



Enrutamiento seguro con BGP y RPKI

RFI – Facultad de Ingeniería – UDELAR
Montevideo, Uruguay
Carlos Martínez



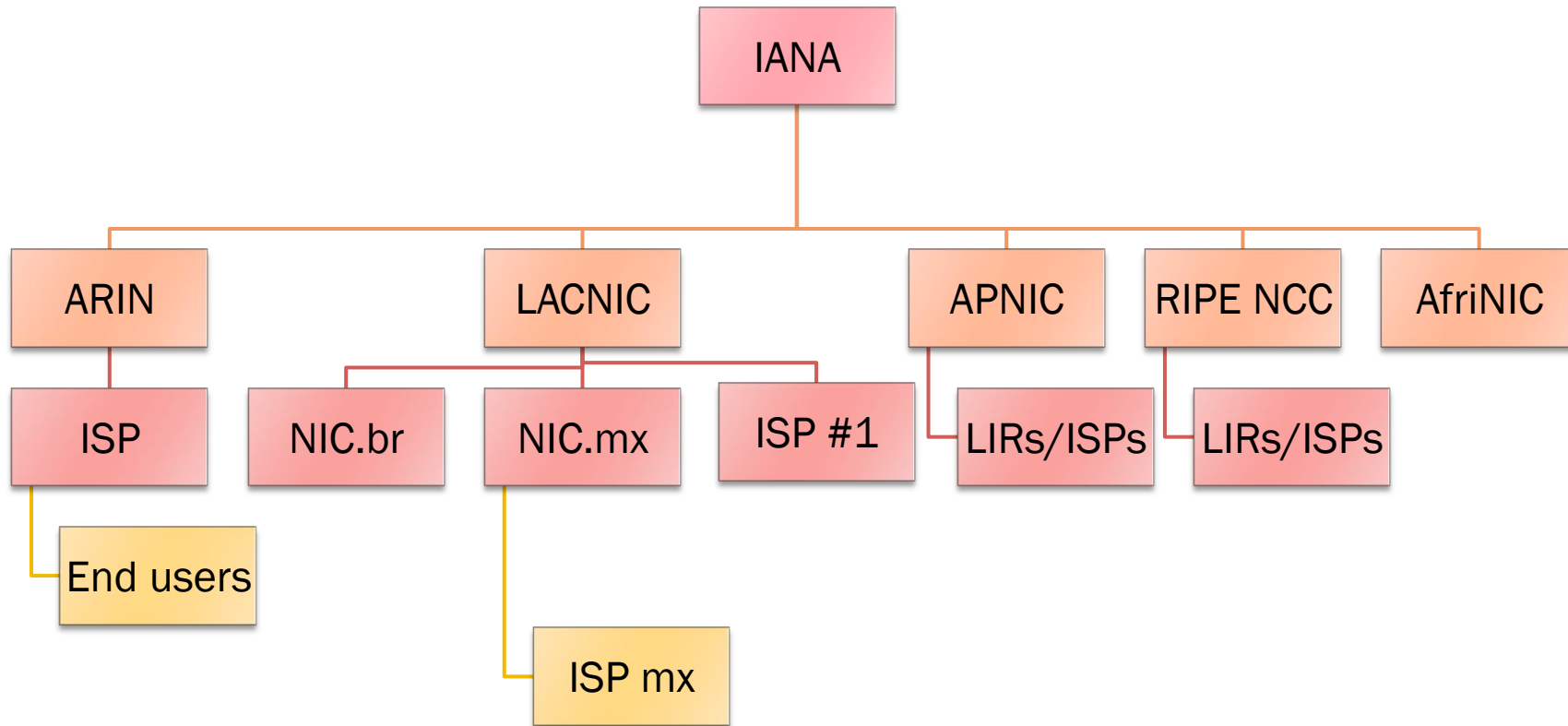
Gestión de recursos en Internet

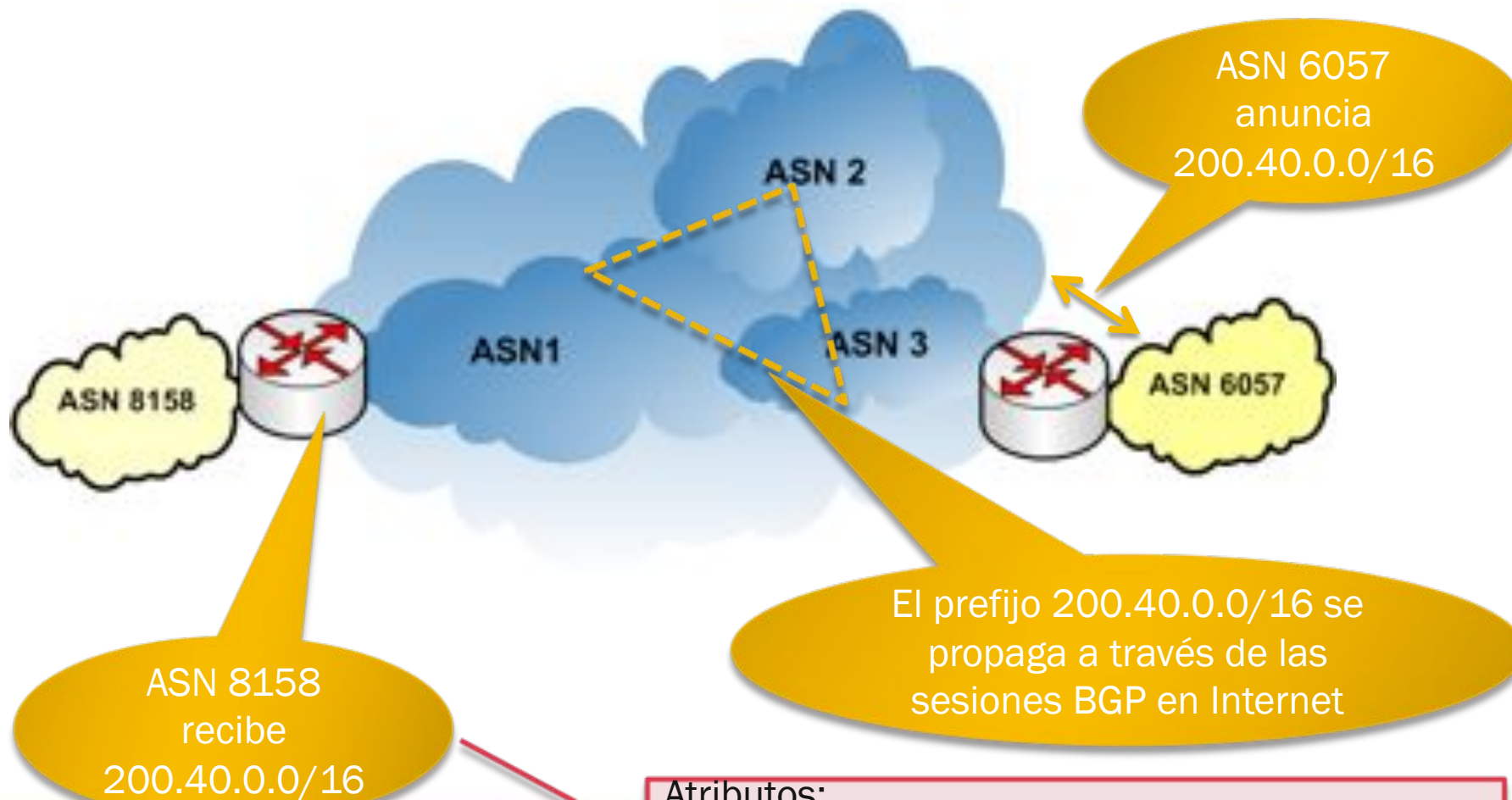
- ▶ Recursos
 - ▶ Direcciones IPv4
 - ▶ Direcciones IPv6
 - ▶ Sistemas autónomos
 - ▶ 16 y 32 bits
- ▶ Documento fundacional: RFC 2050
 - ▶ “*IP Registry Allocation Guidelines*”
- ▶ Cada RIR es **fuente autoritativa de información sobre la relación “usuario” <-> “recurso”**
 - ▶ Cada RIR opera su base de datos de registro
 - ▶ Asociados y RIRs *firman contratos de servicio* entre si





