RPKI – Resource Public Key Infrastructure
Validación de Origen en BGP

Darío Gómez

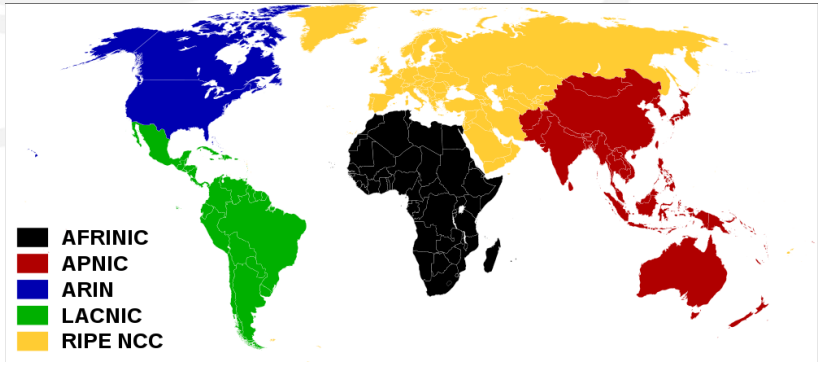
RPKI – Resource Public Key Infrastructure

ASIGNACIÓN Y ADMINISTRACIÓN DE RECURSOS DE INTERNET

lacnic

Administración de los Recurso de Internet

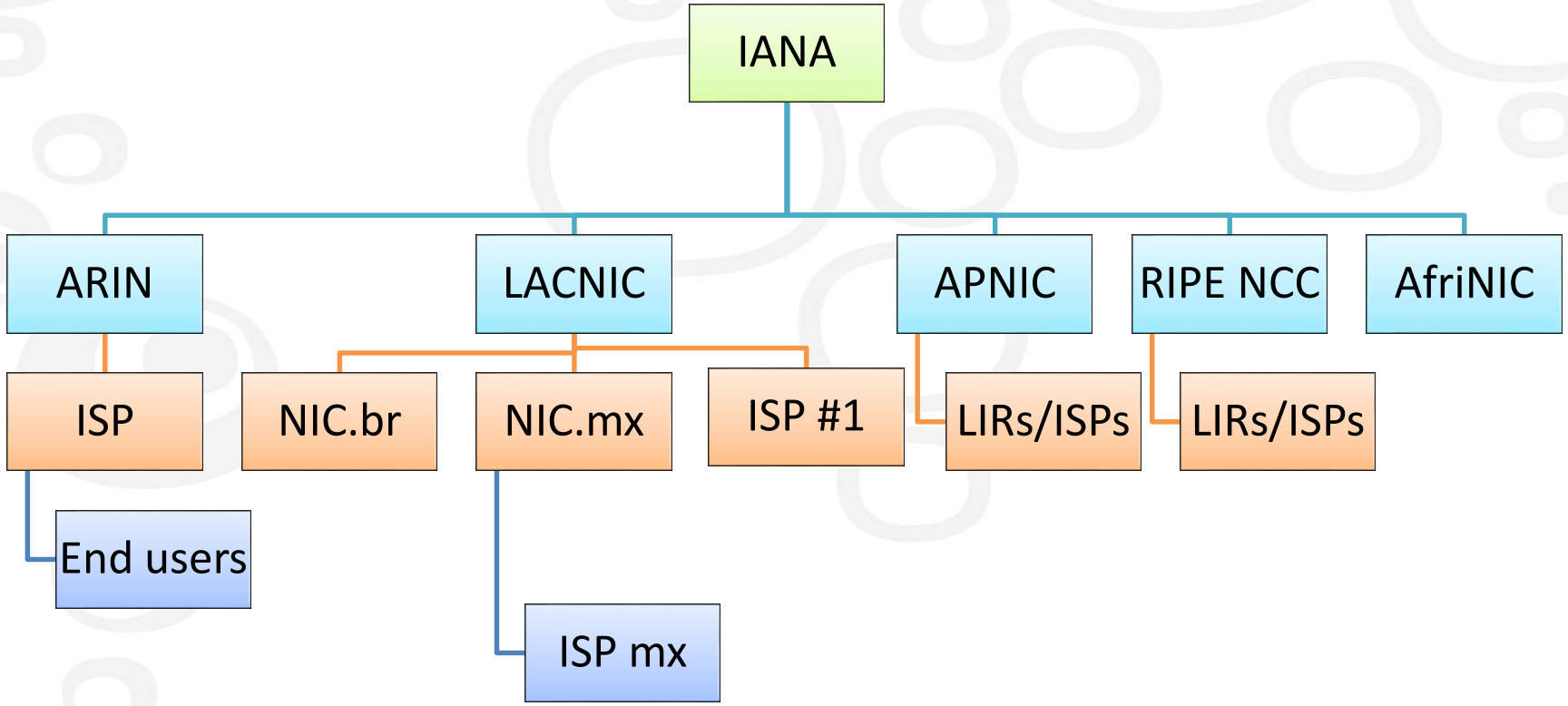
- Recursos
  - Bloques IPv4
  - Bloques IPv6
  - Sistemas Autonomos
    - 16 y 32 bits



- Documento fundacional: RFC 2050
  - *"IP Registry Allocation Guidelines"*

- Cada RIR es **fuente autoritativa de información de la relación "usuario" <-> "recurso"**
  - Cada RIR opera su propia base de datos

Administración de los Recurso de Internet (ii)



