lacnic45

25 - 28 MAYO / CIUDAD DE PANAMÁ, PANAMÁ

ASPA - Autonomous System Provider Authorization

Guillermo Cicileo – guillermo@lacnic.net

LIMITACIONES DE RPKI:
¡CUANDO TENIAMOS TODAS LAS RESPUESTAS NOS CAMBIARON LAS PREGUNTAS!

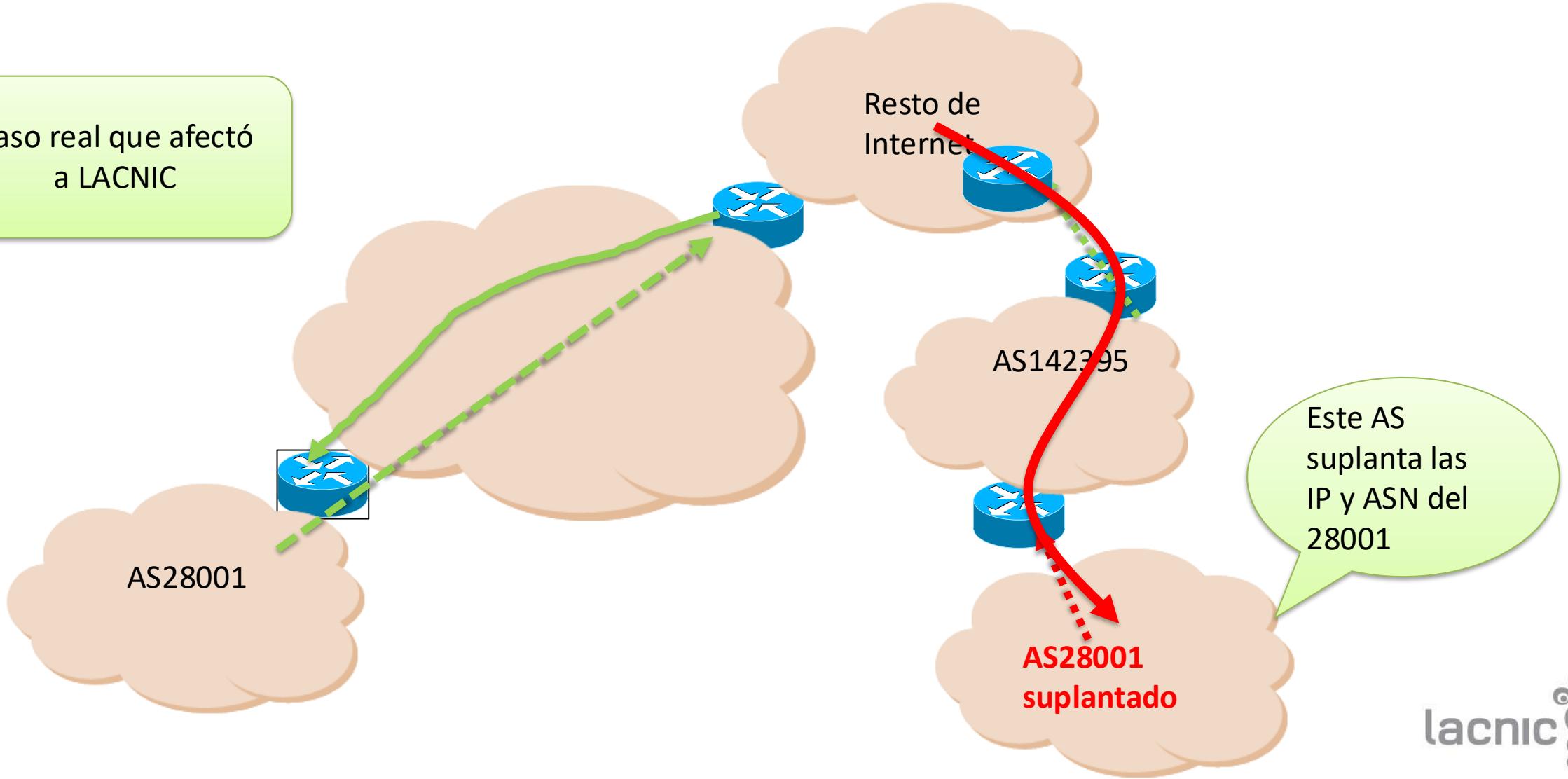
lacnic

¿Cuál es el problema a resolver?