Gestión de recursos en Internet

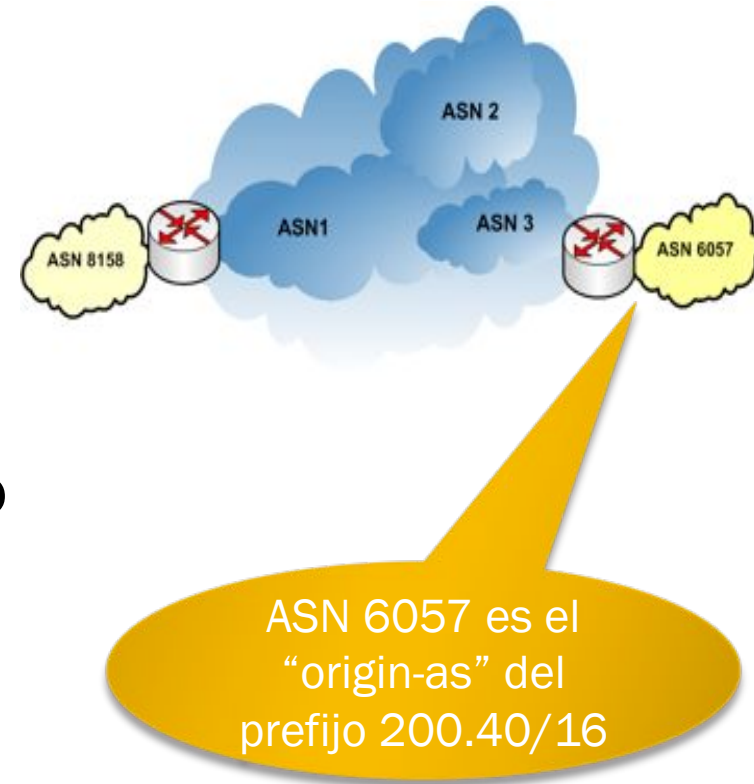




Atributos:

200.40.0.0/16 AS_PATH ASN1 ASN3 ASN6057

- ▶ BGP elige rutas de acuerdo a un **algoritmo de decisión** y a los valores de los **atributos**
- ▶ AS_PATH es la lista de sistemas autónomos recorridos por un UPDATE dado
 - ▶ Incluye el AS que origina el anuncio (“origin-as”)



▶ Algoritmo de decisión de BGP

▶ Fuente <http://netcerts.net/?p=116> :

#	Paso
1	Verificar si NEXT HOP es alcanzable
2	Seleccionar la ruta con el <i>WEIGHT</i> mas alto**
3	Seleccionar la ruta con el LOCAL PREFERENCE mas alto
4	Seleccionar la ruta originada localmente
5	Seleccionar el AS_PATH mas corto
6	Seleccionar el origin code mas bajo (IGP > EGP > Incomplete)
7	Seleccionar el MED mas bajo
8	Seleccionar rutas aprendidas por eBGP (<i>sobre las aprendidas por iBGP</i>)
9	Seleccionar la ruta con la menor metrica IGP al NEXT HOP
10	Seleccionar la ruta mas antigua (AGE)
11	Seleccionar la ruta con el menor Router_ID
12	Seleccionar la ruta con la menor dirección IP si el Router_ID es igual

Paso '2.5':
validación de origen



¿Quién puede usar un recurso?

- ▶ Un ISP al obtener recursos de Internet (IPv6/IPv4/ASN)
 - ▶ Indica a su upstream/peers cuales son los prefijos que va a anunciar
 - ▶ Vía e-mail, formas web, IRR (Internet Routing Registry)
- ▶ Proveedores/peers verifican derecho de uso del recurso y configuran filtros
 - ▶ Whois RIRs: Información no firmada, no utilizable directamente para ruteo
 - ▶ Whois IRR: Información no firmada, pocos mecanismos para autenticación de derecho de uso
- ▶ La verificación no siempre es todo lo meticulosa que debería ser