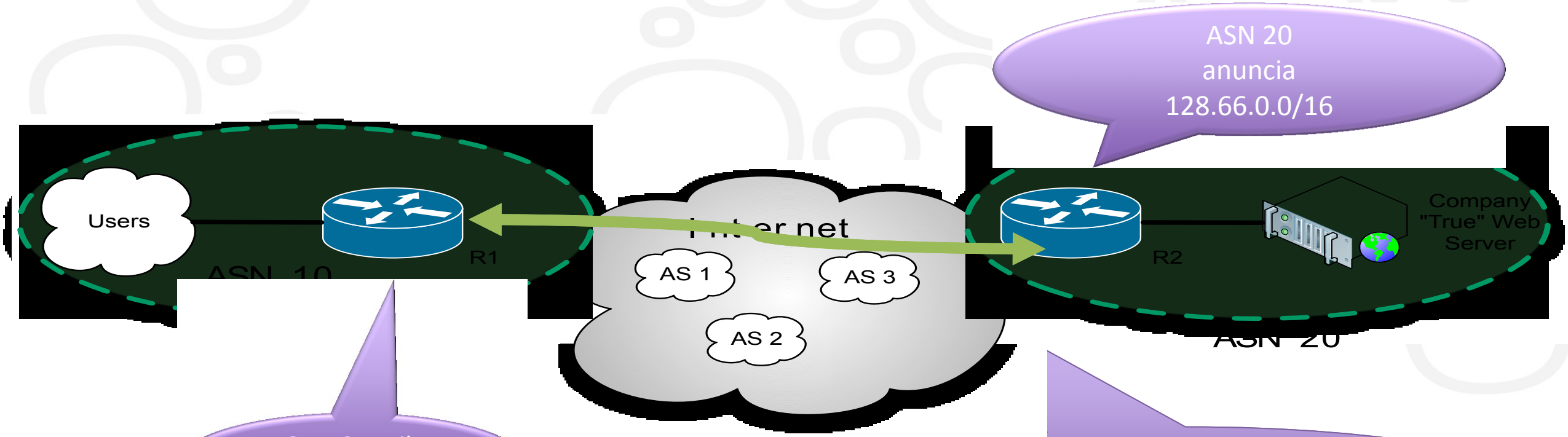
- Cada RIR es **fuente autoritativa de información de la relación "usuario" <-> "recurso"**

RPKI – Resource Public Key Infrastructure

RUTEO EN INTERNET

lacnic

Ruteo en internet



Ruteo en internet (ii)

- BGP selecciona las rutas de acuerdo con un **algoritmo de decisión** y los valores de los **atributos**

- AS_PATH y AS de origen
  - AS_PATH es la lista de sistemas autónomos recorridos por un UPDATE
  - Incluye el AS que origina el anuncio (“origin-as”)

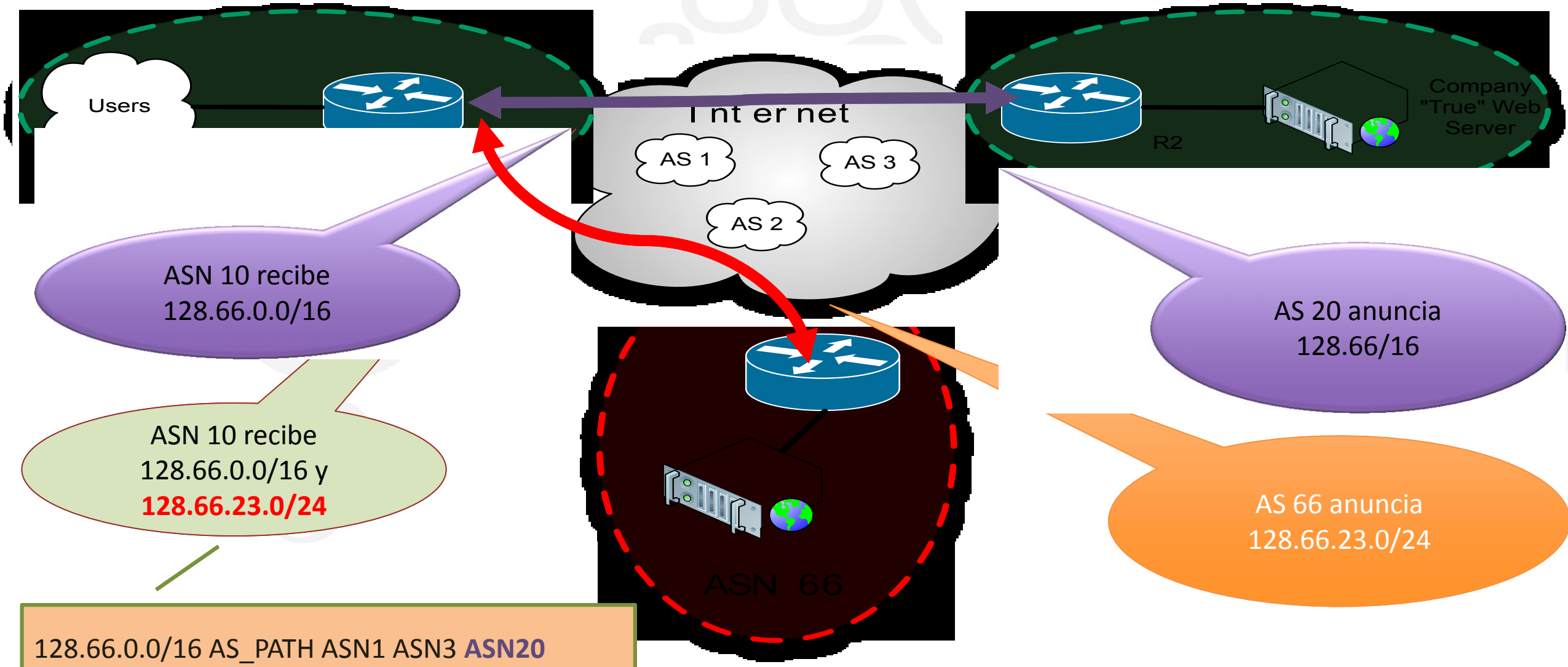
RPKI – Resource Public Key Infrastructure

SECUESTRO DE RUTAS

Secuestro de rutas

- Cuando un participante en el routing en Internet anuncia un prefijo que no esta autorizado a anunciar se produce un "*secuestro de ruta*" (*route hijacking)*
- Malicioso o causado por error operacionales
- Casos más conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - Google en Europa del este (varios AS, 2010)
  - **Casos en nuestra región (enero/febrero de 2011)**

