RPKI

gerardo@lacnic.net
@grada84

BGP
DATOS IMPORTANTES PARA RPKI

- Los **pares** se tienen **confianza**
- Concepto de **ASN de origen**
- Concepto de **ASN PATH**
- En la tabla de enrutamiento se prefieren las **rutas** más **específicas**
- Aparece un ***misterioso*** atributo nuevo “**Estado de validez**”

HIJACKING
DATOS IMPORTANTES PARA RPKI

- Esto no es un problema teorico
  http://bgp.he.net/report/bogons#_bogonsv4asn
- Ya dejaron de ser errores
- Con RPKI clientes y proveedores tendrán mejor protección contra este tipo de ataques

lacnic

CRIPTOGRAFÍA
DATOS IMPORTANTES PARA RPKI

- La firma digital brinda garantías de **integridad y no repudio**
- Toda entidad **certificadora tiene** un **CRL**
- La firma se aplica a cualquier texto, **no todo** lo que se firma **es un certificado, ejemplos ROAs**

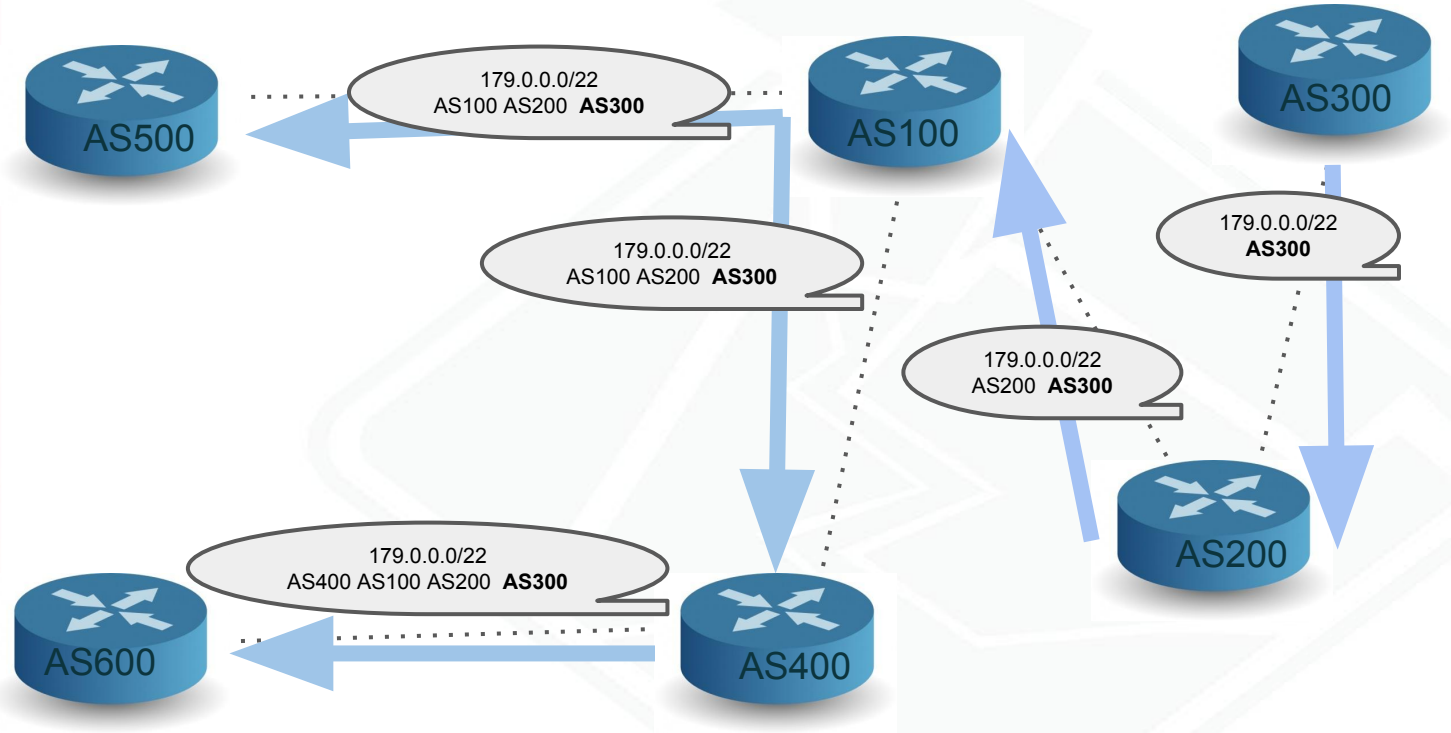
RPKI
DATOS IMPORTANTES

- Construimos ROAs
- Toda la información se publica (CERT, CRL, ROA)
- Toda la información es íntegra, verificable y no repudiable
- Tenemos información **segura** de primera mano sobre quién es el **AS autorizado a originar ruta**

RPKI & BGP

Práctica - Como se calcula la tabla de ruteo?

Update BGP



Quien originó el anuncio del 179/22?

AS 300

Quienes son los vecinos o pares del AS100?

AS 200, AS 400, AS 500

Quienes propagaron la ruta?

AS 200, AS 100, AS 400

Quienes conocen la ruta

TODOS

lacnic

Tabla BGP simplificada

