Recomendaciones operativas para RPKI

Arturo Servín

Carlos Martinez Cagnazzo

Recomendación no operativa

Personas		
Organizaciones		
Contactos		

las pilas

+1

Recomendación operativa

Identificaci
ó de
R

Consultas
s

$: whois –h whois.lacnic.net 200.7.84.0

.

.

admin-c: AIL

.

tech-c: SER

.

.

Crear Certificado

Crear Roas

+2

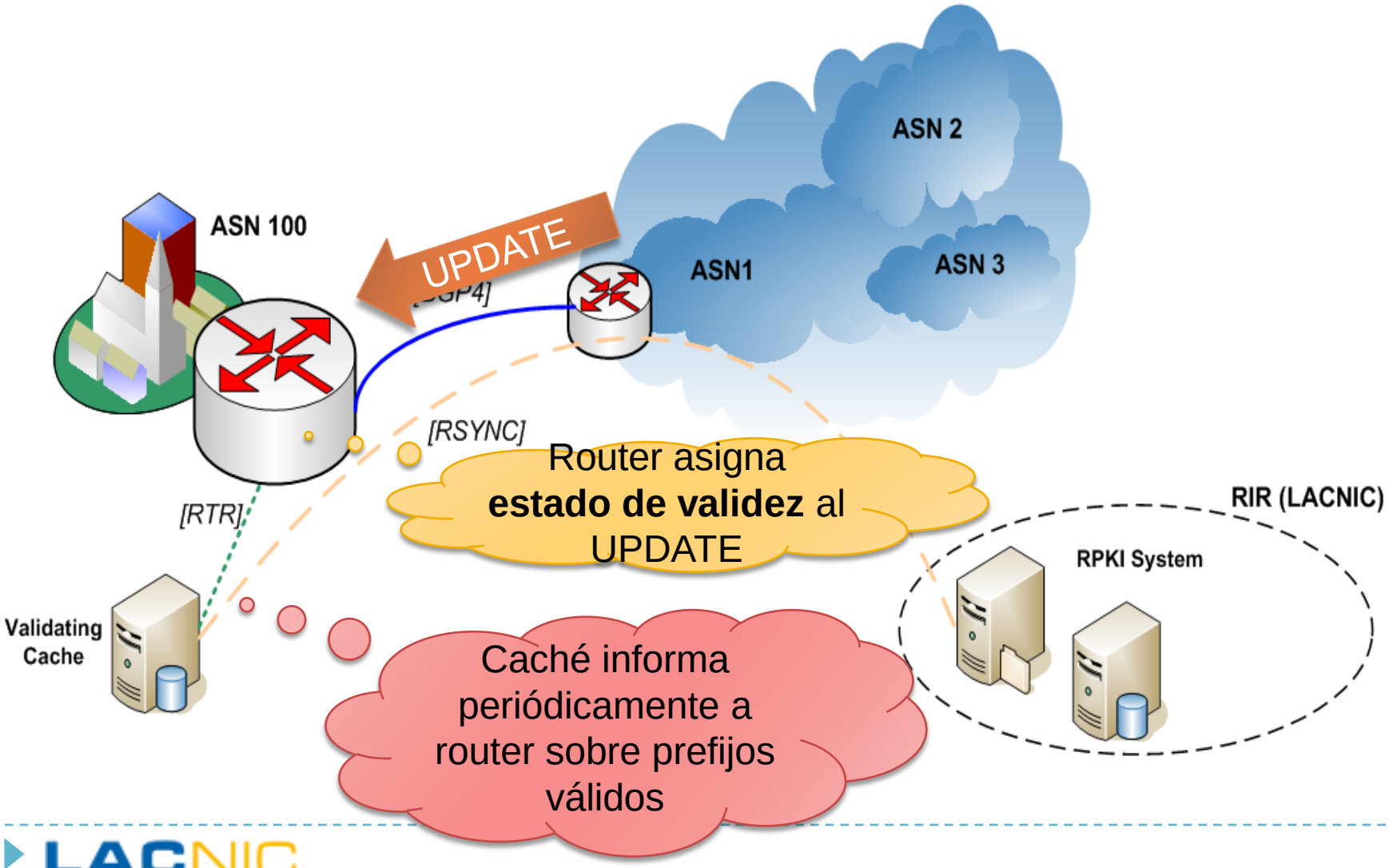
Glosario

- Certificados de recursos:
  - Certificados digitales X.509 v3 con extensiones RFC 3779 que listan recursos de numeración (prefijos v4, v6 y números de sistema autónomo)
    - Cada asociado a LACNIC que asi lo desee puede obtener su certificado de recursos
- RTA (*Resource Trust Anchor*)
  - Certificado de recursos que esta en la cúspide de la jerarquía y lista todos los recursos de numeración de quien lo emite (LACNIC en nuestro caso)