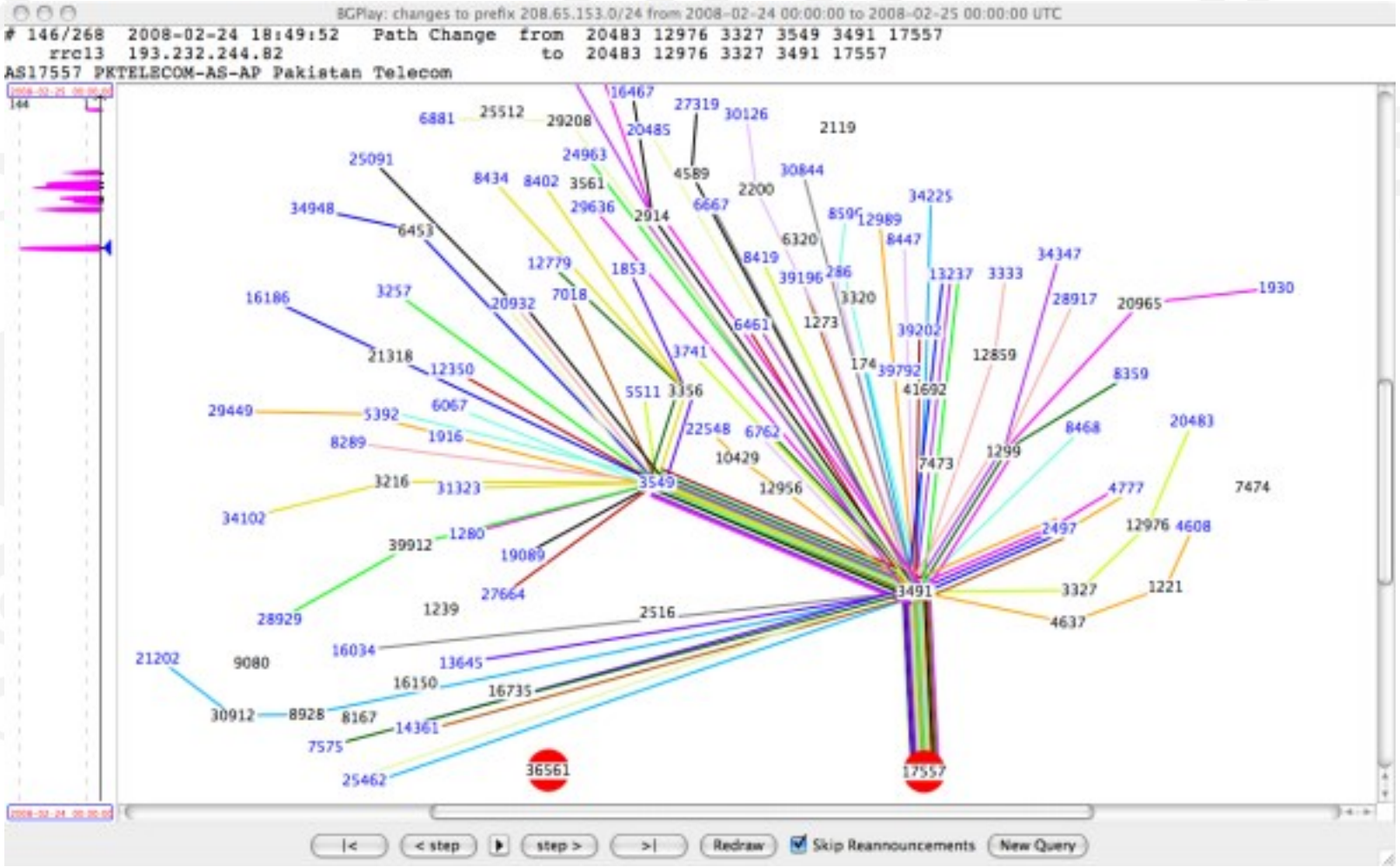
Secuestro de rutas (ii)



Pakistan Telecom vs. YouTube

- El Domingo 24 de Febrero de 2008 Pakistan Telecom (AS 17557) anunció el prefijo 208.65.153.0/24 sin autorización
- El upstream provider PCCW Global (AS3491) reenvió este anuncio al resto de Internet, resultando en que YouTube quedó inaccesible
- Análisis detallado (por RIPE NCC): http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
- Video en YouTube sobre el evento: http://www.youtube.com/watch?v=IzLPKuAOe50

Pakistan Telecom vs. YouTube



lacnic

Secuestro de rutas (iii)

- La mayoría de los secuestros de rutas ocurridos hasta ahora han sido redirecciones de tráfico
  - El problema es detectado por inaccesibilidad del sitio original (ej: caso YouTube)

- Eventualmente publicación temporal de prefijos para hacer spamming

Que solución propone RPKI?

- Validar el AS que origina una ruta
  - Sólo quien tiene delegados los prefijos podrá originar una ruta anunciándolos
- De esta forma, los ejemplos que vimos no podrían ocurrir
- No previene otro tipo de ataques no relacionados al AS de origen de una ruta
  - Ej: AS simulando dar tránsito a un AS y rutas válidas

Validación de recursos

RPKI

¿Qué es RPKI?

- RPKI (Resource Public Key Infrastructure) permite la validación del derecho de una organización a usar un recurso determinado (IPv4, IPv6, ASN)
- RPKI combina la jerarquía del modelo de asignación de recursos de Internet a través de los RIRs con el uso de certificados digitales basados en el estándar X.509
- RPKI es estandarizado en el IETF a través del grupo de trabajo SIDR, el cual ha producido los RFCs 6480 – 6492
- Gran trabajo de los RIRs en la implementación

¿Qué compone la solución RPKI?