Verificación de autorización de uso

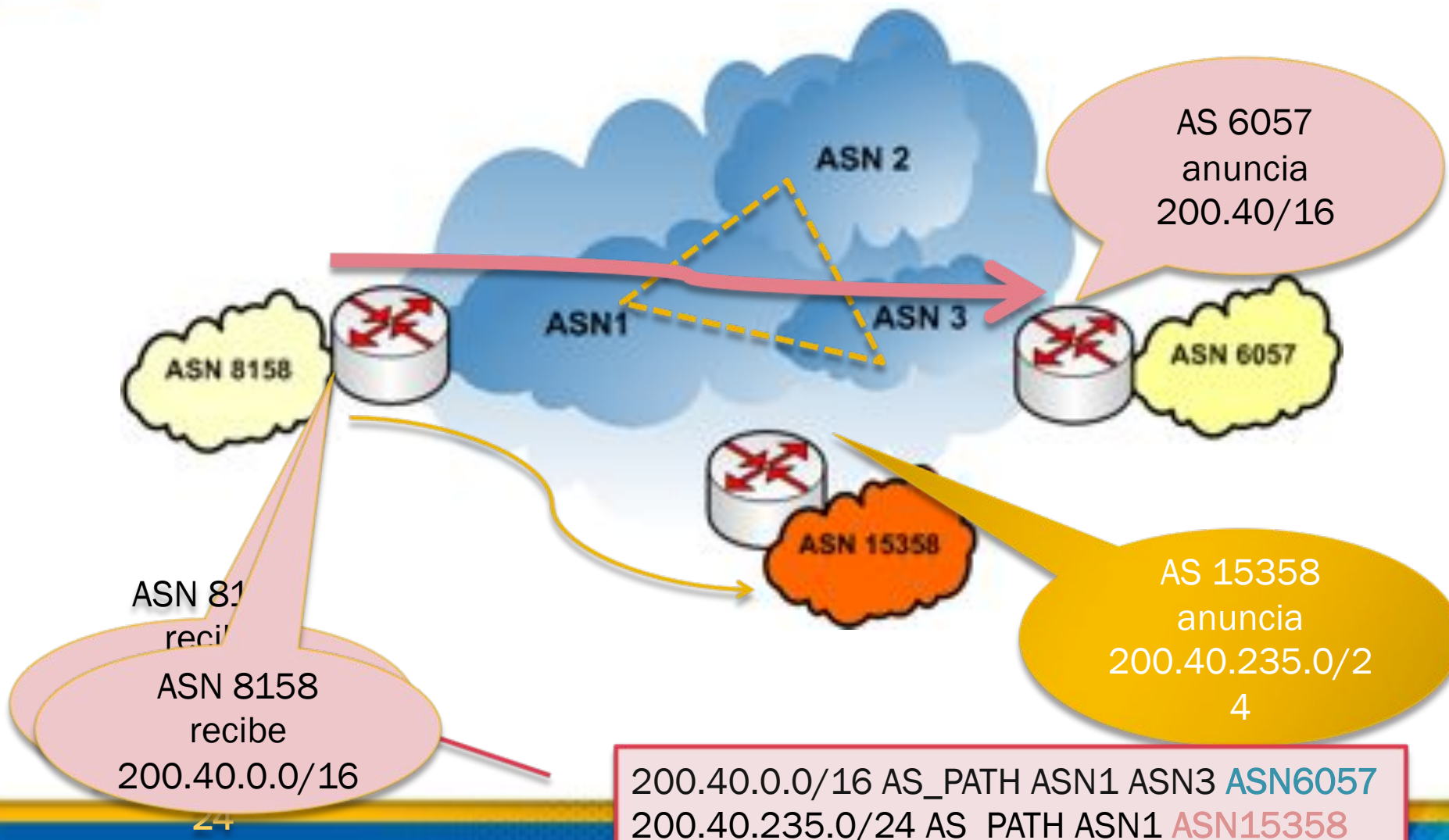
- ▶ Administrador de la red
 - ▶ Controles locales en su infraestructura de rutas
 - ▶ Pedir algún proceso previo (ej. Registrar el objeto en un IRR)
 - ▶ Protección de routers
 - ▶ Integridad de operación en sus protocolos de ruteo
 - ▶ Autenticación entre peers
- ▶ Filtrado de rutas que se saben inválidas
 - ▶ Filtros 1918 (rfc1918) prefijos de redes privadas
 - ▶ "Bogon Filters" espacios no asignados de IANA
- ▶ La integridad del sistema depende de la **confianza entre peers**



Secuestro de rutas

- ▶ Cuando un participante en el routing en Internet anuncia un prefijo que no está autorizado a anunciar se produce un “*secuestro de ruta*” (*route hijacking*)
- ▶ Malicioso u 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)





