UpDown RPKI LACNIC

Carlos Ortíz
cortiz@lacnic.net

31 lacnic
06/10 DE MAYO 2019
REPÚBLICA DOMINICANA

Agenda

- Secuestro de rutas
- RPKI
- UpDown
- Herramientas para probar el servicio
- Despliegue del servicio UpDown

Secuestro de rutas:

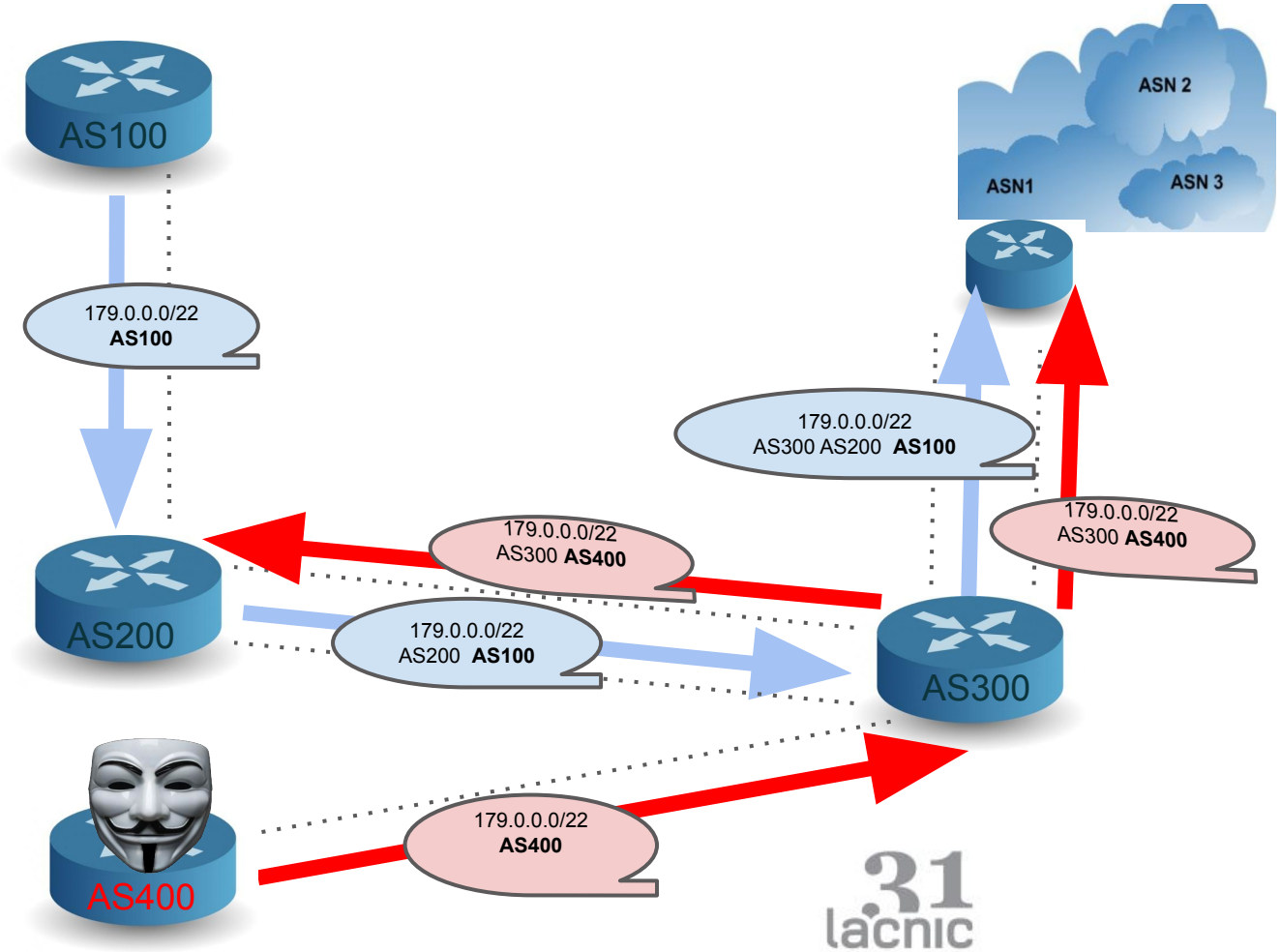
- Proceso donde se anuncia a internet prefijos NO autorizados.
    - Intencional
    - Error en operación

- La mayoría de los secuestros de rutas ocurridos hasta ahora han sido redirecciones de tráfico

- Eventualmente publicación temporal de prefijos para hacer spamming

Secuestro de rutas:

HIJACKING "CAMINO MÁS CORTO"



Quien originó el anuncio del 179/22?