- Public Key Infrastructure de recursos (IP+ASN+certificados)
- Objetos firmados digitalmente para soportar seguridad del enrutamiento (ROAs)
- Un repositorio distribuido que almacena los objetos PKI y los objetos de enrutamiento firmados (ROAs+CRL+MNF)

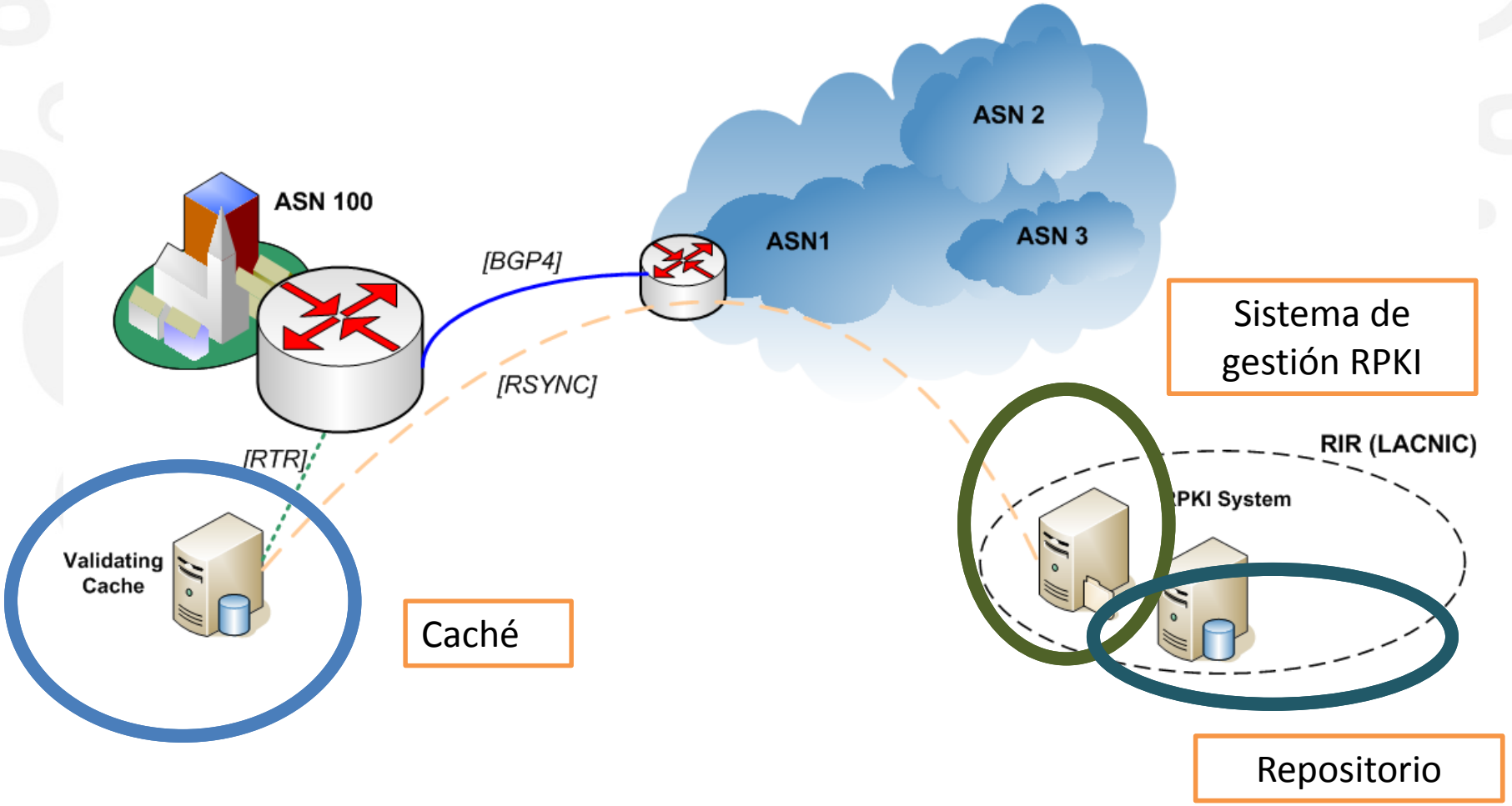
RPKI

- Metodología automatizada que permita validar la autoridad asociada a un anuncio de una ruta “**origen de una ruta**”
- El emisor de la información de ruta "**firma**" la información de “AS de origen”
- Para validar certificados e información de enrutamiento se utilizan:
  - Las propiedades del cifrado de clave pública (certificados)
  - Las propiedades de los bloques CIDR
- Se impide entonces que terceros falsifiquen la información de enrutamiento o las firmas