    - El RTA firma el certificado de producción, el que a su vez firma los certificados de recursos de los asociados
- Certificado de producción
  - Certificado de recursos que hereda sus recursos del RTA y es el que se usa para las operaciones del día a día

Glosario (II)

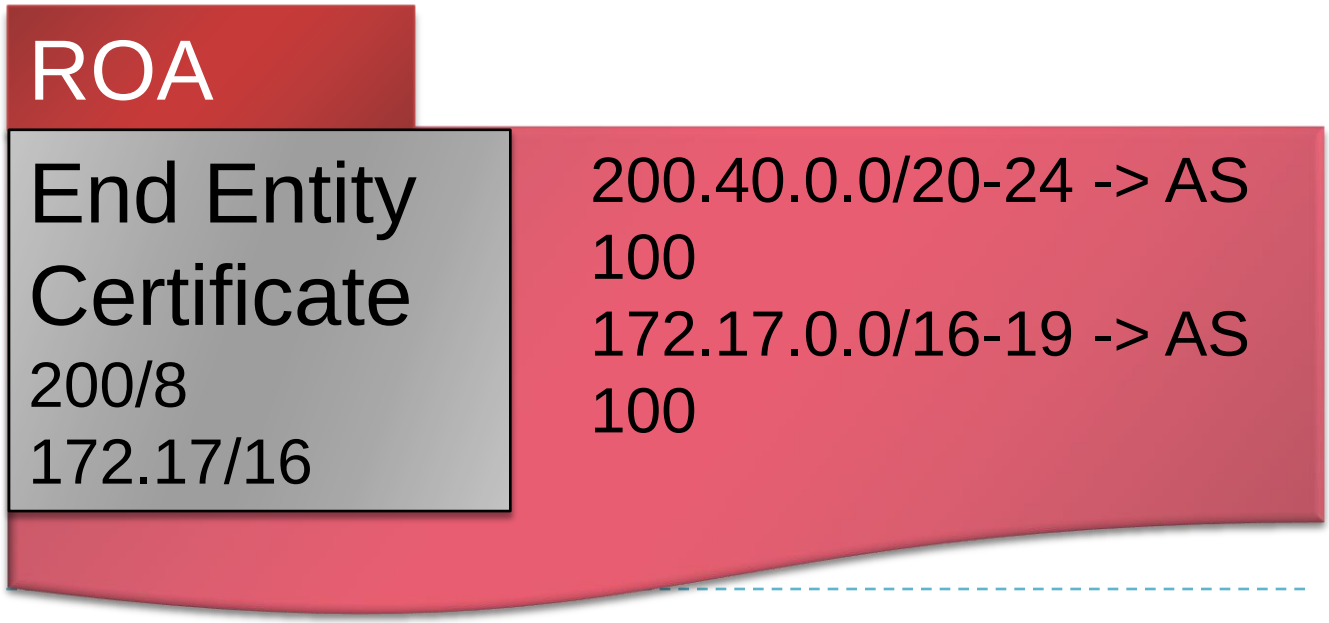
- Repositorio:
  - Punto de publicación de todo el material de la RPKI, accesible vía RSYNC
- ROA (*Route Origin Authorization)*
  - Objeto que contiene afirmaciones firmadas sobre el origen de rutas
- Manifiestos, CRLs
  - Otros objetos del repositorio utilizados para verificar la integridad del repositorio y el estado de revocación del mismo

RPKI en una diapositiva



ROAs

- Los ROAs nos permiten expresar **afirmaciones de origen de rutas**
- Los ROA contienen
  - Un certificado End Entity con recursos
  - Una lista de “route origin attestations”



ROAs y su interacción con BGP (i)