AS100

Quienes propagaron la ruta?

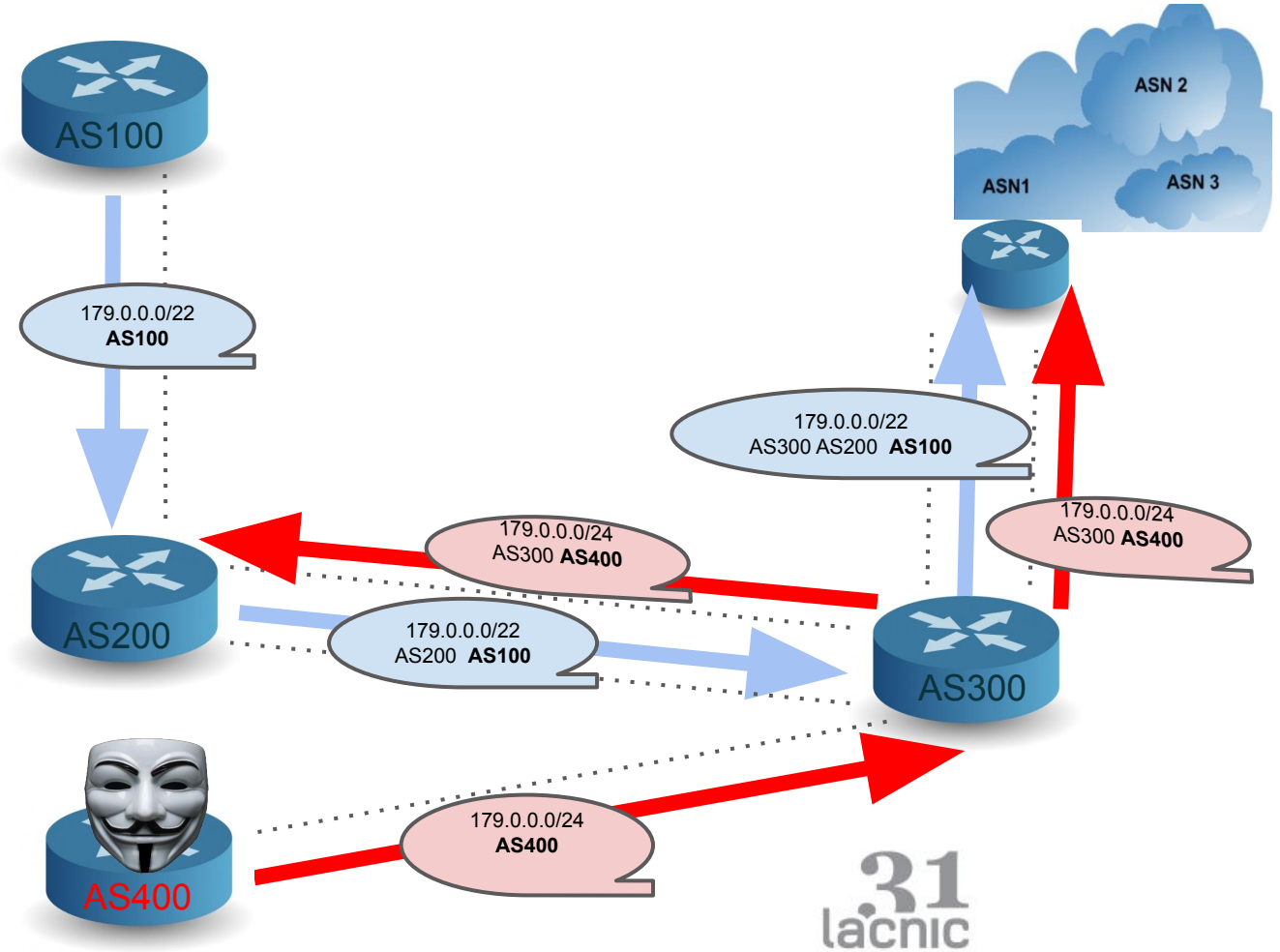
AS200,AS300

Como se da cuenta el AS100 que hay un problema?