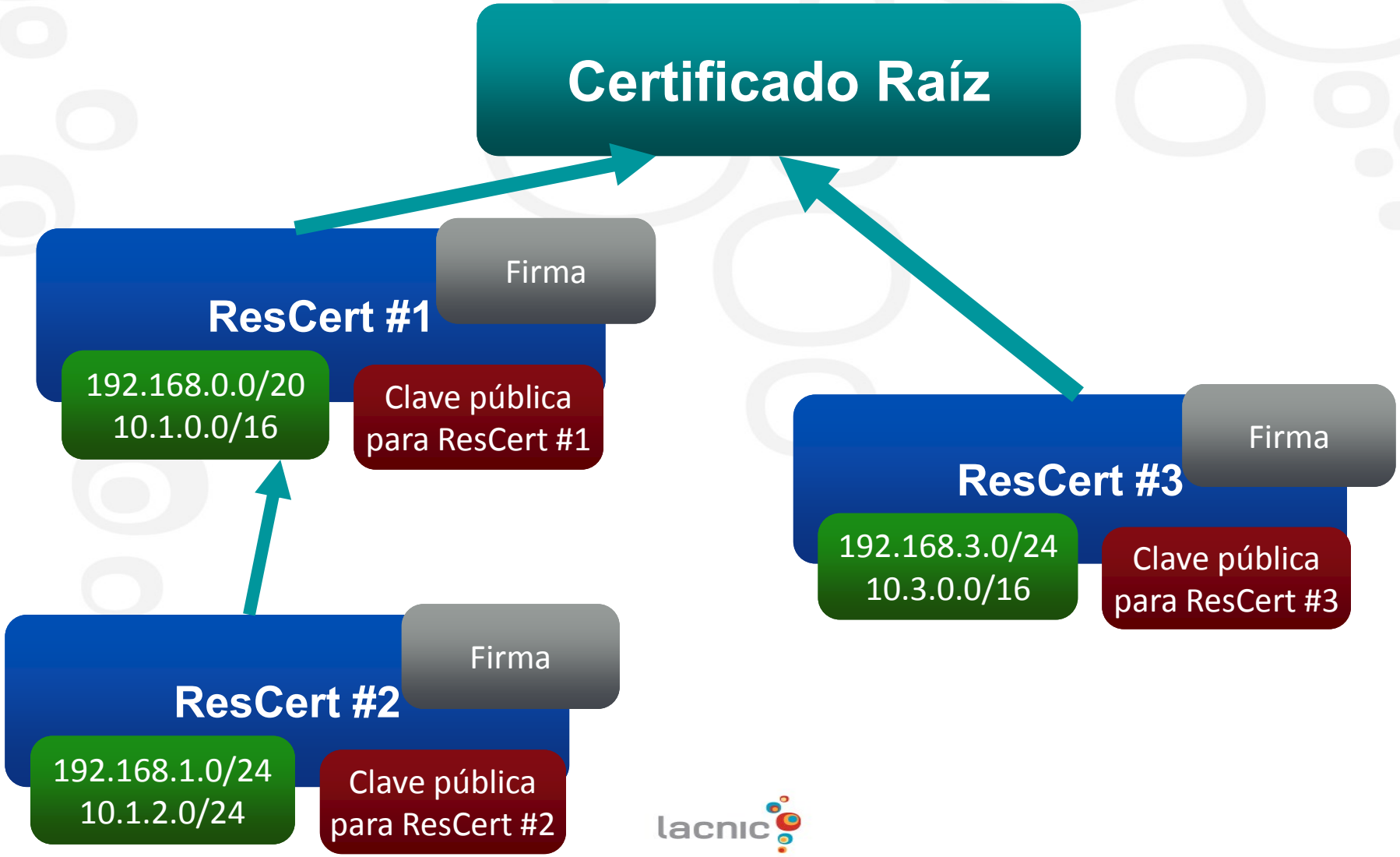
RPKI

- Todos los objetos firmados de RPKI se listan en repositorios públicos
- Luego de ser verificados, estos objetos pueden ser usados para configurar filtros en los routers
- Proceso de validación
  - Los objetos firmados tienen referencias al certificado usado para firmarlos
  - Cada certificado tiene un puntero a un certificado de un nivel superior
  - Los recursos listados en un certificado DEBEN ser subconjuntos válidos de los recursos listados en el certificado padre
  - De esta forma se puede seguir una cadena de confianza hasta un "trust anchor" tanto criptográficamente como en términos de CIDR

Modelo RPKI


ASN 100
[BGP4]
ASN 2
ASN1
ASN 3
[RSYNC]
[RTR]
Validating Cache
Caché
Sistema de gestión RPKI
RIR (LACNIC)
RPKI System
Repositorio

PKI de Recursos



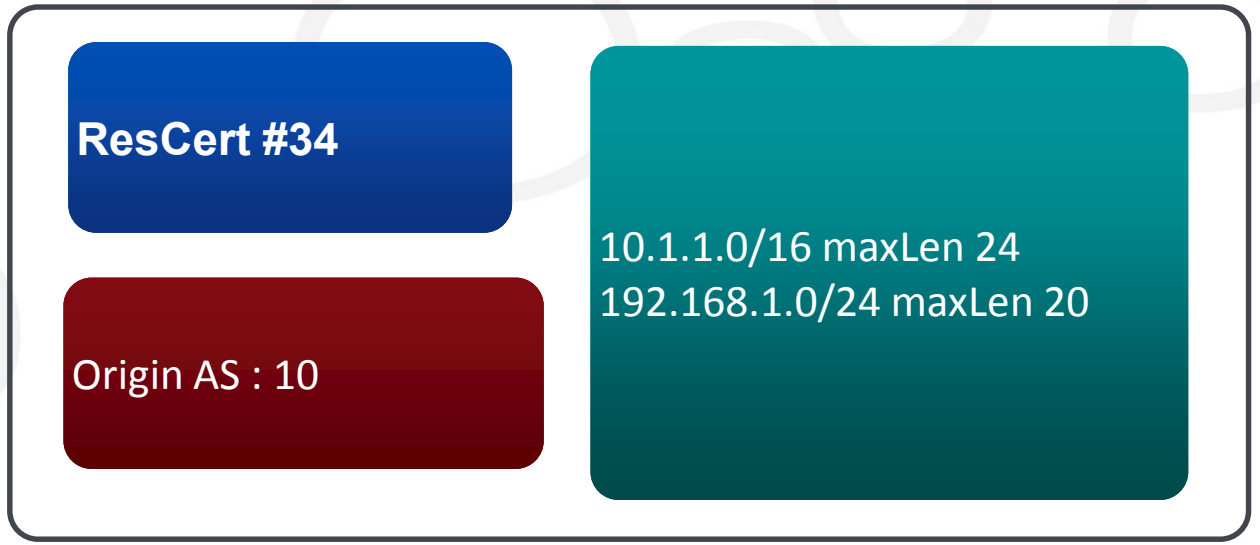
ROAs

- Usando certificados podemos crear objetos que describan el origen de un prefijo

- ROAs: Routing Origin Authorization
  - Los ROAs contienen información sobre el AS de origen permitido para un conjunto de prefijos
  - Los ROAs son firmados usando los certificados generados por RPKI
  - Los ROAs firmados son copiados al repositorio

ROAs (ii)

ROA: route origin authorization



Un ROA es una sentencia sobre ruteo:

"El prefijo 10.1.1.0/16, desagregado hasta /24s, será anunciado desde el AS 10"