UPDATE
200.0.0.0/9
ORIGIN-AS 66

INVALID

max_len]	AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el “UPDATE pfx” **no** encuentra ninguna entrada que lo cubra en la BdeD -> “**not found**”
- Si el “UPDATE pfx” si encuentra al menos una entrada que lo cubra en la BdeD y además el AS de origen del “UPDATE pfx” coincide con uno de ellos -> “**valid**”
- En el caso anterior, si **no** coincide ningun AS de origen -> “**invalid**”

ROAs y su interacción con BGP (ii)

UPDATE 200.0.0.0/9 ORIGIN-AS 20

VALID

max_len]	Origin AS
172.16.0.0 / [16-20]	10
200.0.0.0/[8-21]	20

- Si el “UPDATE pfx” **no** encuentra ninguna entrada que lo cubra en la BdeD -> “**not found**”
- Si el “UPDATE pfx” si encuentra al menos una entrada que lo cubra en la BdeD y además el AS de origen del “UPDATE pfx” coincide con uno de ellos -> “**valid**”
- En el caso anterior, si **no** coincide ningun AS de origen -> “**invalid**”

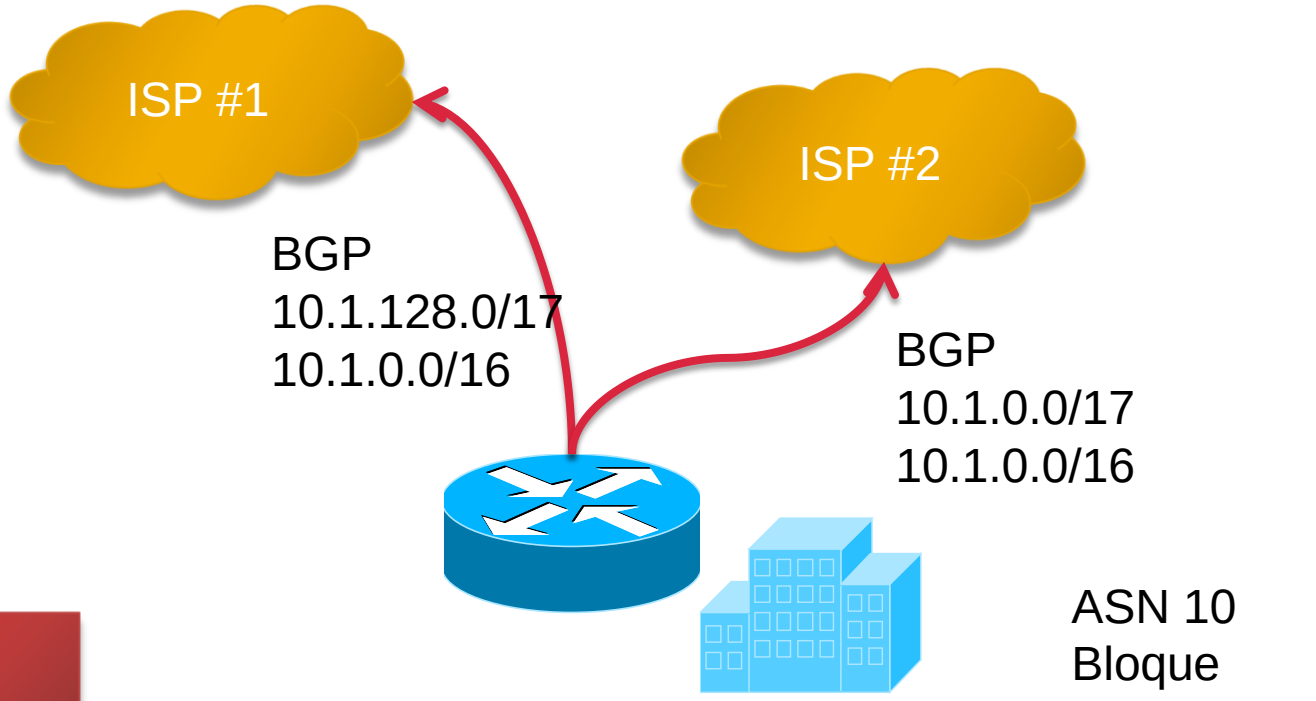
Gestión de ROAs

- Los ROAs expresan nuestras políticas de enrutamiento en cuanto al AS de origen
- Los ROAs deben ser **correctos**
  - Un ROA asocia un prefijo a un sistema autónomo que va a ser su sistema autónomo de origen
  - Cuando creamos el ROA el AS de origen tiene que ser el **correcto**
    - De lo contrario corremos el riesgo de hacernos una DoS a nosotros mismos ☺
  - Las organizaciones **que tienen mas de un AS** tienen que ser **particularmente cuidadosas**