Infraestructura de PK de recursos

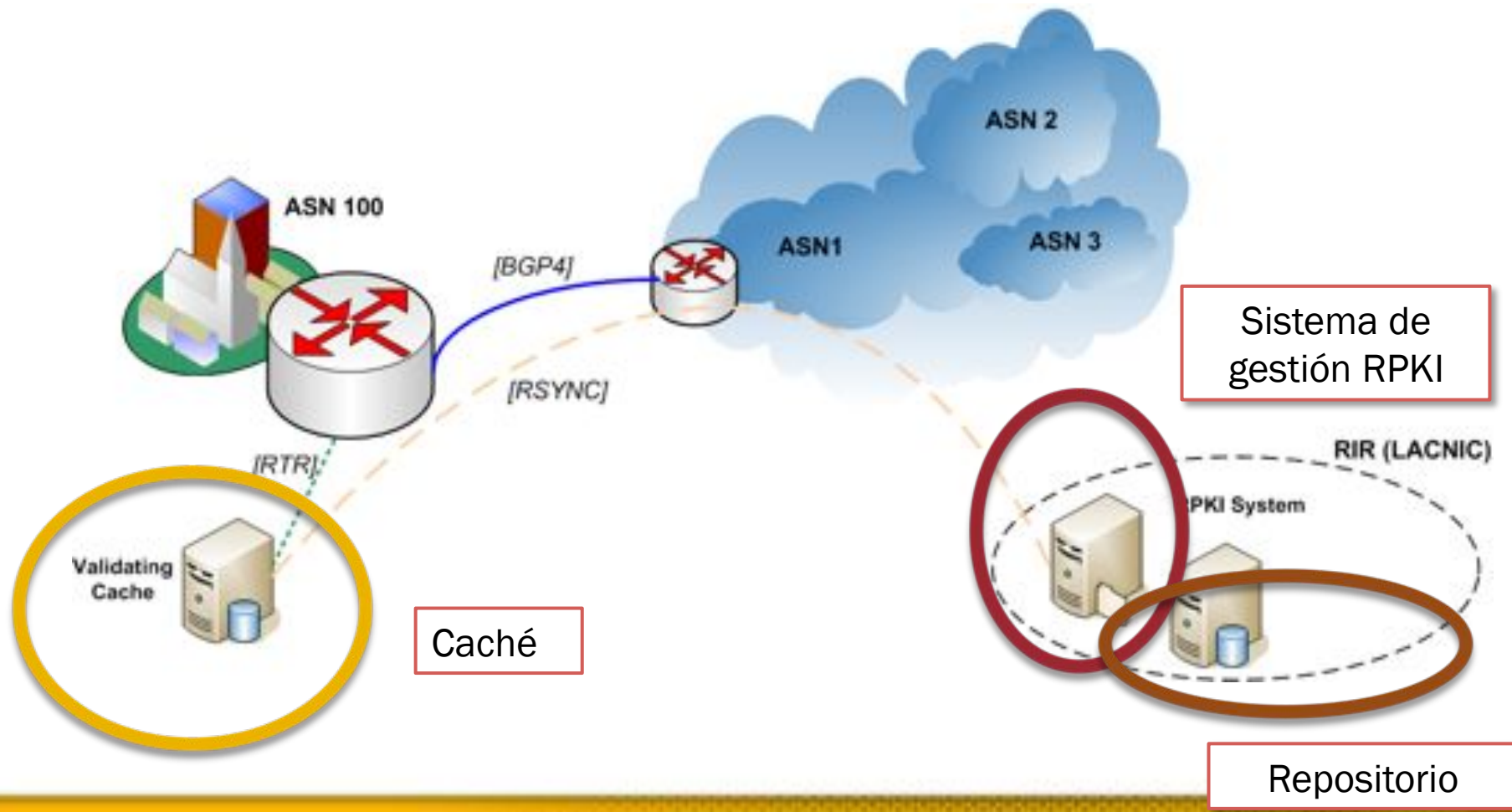
- ▶ Resource Public Key Infrastructure
 - ▶ Objetivo: poder certificar la autorización a utilizar un cierto recurso de Internet
 - ▶ Mecanismo propuesto
 - ▶ Uso de certificados X.509 v3
 - ▶ Uso de extensiones RFC 3779 que permiten representar recursos de Internet (direcciones v4/v6, ASNs)
 - ▶ Mecanismo de validación de prefijos
 - ▶ Esfuerzo de estandarización:
 - ▶ SIDR working group en IETF



Resource PKI (ii)

- ▶ Metodología 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” (ROA)
- ▶ 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

Resource PKI (iii)





Resource PKI (iv)

- ▶ Los objetos firmados son listados en directorios públicos
- ▶ Los objetos pueden ser usados para configurar filtros en routers
- ▶ Proceso de Validación
 - ▶ Los objetos firmados son referenciados al certificado que los generó
 - ▶ Cada certificado tiene una referencia al certificado en un nivel superior
 - ▶ Los recursos listados en un certificado tienen que ser subsets válidos de los recursos de su padre (en el sentido CIDR)
 - ▶ Sigue una cadena de confianza hasta el “trust anchor”, verificando también que los recursos estén contenidos en los recursos del certificado padre



Certificados de recursos

- ▶ **Certificados Digitales X.509**
 - ▶ Información del sujeto, plazo de validez, llave publica, etc
- ▶ **Con extensión:**
 - ▶ RFC 3779 estándar IETF define extensión para recursos internet.
- ▶ **Listado de IPv4, IPv6, ASN asignados a una organización**
- ▶ **OpenSSL 1.0c en adelante implementa RFC 3779**
 - ▶ Hay que habilitarlo a la hora del “./configure” ya que no se compila por defecto

Version
Serial Number
Signature Algorithm
Issuer
Subject
Subject Public Key
Extensions
Subject Information Authority (SIA)
Authority Information Access (AIA)
Addr: 10.10.10.0 Asid: 65535