Que puede hacer el AS100 para solucionarlo?

Secuestro de rutas:

HIJACKING "RUTA MÁS ESPECÍFICA"



Que pasa con el AS200?

Que puede hacer el AS100 para solucionarlo?

RPKI (Infraestructura de clave publica de recursos)

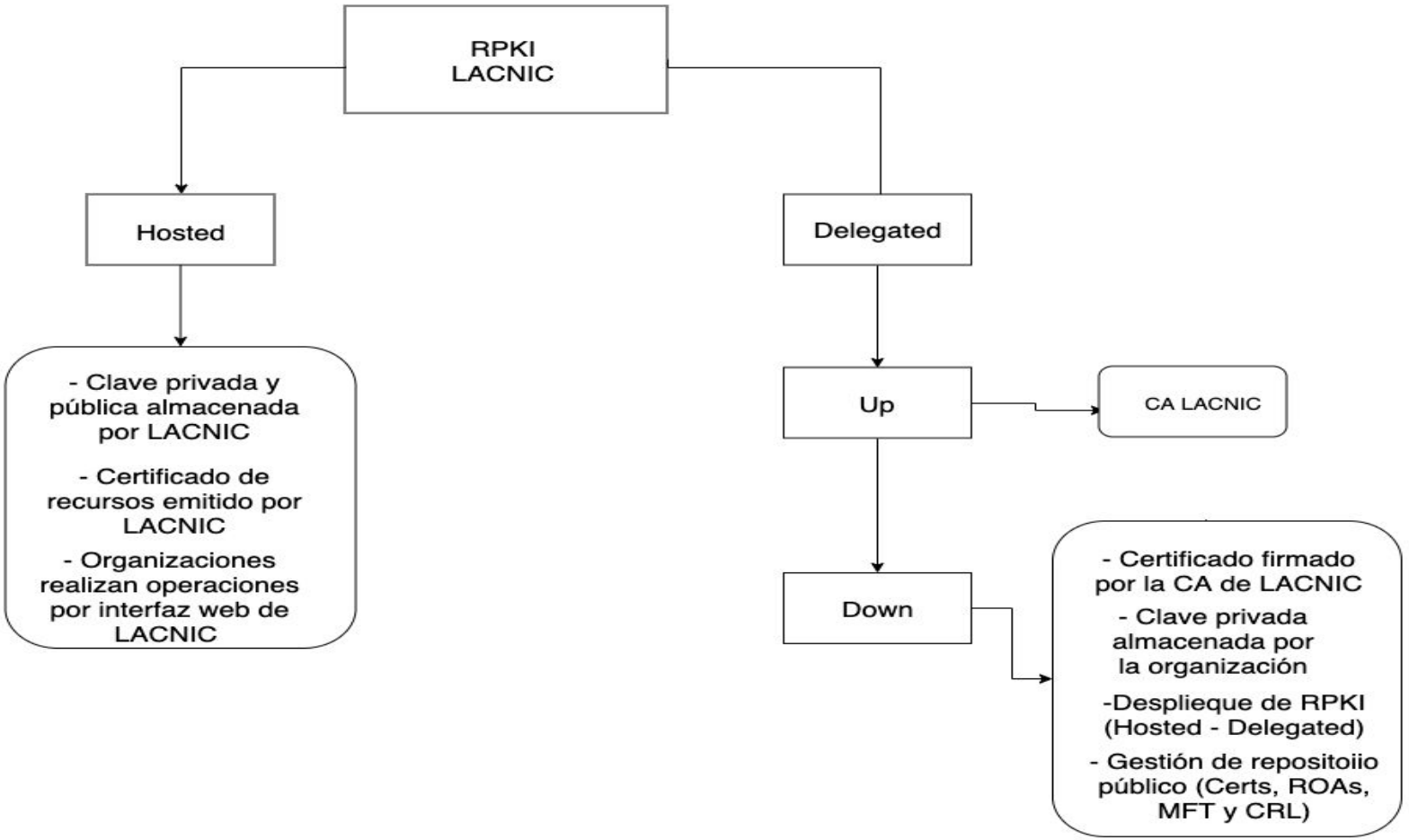
- Certificar la autorización a utilizar un recurso de internet.
- Modelo jerárquico de asignación de recursos por medio de los RIRs.
- Uso de certificados digitales X.509 v3
- Uso de extensiones para incluir recursos de internet (IPv4,IPv6,ASNs).
- Generación de objetos firmados digitalmente para soportar seguridad del enrutamiento, ROAs (Routing Origin Authorization).
- Repositorio público, íntegro y accesible por rsync, donde se publican objetos RPKI.