Gestión de ROAs (ii)

- Los ROAs deben apoyar la implementación eficiente de la validación de origen
- Por cada mensaje de UPDATE que un router recibe debe hacer un lookup en una tabla
  - Esta búsqueda debe ser lo mas eficiente posible
- [SIDROPS] recomienda entonces:
  - No abusar del campo “maximum length” de los ROAs
    - Es decir, en el caso de IPv4, no hacer siempre los ROAs hasta /32
    - O en el caso de IPv6, no hacerlos siempre hasta /128
  - Los ROAs se deberían alinear lo mas posible con los anuncios BGP que hace un sistema autónomo

Ejemplo de ROA #1 (Correcto)

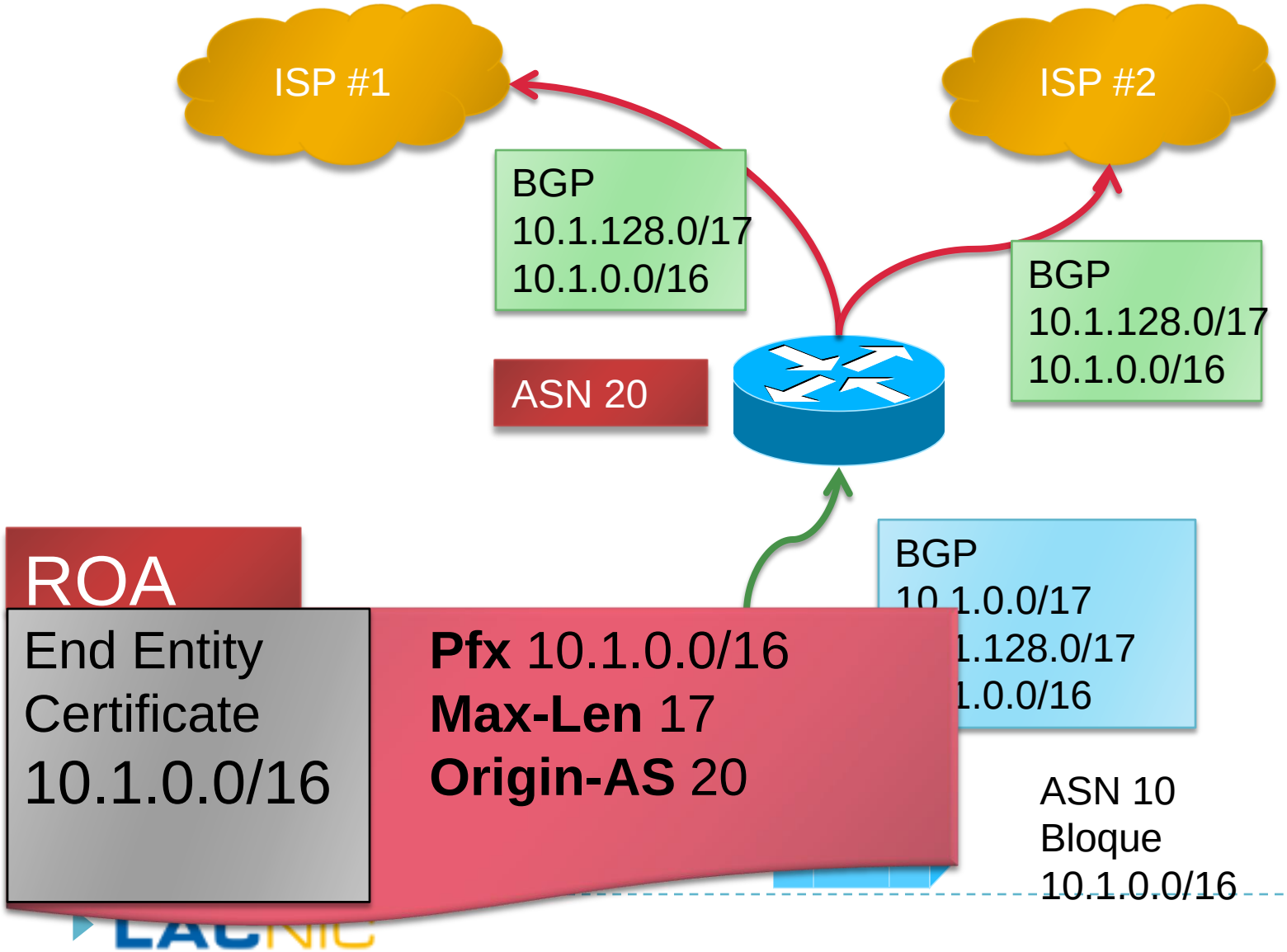


ROA

End Entity Certificate
10.1.0.0/16

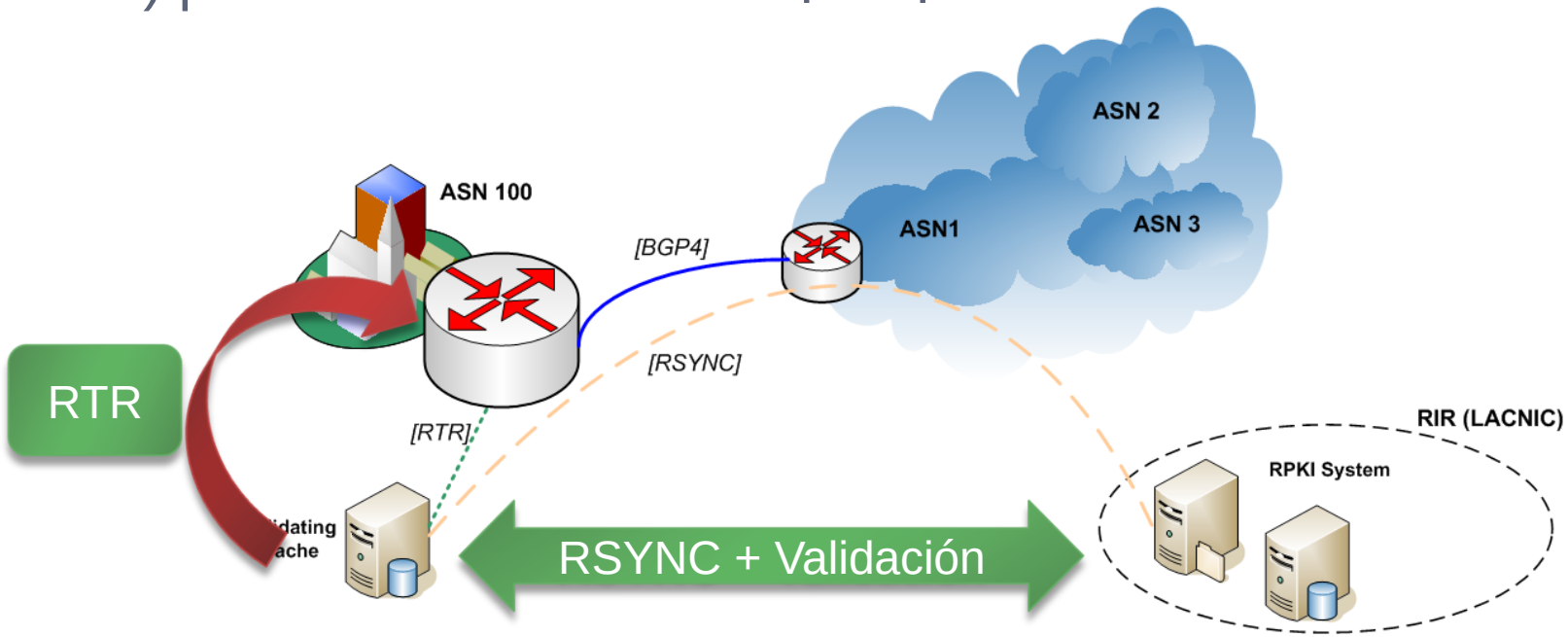
Pfx 10.1.0.0/16
Max-Len 17
Origin-AS 10

Ejemplo de ROA #2 (Erróneo)