Los ROAs son **firmados** usando la clave del certificado de recursos incluido

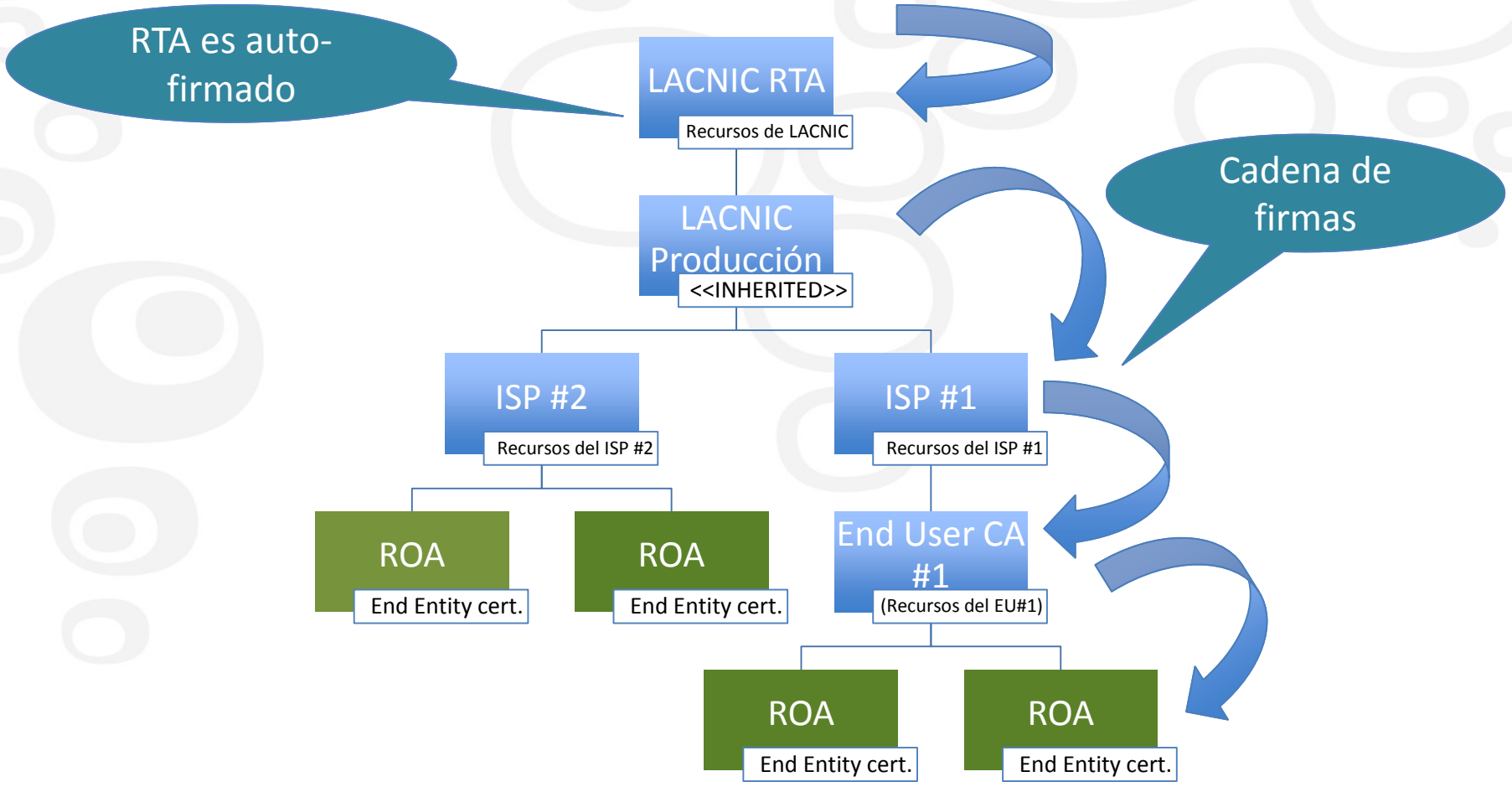
ROAs (iii)

- Un ROA simplificado contiene la siguiente información:

Prefix	MaxLen	Origin AS	Valid Since	Valid Until
200.40.0.0/17	20	6057	2013-01-02	2013-12-31
200.3.12.0/22	24	28000	2013-01-02	2014-12-31

- Este ROA establece que:
  - ”El prefijo 200.40.0.0/17 será originado por el ASN 6057 y podría ser desagregado hasta un /20" ”Esto es válido desde el 2 de Enero de 2013 hasta el 31 de Diciembre de 2013"
- Otro contenido del ROA:
  - Los ROAs contienen material criptográfico que permite la validación del contenido del ROA

Estructura de la RPKI de LACNIC



Estructura de la RPKI LACNIC (ii)

- CAs
  - Entidad emisora de certificados (bit CA=1)
    - ISPs pueden usar este certificado para firmar certificados de sus clientes
- Repositorio
  - Repositorio de certificados, CRLs y manifiestos
  - Accesible via “rsync”
- Interfaz de gestión
  - Interfaz web de usuario para aquellos que prefieran el modo “hosted”

Validación de Origen

- Los routers arman una base de datos con la información que reciben de los caches
- Esta tabla contiene
  - Prefix, Min length, Max length, Origin-AS
- Aplicando un conjunto de reglas, se asigna un estado de validez a cada UPDATE de BGP
- Los operadores de red pueden usar el atributo “validez” para construir políticas de ruteo
- 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