Funcionamiento RPKI

- Modo Hosteado:
  - LACNIC emite los certificados de recursos y almacena tanto claves públicas como privadas.
  - Los certificados se emiten a demanda de las organizaciones y son estas las que realizan operaciones por medio de una interfaz web provista por LACNIC.

- Modo Delegado:
  - Estándar UpDown RPKI, protocolo de aprovisionamiento de certificados RPKI.
  - Simple interacción request / response.
  - Cliente almacena su clave privada, garantiza integridad del repositorio con todos sus objetos (Certs, ROAs, MFT, CRLs).

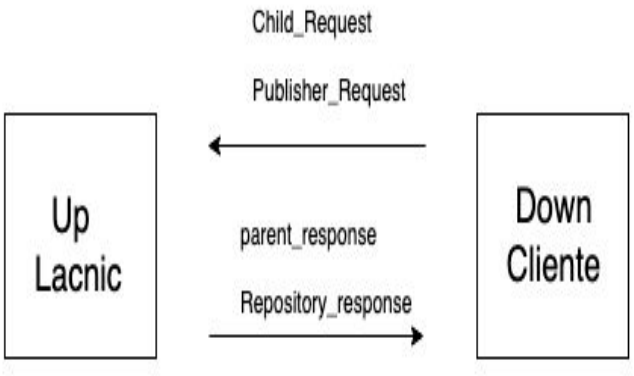
Funcionamiento RPKI



UpDown RPKI

¿Cómo empezar?

1- Out-of-Band. RFC 8183



Seguir

2- Protocol for Provisioning Resource Certificate. RFC 6492

- List
- Issuance
- Revoke

UpDown RPKI

Retos de implementación parte Up:

- Garantizar funcionamiento de sistema RPKI:
  - Generación de repositorio con todos los objetos.
  - Validación de objetos en repositorio.
  - Implementación de nuevos mecanismos de monitoreo

UpDown RPKI

Responsabilidades de la implementación Down:

- Almacenar clave privada.
- Desplegar RPKI mediante modelo hosteado o delegado.
- Garantizar integridad del repositorio donde se publican todos los objetos RPKI como Certs, ROAs, MFT y CRLs.

UpDown RPKI

Herramientas:

- Software rpki.net de dragonresearch para probar UpDown

- Instalar validador RPKI de RIPE, México.

- Interoperabilidad a través de otros RIRs.

Despliegue del servicio

Servicio Beta UpDown LACNIC:

- Finales de Junio de 2019

Dirigido:

- Organizaciones que quieran proveer a sus clientes, con su propio sistema de gestión RPKI.

Conclusiones

- UpDown permite automatizar la gestión de certificados RPKI.

- El cliente (parte Down), contará con certificado firmado por la CA de LACNIC.

- El cliente debe almacenar su clave privada y requiere desplegar RPKI en modo hosteado o delegado.

- El cliente debe generar un repositorio íntegro con todos los objetos presentes en RPKI (Certs, ROAs, MFT, CRLs).

- Secuestro de rutas
- RPKI
- UpDown
- Herramientas para probar el servicio
- Despliegue del servicio UpDown