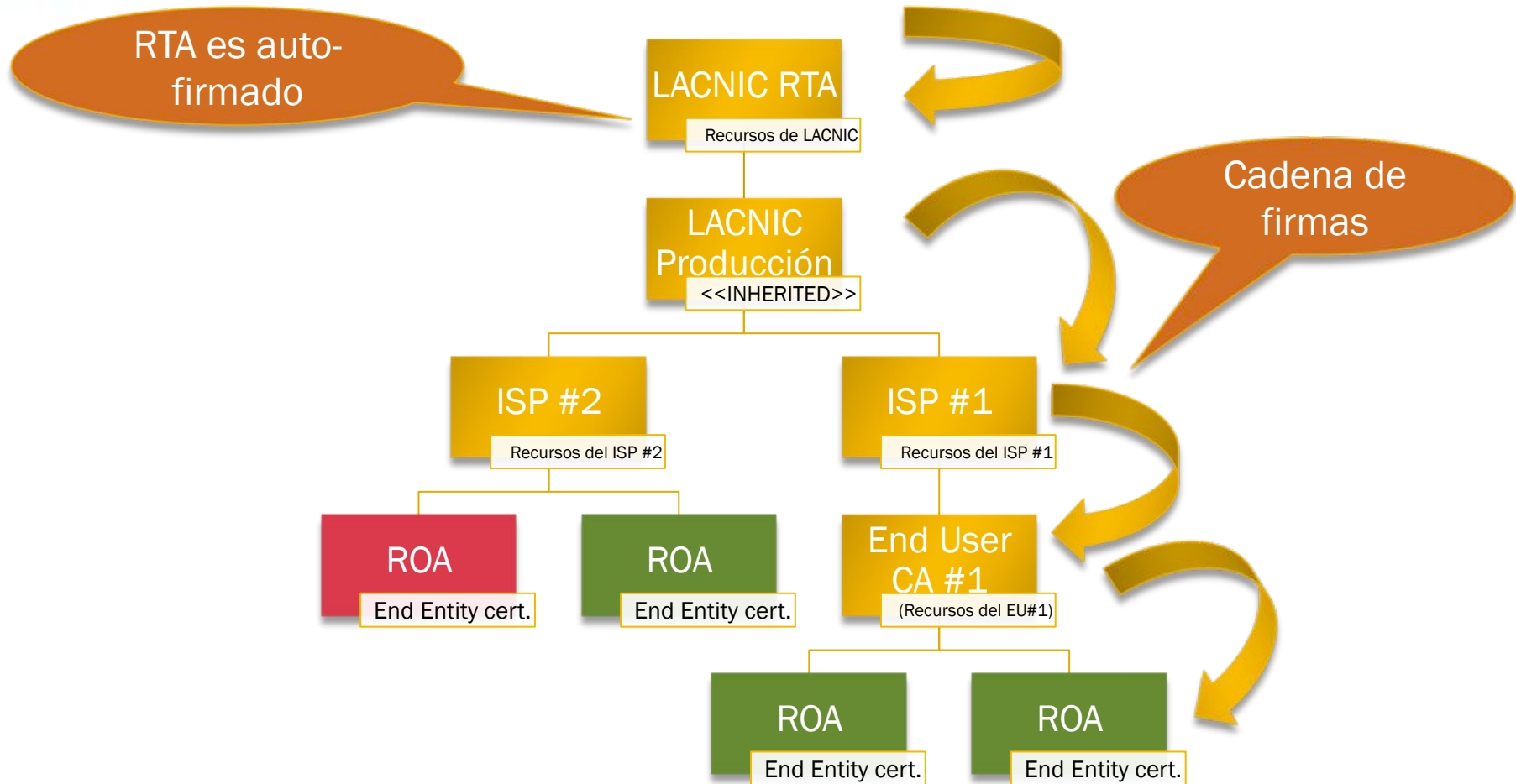


Certificados con extensiones RFC 3779

- ▶ Sección “IP Delegation”
 - ▶ Valor especial “INHERITED”
- ▶ Sección “AS Delegation”
 - ▶ Valor especial “INHERITED”
- ▶ Proceso de validación

Version
Serial Number
Signature Algorithm
Issuer
Subject
Subject Public Key
Extensions
Subject Information Authority (SIA)
Authority Information Access (AIA)
Addr: 10.10.10.0 Asid: 65535

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 de certificados
 - ▶ Repositorio de certificados, CRLs y manifiestos
 - ▶ Accesible via “rsync”
- ▶ Interfaz de gestión
 - ▶ Interfaz web de usuario para aquellos que prefieran el modo “hosted”



Detalles de los certificados

The screenshot shows the 'Certificación de Recursos beta' web interface. The main content area displays the details for the LACNIC CA. The left sidebar contains navigation options for 'Entidades' and 'Gestionar ROAs'. The main content area is titled 'Detalles CA' and lists the following information:

Nombre	LACNIC
Contacto	Latin American and Caribbean IP address
Teléfono	5042222
Ciudad-País	Montevideo - UY
Dirección	Rambla República de México
Tipo	hosted
Último serial	12181
Recursos	A526000-A526002, A526115, A552224, 200.0.88.0/24, 200.3.12.0/22, 200.7.84.0/22, 200.10.60.0/23, 2001:13c7:7001::2001:13c7:7003::/48, 2001:13c7:7010::/48, 2801::/48
Fecha Creación	2005-10-05 12:00:00.0
Fecha Límite	2011-10-05 12:00:00.0

At the bottom of the page, there is a footer with the text 'Registro de Direcciones de Internet para América Latina y Caribe' and the LACNIC logo.



Política de enrutamiento y RPKI

- ▶ ROAs: Routing Origin Authorization
 - ▶ Los ROAs contienen información sobre el origen permitido de un prefijo
 - ▶ Los ROAs se firman utilizando los certificados generados por la RPKI
 - ▶ Los ROAs firmados se copian en un repositorio públicamente accesible

- ▶ Un ROA (simplificado) contiene esta información:

Prefijo	Largo_Máximo	AS Origen	Valido_Desde	Valido_Hasta
200.40.0.0/17	20	6057	2011-01-02	2012-01-01
200.3.12.0/22	24	28000	2011-01-07	2012-01-06

- ▶ Este ROA afirma que:
 - ▶ *“El prefijo 200.40.0.0/17 será anunciado por el sistema autónomo 6057 y podrá ser fraccionado en prefijos de hasta 20 bits de largo. Esto será válido desde el 2 de enero de 2011 hasta el 1 de enero de 2012”*
- ▶ Además
 - ▶ El ROA contiene el material criptográfico que permite **verificar** la validez de esta información contra la RPKI

- ▶ Los ROA contienen
 - ▶ Un certificado End Entity con recursos
 - ▶ Una lista de “route origin attestations”