Validación de Origen

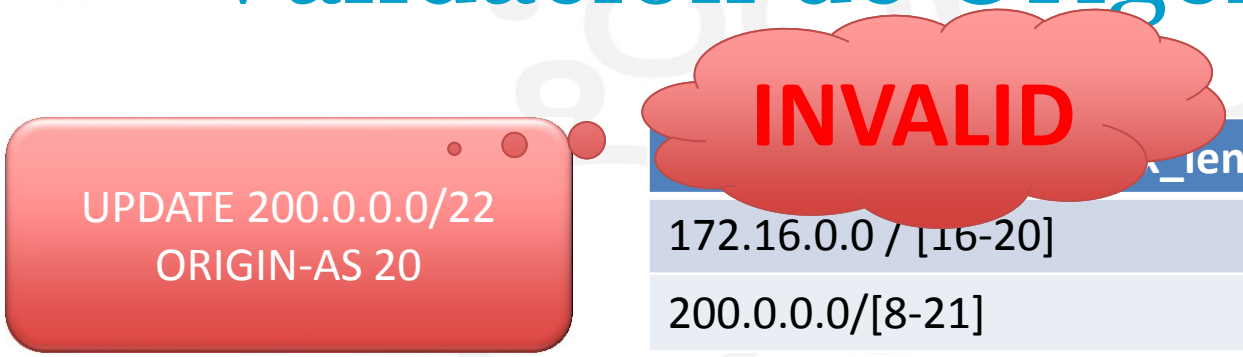
UPDATE 200.0.0.0/9
ORIGIN-AS 20

VALID

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

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen



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

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen

UPDATE 200.0.0.0/9
ORIGIN-AS 66

INVALID

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

- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Validación de Origen

UPDATE 189.0.0.0/9
ORIGIN-AS 66

NOT FOUND

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

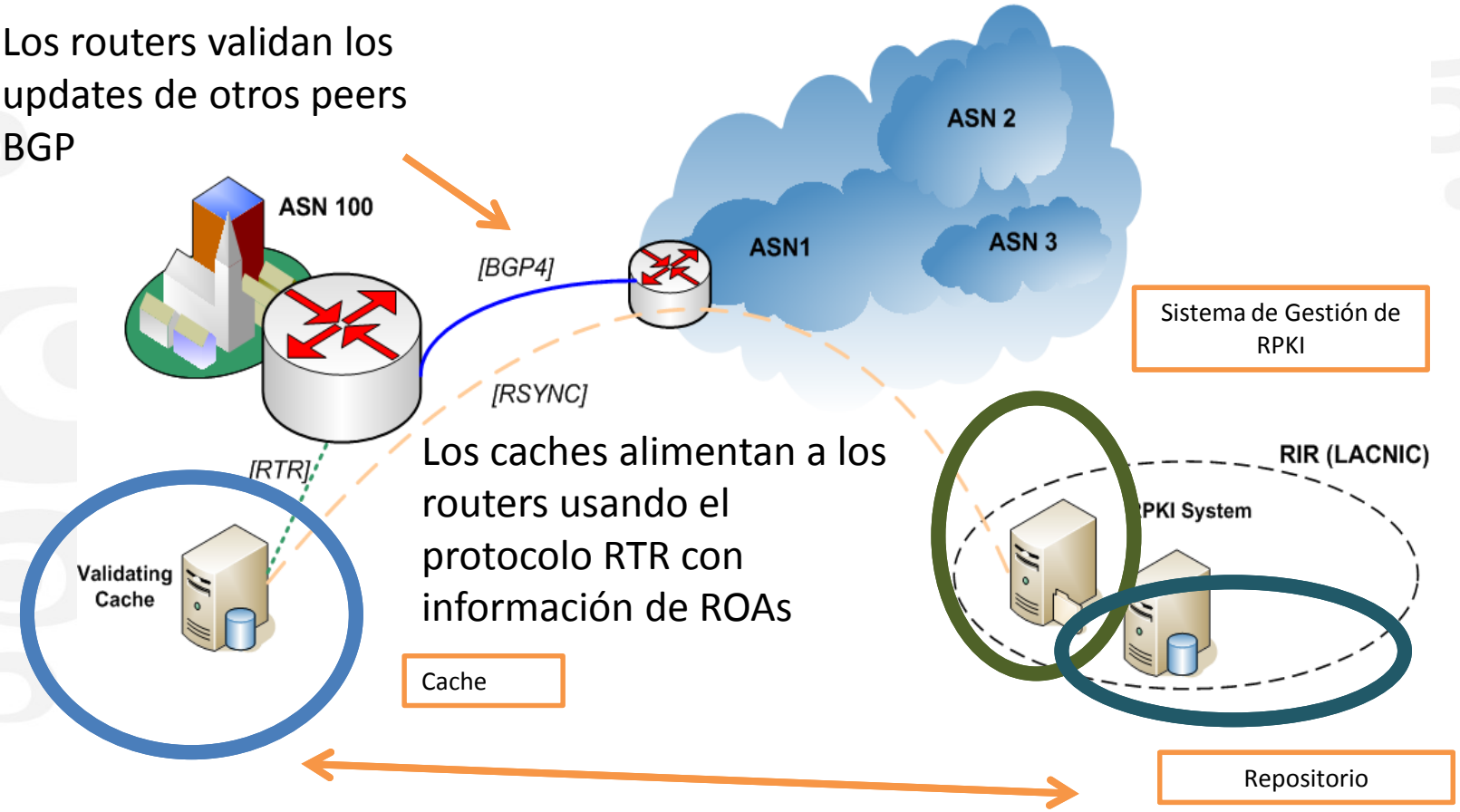
- Si el prefijo del UPDATE no está cubierto por ninguna entrada en la BD -> "**not found**"
- Si el prefijo del UPDATE está cubierto al menos por una entrada en la BD, y el AS de origen coincide con el AS en la BD -> "**valid**"
- Si el AS de origen no coincide -> "**invalid**"

Políticas de Ruteo con Validación de Origen

- Usando el atributo de validez de BGP los operadores de red pueden construir políticas de ruteo
- Por ejemplo:
  - A las rutas con estado “valid” asignarles mayor preferencia que a las rutas con estado “not found”
  - Descartar rutas con estado “invalid”
- MUY IMPORTANTE: RPKI es una fuente de información! Los operadores son libres de usarla como les parezca mejor

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

RPKI en acción (ii)