- RPKI brinda una solución parcial: validación de origen
  - Validar que el ASN que publica los prefijos es el autorizado a hacerlo
- IRR brinda una solución parecida
  - Si bien tendría potencial para más información, se utiliza mayormente lo básico (route, route6, as-sets)
  - Problemas: mecanismo de autorización débil, información desactualizada
- Necesitamos mecanismos para validar todo el camino de los anuncios BGP, no sólo el origen
  - Leaks: generalmente el ASN de origen se preserva, RPKI no los evita
  - Es posible agregar el ASN de origen correcto en un AS-PATH falsificado
- BGPSec es una propuesta, pero no ha tenido mucha aceptación

Secuestro de rutas: suplantación de AS de origen

Caso real que afectó a LACNIC



ASPA

¿Qué es ASPA?

- Autonomous System Provider Authorization
- https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/
- Un nuevo objeto criptográfico dentro de RPKI
- Permite al titular de un ASN autorizar explícitamente a otros ASNs para que actúen como sus proveedores de tránsito (upstreams)
- **Caso Especial:** "AS0 ASPA" indica que el ASN no tiene proveedores (ej. Tier-1 o clientes de un Route Server ciego)

Estructura del objeto ASPA

- **Certificado EE:** Contiene el ASN titular, la clave pública y la firma de la CA.
- **Contenido (eContent):**
  - *Customer ASN* (ASN Firmante)
  - *Set of Provider ASNs* (Lista de ASNs Autorizados).
  - Aplica universalmente al ASN, independientemente del protocolo IP
- Básicamente:

  ASN => [ASx, ASy, ASz, …]

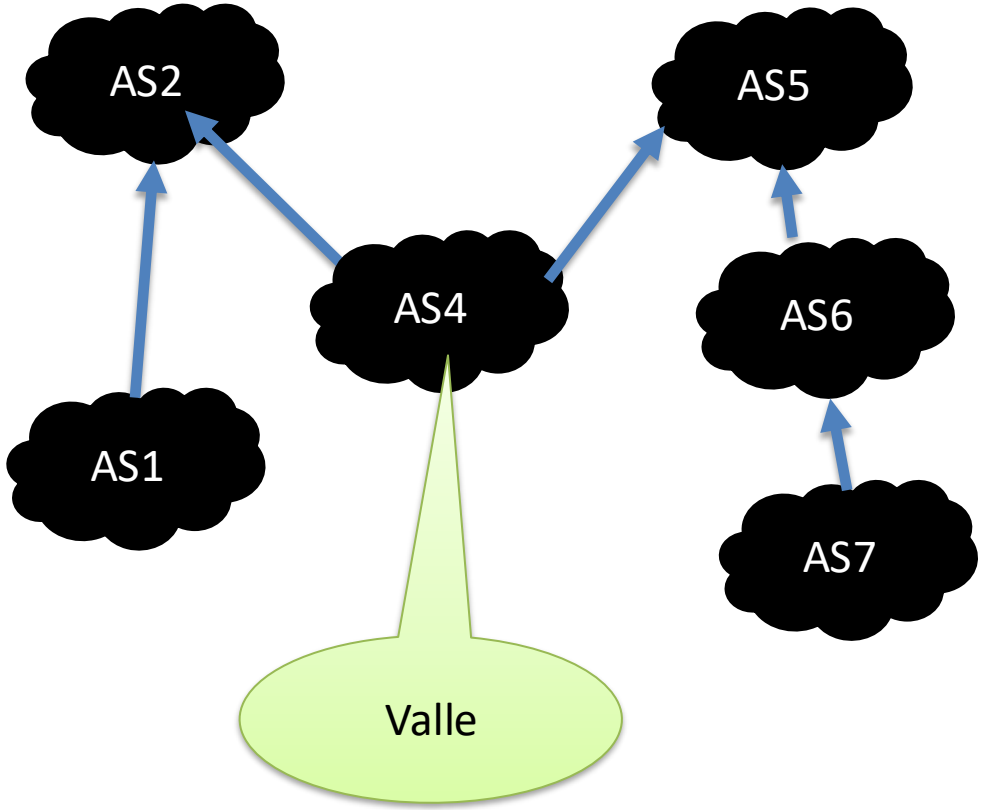
El ASN define cuáles son sus upstream

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)

