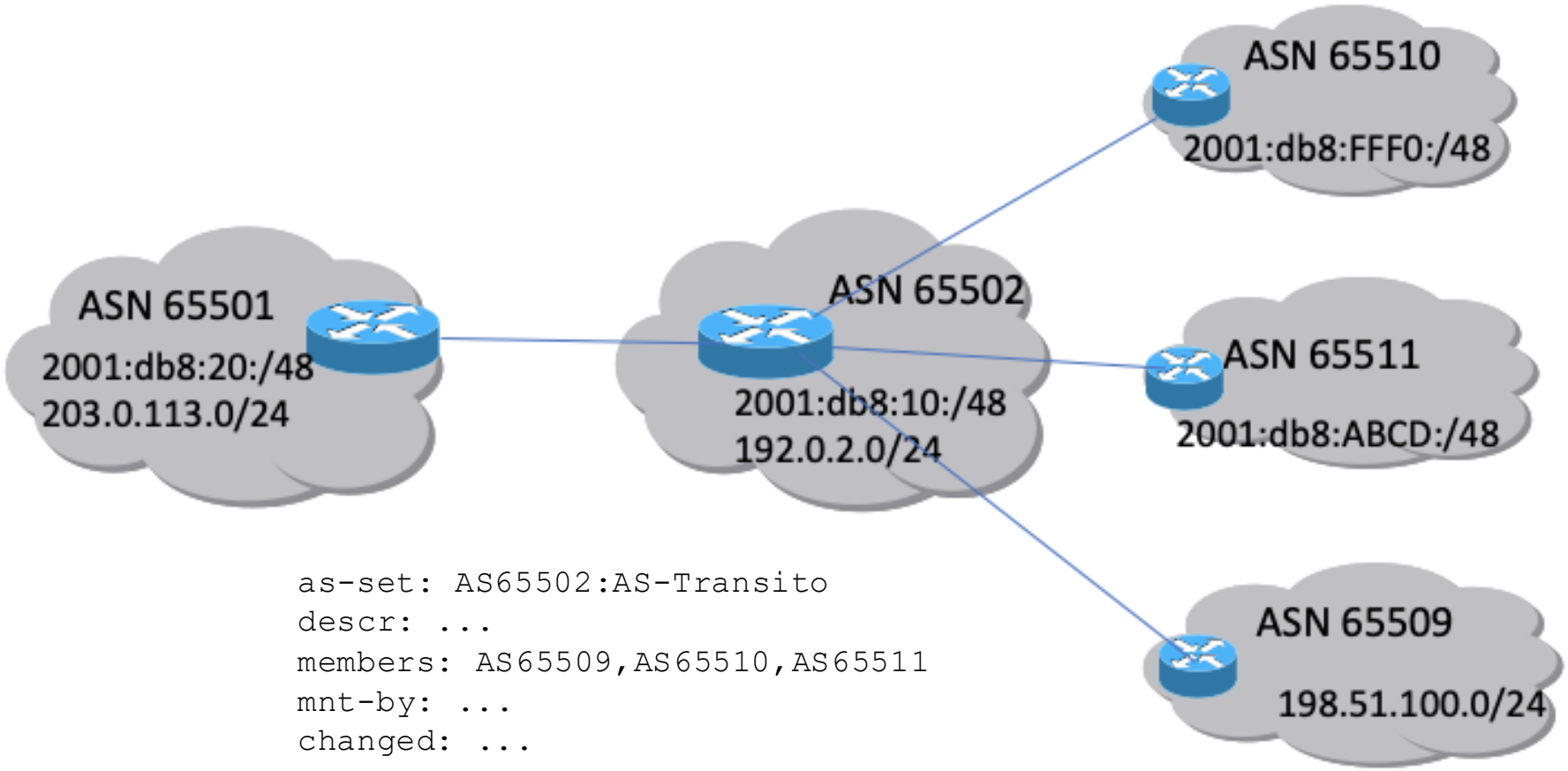
- Muchos proveedores de contenido (CDN) solicitan definir un AS-SET en un IRR conteniendo los sistemas autónomos a los que darán tránsito (conectividad con la CDN).
- Lo mismo sucede con proveedores de cloud o servicios VPS.

Peering con otros ASN

- ¿Qué es un AS-SET?
  - Un AS-SET es objeto en un IRR que define un conjunto de AS (sistemas autónomos)
  - Su uso puede ser muy variado y no tiene una semántica predefinida
  - Uno de los usos más comunes de los AS-SET es definir un conjunto de sistemas autónomos que comparten una política determinada, por ejemplo, ser anunciados a través de un peering o un enlace de tránsito.

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

Ejemplo de tránsito




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

Peering con otros ASN

- Cómo usar un AS-SET para los peerings con otras organizaciones
  - Podemos definir un AS-SET indicando cuáles son los ASN que queremos anunciar a un determinado peer
  - Ese AS-SET se lo informaremos de alguna manera al operador remoto.
  - En el caso de muchos proveedores de contenido, lo que es habitual es que tomen esa información del registro de PeeringDB:

```
$ whois -h whois.peeringdb.net as65200
...
IRR AS-SET              : AS65200:AS-Transito
...
```

Ver: https://www.labs.lacnic.net/Peering-IRR/

lacnic

Referencias

- IRR de LACNIC: https://query.milacnic.lacnic.net/irr
- Peering, IRR y AS-SET: https://blog.lacnic.net/enrutamiento/irr-y-su-utilidad-al-hacer-peering
- Bgpq4: https://github.com/bgp/bgpq4
- IRRd v4 Documentación de queries (flags): https://irrd.readthedocs.io/en/stable/users/queries/whois/

- Documentación Mi LACNIC:
  - General: https://lacnic.zendesk.com/hc/es
  - RPKI: https://lacnic.zendesk.com/hc/es/sections/206490008-RPKI
  - IRR: https://lacnic.zendesk.com/hc/es/sections/1464569752859 9-Internet-Routing-Registry-IRR