ROA

End Entity
Certificate

200/8

172.17/16

200.40.0.0/20-24 -> AS 100

172.17.0.0/16-19 -> AS 100

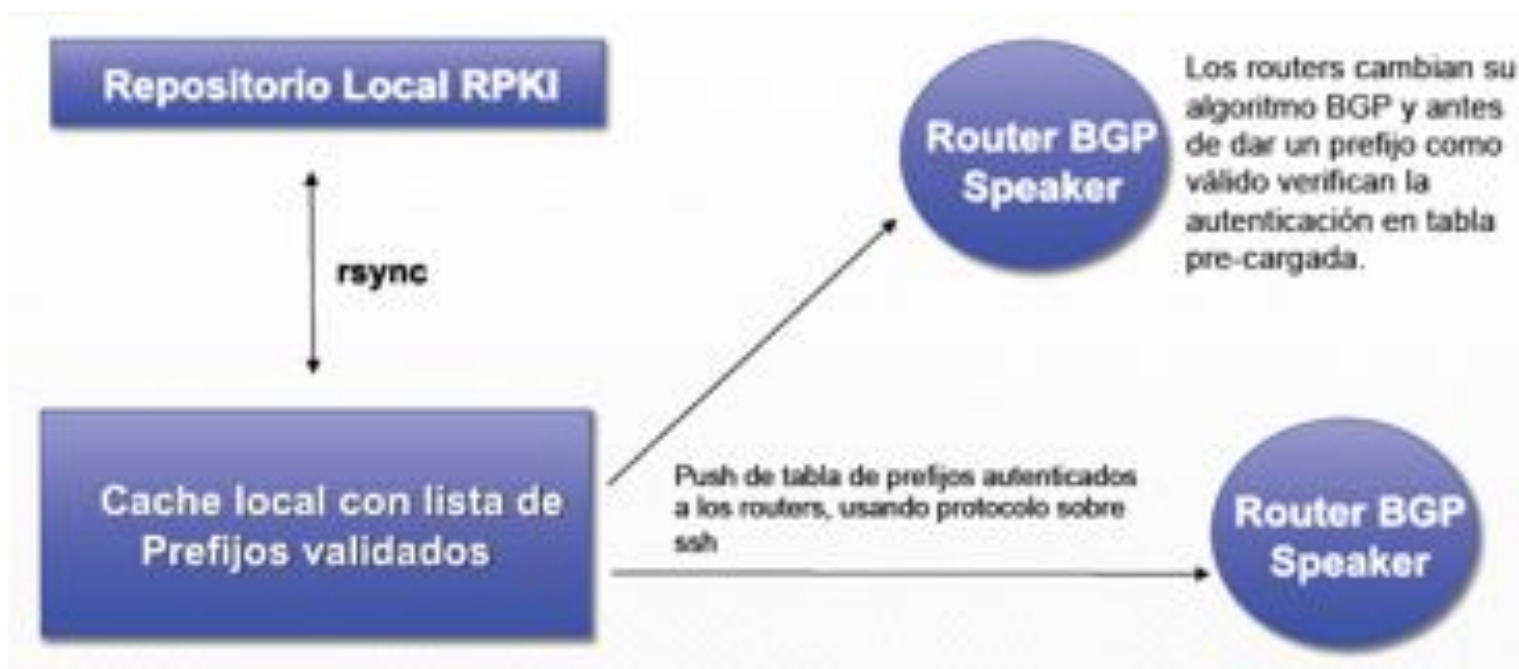


ROAs (iii) - Validación

- ▶ El proceso de validación de los ROAs involucra:
 - ▶ La validación criptográfica de los certificados end entity (EE) que están contenidos dentro de cada ROA
 - ▶ La validación CIDR de los recursos listados en el EE respecto de los recursos listados en el certificado emisor
 - ▶ La verificación de que los prefijos listados en los route origin attestations están incluidos en los prefijos listados en los certificados end entity de cada ROA

ROAs (iv)

- ▶ Un router podría entonces utilizar los ROAs** para validar una ruta y eventualmente, rechazarla
 - ▶ RPKI Routing Protocol



10
2002:2012



Creación de ROA

The screenshot shows the 'Certificación de Recursos beta' web interface. The main content area is titled 'Nuevo ROA' and contains the following form fields:

- Nombre ROA:
- Válido Desde:
- Válido Hasta:
- ASN de origen:
- Prefijo:
- Largo de Prefijo:

Below the form fields, there is a link for 'Ver IPs Autorizadas' and a 'Crear ROA' button. A yellow arrow points from the 'Ver IPs Autorizadas' link to a dropdown menu titled 'Recursos'. The dropdown menu contains the following list of IP ranges:

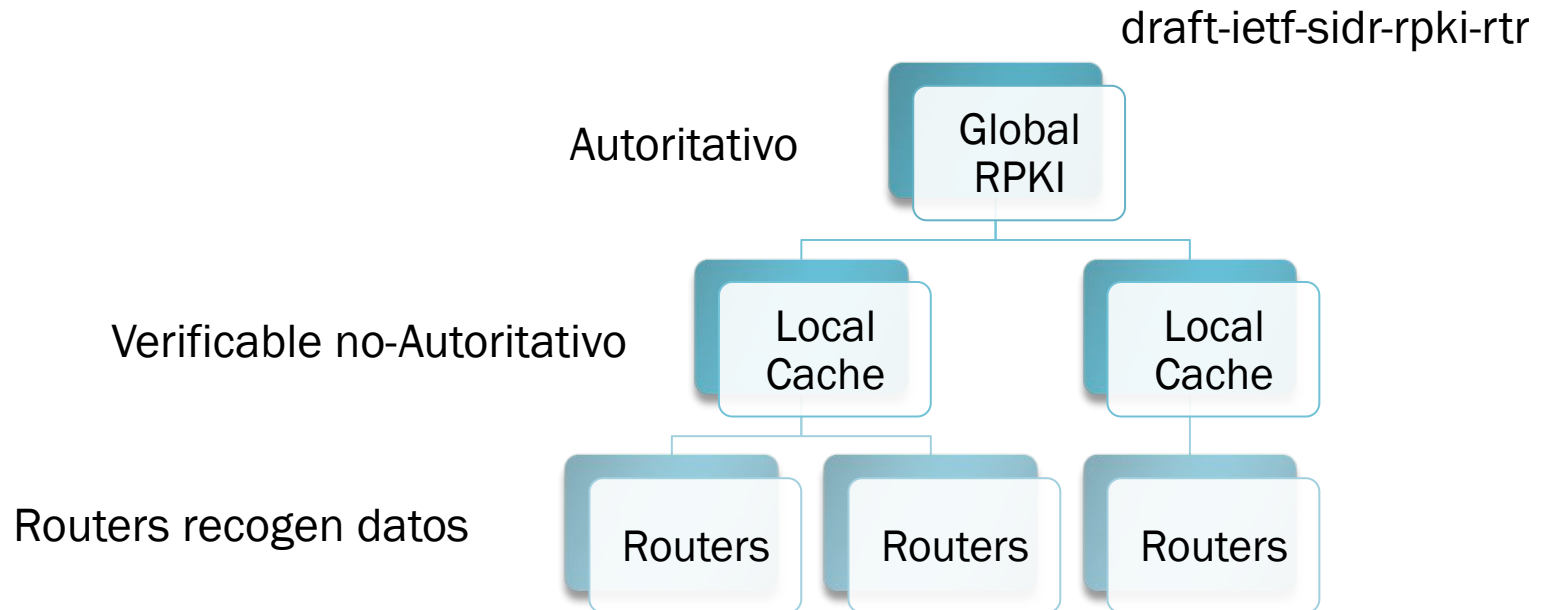
- 200.0.88.0/24
- 200.3.12.0/22
- 200.7.84.0/23
- 200.7.86.0/23
- 200.10.60.0/23
- 2001:13c7:7001::/48
- 2001:13c7:7002::/48
- 2001:13c7:7003::/48
- 2001:13c7:7010::/48