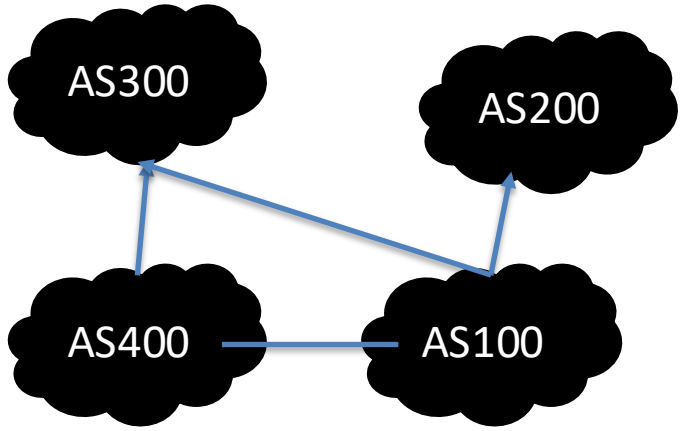
Concepto de "Valley-Free Routing"

- Las rutas de Internet tienen trayectorias lógicas:
  - Rampa de Subida (Up-ramp): De cliente a proveedor
  - Ápice (apex): Proveedor Tier-1 o un enlace lateral (Peer-to-Peer)
  - Rampa de Bajada (Down-ramp): De proveedor a cliente
- Un **Route Leak (Valle):** Ocurre cuando un camino baja a un cliente o peer, y luego vuelve a subir. ASPA formaliza la detección matemática de esta anomalía



La Función "Hop Check" (Validación Salto a Salto)

- Para cualquier par de ASN adyacentes {AS(i), AS(j)} en la ruta:
  AS_n … AS_3 AS_2 AS_1
  Se verifica en el caché RPKI la declaración (attestation) de AS(i):
- ✅ **P (Provider):**
  - Existe ASPA para AS(i) y declara a AS(j) como proveedor.
    - AS100 => [AS200, AS300]
- ❌ **nP (not Provider):**
  - Existe ASPA para AS(i), pero **NO** incluye a AS(j)
    - Ej: AS400 no está incluido en el ASPA anterior
    - Indica un salto lateral o hacia un cliente
- ⚠️ **nA (no Attestation):**
  - AS(i) no ha publicado un objeto ASPA.
    - Ej: AS400 no tiene registro ASPA definido



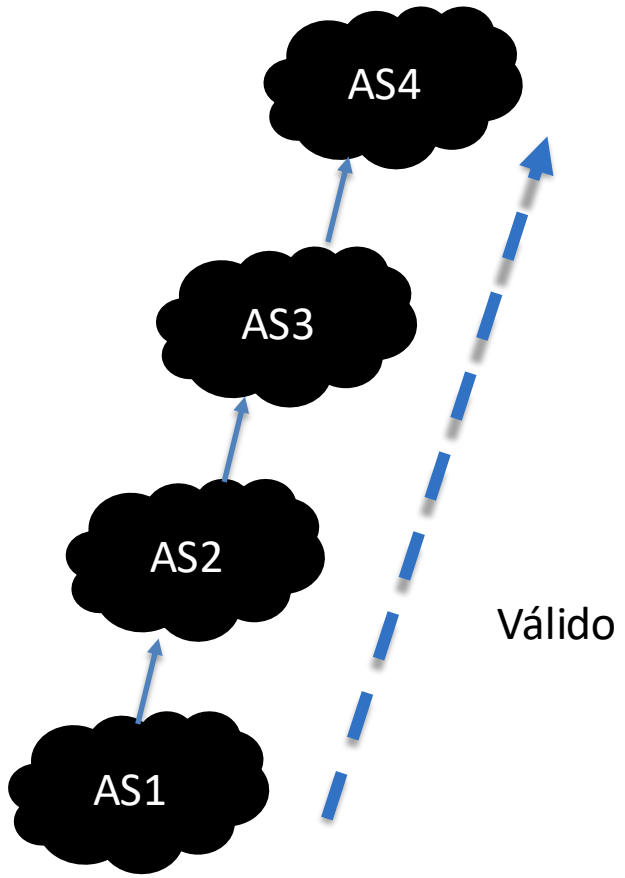
ASPA – Verificación upstream

https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

- Si el camino es ascendente, es simple
- En AS4 podemos verificar si cada uno de los AS del PATH es un “proveedor” del AS anterior
- El path AS3, AS2, AS1 es válido ya que están definidos como proveedores del AS(n-1)