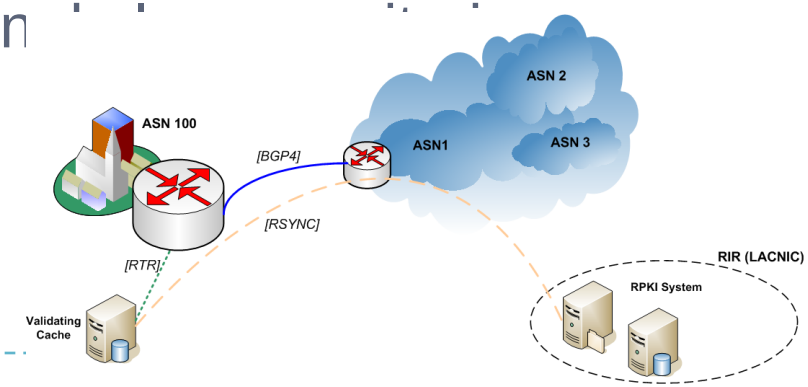
Recomendaciones sobre Cachés

- Los cachés cumplen dos funciones fundamentales:
  - Ejecutan la validación de los repositorios
    - Producto: lista de prefijos validados
  - Hablan con los routers mediante RTR (draft-ietf-sidr-rpki-rtr-17) para informarles de los prefijos válidos



Recomendaciones sobre Cachés

- Redundancia
  - Cada router puede utilizar mas de un caché
  - Podemos tener varios cachés por sistema autónomo e incluso utilizar los cachés como un servicio provisto por terceros
- Transporte
  - Raw TCP, SSH, TCP-AO
- Refresh time
  - Compatible con la regeneración



Recomendaciones para Cachés

- Implementaciones – Validación
  - rcynic: http://subvert-rpki.hactrn.net/rcynic/
  - RIPE-NCC's
- Implementaciones – RTR
  - rpki.net
  - RIPE-NCC
    - Todavía no liberada, en testing
  - BBN: rsync -a rsync://rpki.bbn.com/vm/bbn_rpki30b.tar.gz .

Políticas de enrutamiento

- RPKI no es una proposición de todo-o-nada
  - Despliegue voluntario y no coordinado
- Estados de validez {VALID, INVALID, NOT_FOUND}
- Política:
  - ¿Que hacemos con las rutas INVALID y NOT_FOUND?
- Posibilidades
  - No aceptar rutas INVALID o marcarlas de alguna forma
  - Aceptar las rutas VALID y marcarlas de alguna forma
- Estado de validez en iBGP
  - La validación tiene sentido en las sesiones eBGP

Política de enrutamiento (ii)

- Actualmente el mayor número de rutas va a ser {NOT_FOUND}
- Quizás es temprano (en términos de despliegue de RPKI) para descartar {INVALID}
  - Pero seguro nunca es tarde para saber si estoy recibiendo este tipo de rutas
- ISPs:
  - Entender el estado de validez de las rutas que estoy recibiendo
  - Trasladar la decisión de política hacia los clientes

Política de enrutamiento (iii)

- Local-Preference
  - Tanto Cisco como Juniper permitirán asociar una local-preference a los estados de validez
  - Esto me permite
    - Trasladar la decisión hacia el interior de la red, donde pueden aplicarse diferentes criterios
      - Instalaciones de mayor o menor seguridad

Ejemplo (Cisco)

- Asignar local-preference

```
!
route-map rpki permit 10
match rpki invalid
set local-preference 50
!
route-map rpki permit 20
match rpki incomplete
set local-preference 100
!
route-map rpki permit 30
match rpki valid
set local-preference 200
```

Referencias

- [SIDROPS] “RPKI-Based Origin Validation Operation” http://tools.ietf.org/html/draft-ietf-sidr-origin-ops-10
- [SIDRUSEC] “Use Cases and Interpretation of RPKI Objects for Issuers and Relying Parties” http://tools.ietf.org/html/draft-ietf-sidr-usecases-02

Referencias

- RPKI LACNIC: http://rpki.lacnic.net
- Estadísticas RPKI: http://www.labs.lacnic.net/~rpki
- RPKI Demo:
  - Acceso: http://rpkidemo.labs.lacnic.net
  - Documento de uso: http://www.labs.lacnic.net/drupal/acceso-al-demo-rpki
- IETF SIDR Working Group: http://tools.ietf.org/wg/sidr/
- RIPE Repository Validator:
  - http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification

¡Muchas gracias por su atención!

Carlos M. Martínez (carlos @ lacnic.net)