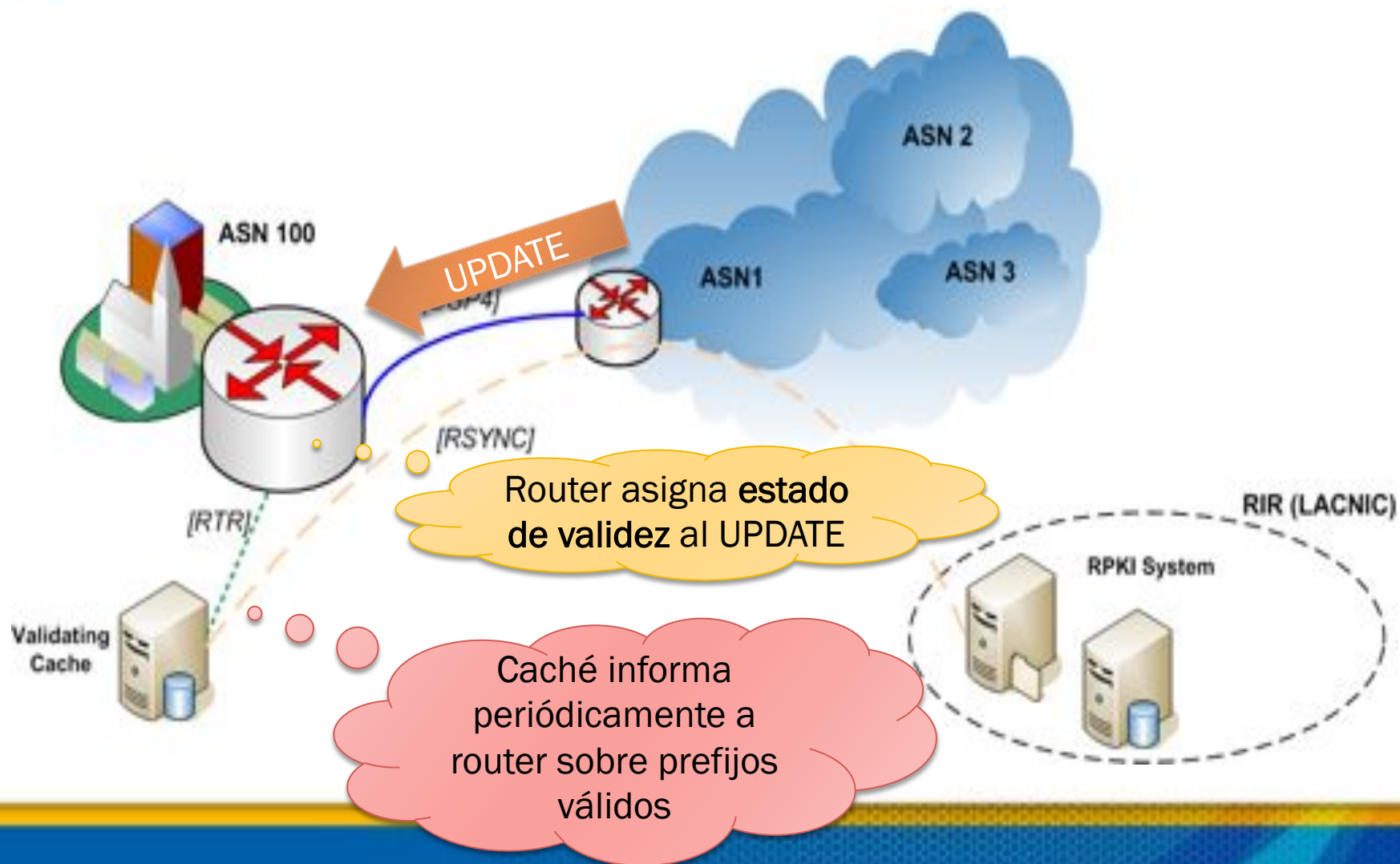
Modos de operación de RPKI

- ▶ Modo “*hosted*”
 - ▶ LACNIC emite los certificados y guarda en sus sistemas tanto claves publicas como privadas
 - ▶ Los certificados son emitidos a pedido de las organizaciones miembro
 - ▶ Los usuarios realizan operaciones via una interfaz web provista por LACNIC
- ▶ Modo “*delegado*”
 - ▶ Una organización tiene su propio certificado, firmado por la CA de LACNIC
 - ▶ La organización envia solicitudes de firma a LACNIC, quien se las devuelve firmadas
 - ▶ Protocolo “up-down”

- ▶ Validar los ASs que originan anuncios de BGP
- ▶ Routers requieren mecanismos simple pero confiable



RPKI en funcionamiento





RPKI en funcionamiento (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 siendo definido en el IETF actualmente



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

Validación de prefijos en el router

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”

Validación de prefijos en el router

UPDATE 200.0.0.0/22
ORIGIN-AS 20

INVALID

	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”

UPDATE 200.0.0.0/22
ORIGIN-AS 66

INVALID

	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”

UPDATE 188.0.0.0/9
ORIGIN-AS 66

NOT FOUND

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”



Interacción con BGP

- ▶ El estado {valid, invalid, not found} de un prefijo puede hacerse pesar en la selección de rutas

```
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
```



Herramientas

- ▶ Validadores
 - ▶ RIPE
 - ▶ <http://labs.ripe.net/Members/agowland/ripe-ncc-validator-for-resource-certification/view>
 - ▶ RCyinc
 - ▶ <http://subvert-rpki.hactrn.net/rcynic/>
 - ▶ BBN Relaying Party Tools
- ▶ Visualización y estadísticas
 - ▶ Construidas sobre la salida de los validadores



RIPE Validator 2.3.x

The screenshot shows the RIPE Validator web interface. The browser address bar displays 'mvuy10.labs.lacnic.net:8080/roas'. The page title is 'RPKI Validator - Validated ROAs'. The navigation menu includes 'Home', 'Trust Anchors', 'ROAs', 'Ignore Filters', 'Whitelist', 'BGP Preview', 'Export', and 'Router Sessions'. The main heading is 'Validated ROAs'. A light blue notification box states: 'Validated ROAs from APNIC RPKI Root, ARIN Test Lab, AfrNIC RPKI Root, LACNIC RPKI Root, RIPE NCC RPKI Root.' Below this, a search bar contains 'LACNIC'. The table shows 10 entries for AS 3549, all with 'LACNIC RPKI Root' as the Trust Anchor. A 'Feedback' button is visible on the left side of the table. At the bottom, pagination controls show '1' selected, and a status message reads 'Showing 1 to 10 of 193 entries (filtered from 2,202 total entries)'.