- El proceso de validación a nivel de la infraestructura de enrutamiento está dividido en dos
  - Validación de los ROAs como objetos firmados
    - Lo realiza el caché validador
  - Validación de la información recibida en los UPDATE de BGP
    - Lo realizan los “bgp speakers” de la red
- Existe un protocolo de comunicación entre caché y routers (RTR) que está definido en la RFC 6810

RPKI en funcionamiento (iii)

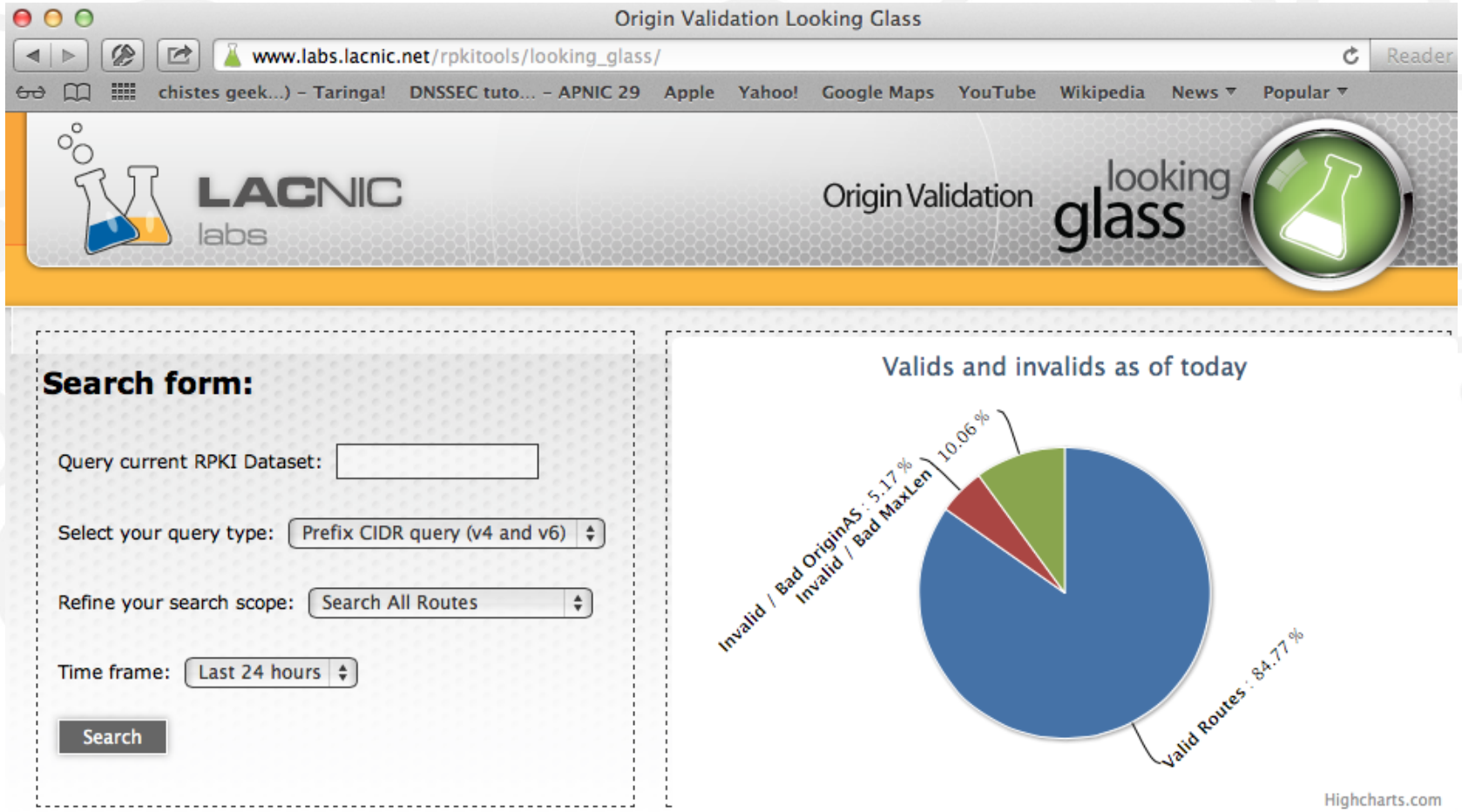
- En el caché
  - Se bajan por RSYNC los contenidos de los repositorios RPKI
  - Se validan los certificados y ROAs
    - Criptográficamente (cadena de firmas)
    - Inclusión correcta de recursos
- En los routers
  - Se construye una base de datos con la relación entre prefijos y AS de origen

Conclusiones

- El sistema de ruteo es una de las operaciones principales de Internet
- La seguridad de BGP depende mucho de la confianza mutua y de chequeos ad-hoc
- El sistema de ruteo aún es vulnerable a ataques y a configuraciones erróneas
- Los secuestros ocurren. Alguno de ustedes podrían ser la próxima víctima
- Se ha hecho algo de trabajo (RPKI, Origin Validation)
- Pero es necesario seguir trabajando
  - Especificación del protocolo
  - Despliegue (Filtrado, RPKI, Origin Validation)
- Los certificados de recursos y los ROAs son una herramienta para que quienes tienen recursos asignados señalicen intenciones de ruteo y la mayoría lo pueden empezar a hacer hoy mismo

Herramientas Disponibles

- LACNIC's Origin Validation Looking Glass
  - Permite visualizar y buscar el estado actual de prefijos válidos/inválidos en Internet de la misma forma que lo haría un router
- RIPE validating cache
  - http://www.ripe.net/lir-services/resource-management/certification/tools-and-resources
- Otros validadores
  - BBN, rcynic



Origin Validation LG

http://www.labs.lacnic.net/rpkitools/looking_glass

Links / Referencias

- LACNIC's RPKI System
  - http://rpki.lacnic.net
- LACNIC's RPKI Repository
  - rsync://repository.lacnic.net/rpki/
- To see the repository
  - rsync --list-only rsync://repository.lacnic.net/rpki/lacnic/
- RPKI Statistics
  - http://www.labs.lacnic.net/~rpki

Preguntas?

Muchas gracias…