- ASPA:

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



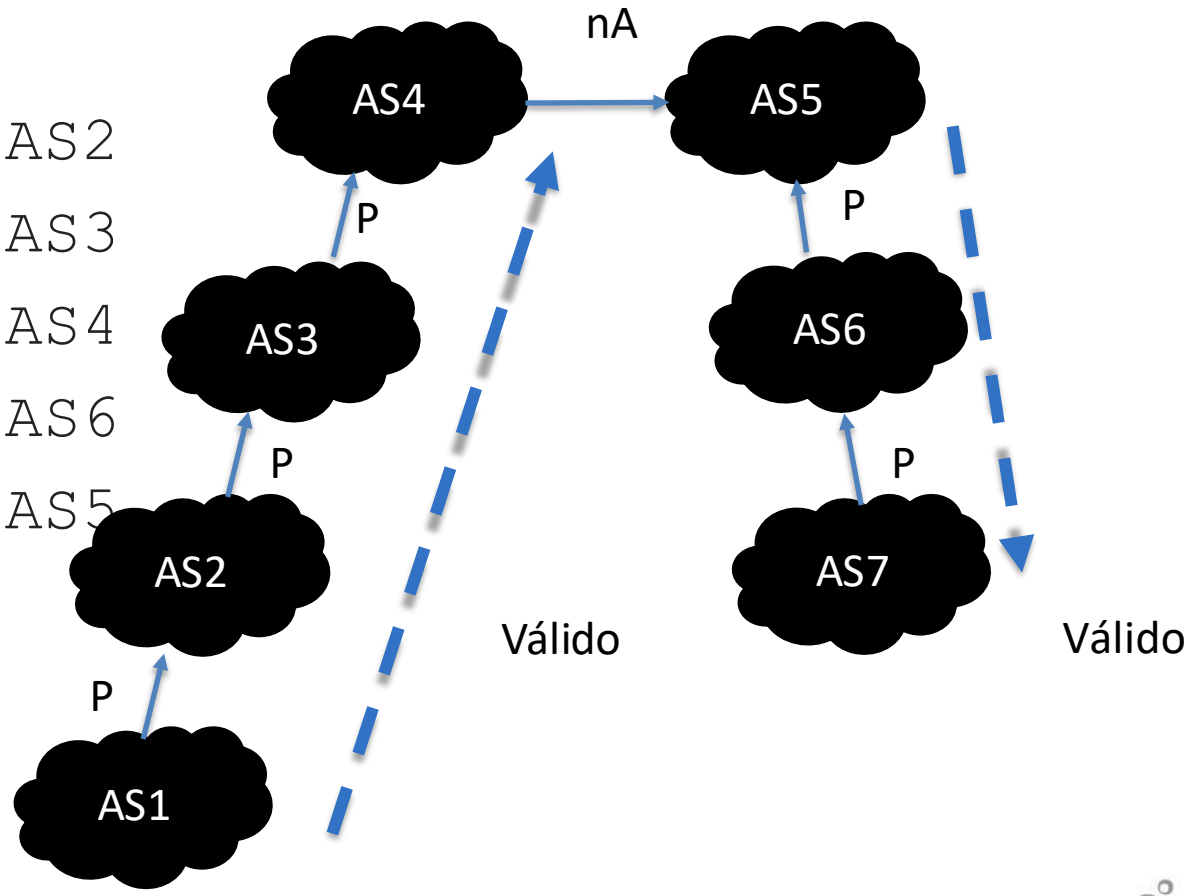
ASPA – Verificación downstream

https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/

- En este caso el camino también es válido, pero ya no es tan trivial
- La cadena upstream y downstream cumple con ASPA
- Hay una única relación de peering que no está registrada

- ASPA:

```
AS1 => AS2
AS2 => AS3
AS3 => AS4
AS7 => AS6
AS6 => AS5
```



¡MUCHAS GRACIAS!

¿Preguntas?