ASN	Prefix	Maximum Length	Trust Anchor
3549	190.216.0.0/16	21	LACNIC RPKI Root
3549	200.0.194.0/23	23	LACNIC RPKI Root
3549	200.0.196.0/23	23	LACNIC RPKI Root
3549	200.31.0.0/19	24	LACNIC RPKI Root
3549	200.32.64.0/19	24	LACNIC RPKI Root
3549	200.32.96.0/19	19	LACNIC RPKI Root
3549	200.41.0.0/19	23	LACNIC RPKI Root
3549	200.41.32.0/19	24	LACNIC RPKI Root
3549	200.41.64.0/18	24	LACNIC RPKI Root
3549	200.49.0.0/20	20	LACNIC RPKI Root



Validación (iii)

▶ ROAs validados y prefijos (lacnic-roas.csv)

URI,ASN,IP Prefix,Max Length,Not Before,Not After"

```
rsync://repository.lacnic.net/rpki/hosted/d62c58a7-668d-41a6-  
a246-af9400104596/UTt-N3nQ91lGZh0jvWpPN-  
KirQ4.roa",AS28000,200.7.84.0/23,24,2011-01-07  
02:00:00,2012-08-05 03:00:00"
```

```
rsync://repository.lacnic.net/rpki/hosted/d62c58a7-668d-41a6-  
a246-af9400104596/UTt-N3nQ91lGZh0jvWpPN-  
KirQ4.roa",AS28000,2001:13c7:7001::/48,48,2011-01-07  
02:00:00,2012-08-05 03:00:00"
```

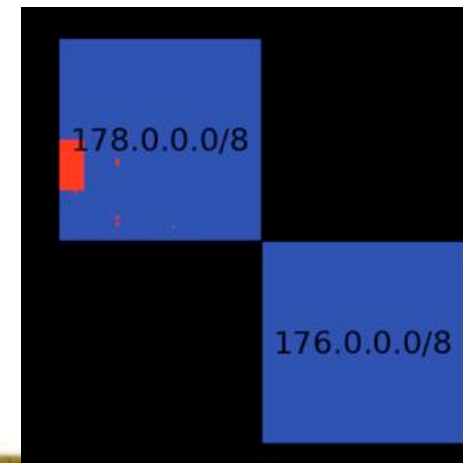
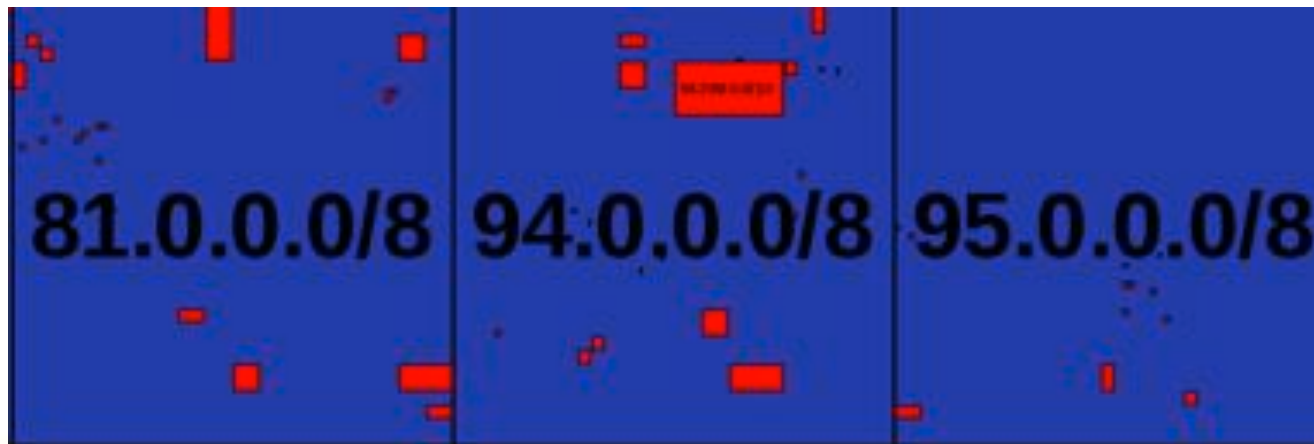
```
rsync://repository.lacnic.net/rpki/hosted/d62c58a7-668d-41a6-  
a246-af9400104596/  
nfNV84A_GA8ZPeCMR4jX1qe557o.roa",AS28001,200.3.12.0/22,24,2011-01-  
-07 02:00:00,2012-08-05 03:00:00"  
rsync://repository.lacnic.net/rpki/hosted/d62c58a7-668d-41a6-  
a246-af9400104596/  
nfNV84A_GA8ZPeCMR4jX1qe557o.roa",AS28001,2001:13c7:7002::/48,48,2  
011-01-07 02:00:00,2012-08-05 03:00:00"
```



Visualizando RPKI

► Fuente:

- <http://www.labs.lacnic.net/~rpki/rpki-heatmaps/latest/>
- Mapas de Hilbert coloreados de acuerdo con el espacio cubierto por ROAs:





Formalización del Protocolo

- ▶ SIDR (Secure InterDomain Routing) Working Group en IETF
- ▶ Architecture, certificate structure and profile, certificate policies, Trust Anchor, Repository structure, ROAs, CP
- ▶ Los documentos mas importantes estan cerca ya del status de RFC
- ▶ <http://tools.ietf.org/wg/sidr/>



Links / Referencias

- ▶ Sistema RPKI de LACNIC
 - ▶ <http://rpki.lacnic.net>
- ▶ Repositorio RPKI LACNIC
 - ▶ `rsync://repository.lacnic.net/rpki/`
- ▶ Para ver el repositorio
 - ▶ `rsync --list-only rsync://repository.lacnic.net/rpki/lacnic/`
- ▶ Estadísticas RPKI
 - ▶ <http://www.labs.lacnic.net/~rpki>



¡Muchas gracias por su
atención!

gerardo_@_lacnic.net
carlos_@_lacnic.net