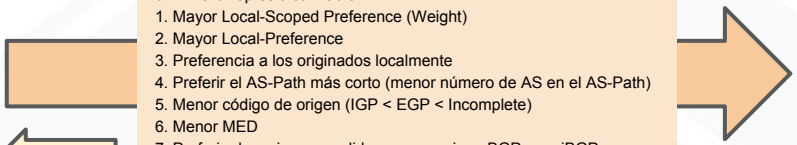
AS100			
Prefijo	Community	Estado Validez	AS PATH
179/22	x	?	AS200 AS300
200.7/20	y	?	AS200
200.107.0/24	z	?	AS400 AS600
8.8/24	x1	?	AS500
98.137/24	y1	?	AS500
179/22	z1	?	AS400 AS300
200.107.0/20	x1	?	AS500 AS300
179/22	y2	?	AS600 AS200 AS300

Tabla Enrutamiento

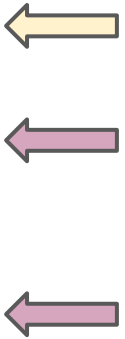
AS100	
Prefijo	AS PATH
179/22	AS200 AS300
200.7/20	AS200
200.107.0/24	AS400 AS600
8.8/24	AS500
98.137/24	AS500
179/22	AS400 AS200 AS300
200.107.0/20	AS500 AS300
179/22	AS600 AS200 AS300

Algoritmo de decisión BGP

0. El next-hop es alcanzable
1. Mayor Local-Scoped Preference (Weight)
2. Mayor Local-Preference
3. Preferencia a los originados localmente
4. Preferir el AS-Path más corto (menor número de AS en el AS-Path)
5. Menor código de origen (IGP < EGP < Incomplete)
6. Menor MED
7. Preferir el camino aprendido por un vecino eBGP a un iBGP.
8. Menor métrica del IGP (el camino más corto al next-hop)
9. Si los anuncios son externos, usar el más antiguo.
9. El camino anunciado por el menor router-id



AS100	
Prefijo	NEXT HOP
179/22	200.7.85.0 (AS200)
200.7/20	179.7.85.0 (AS200)
200.107.0/24	200.7.85.6 (AS400)
8.8/24	8.8.8.0 (AS500)
98.137/24	8.2.7.65(AS500)
200.107.0/20	195.67.43.1(AS500)
...	...
XYZ/N	AS M



Elegimos el AS PATH más corto

Los paquetes se envían a la ruta más específica

RPKI & REPOSITORIO

Práctica - Donde encuentro el material criptográfico?

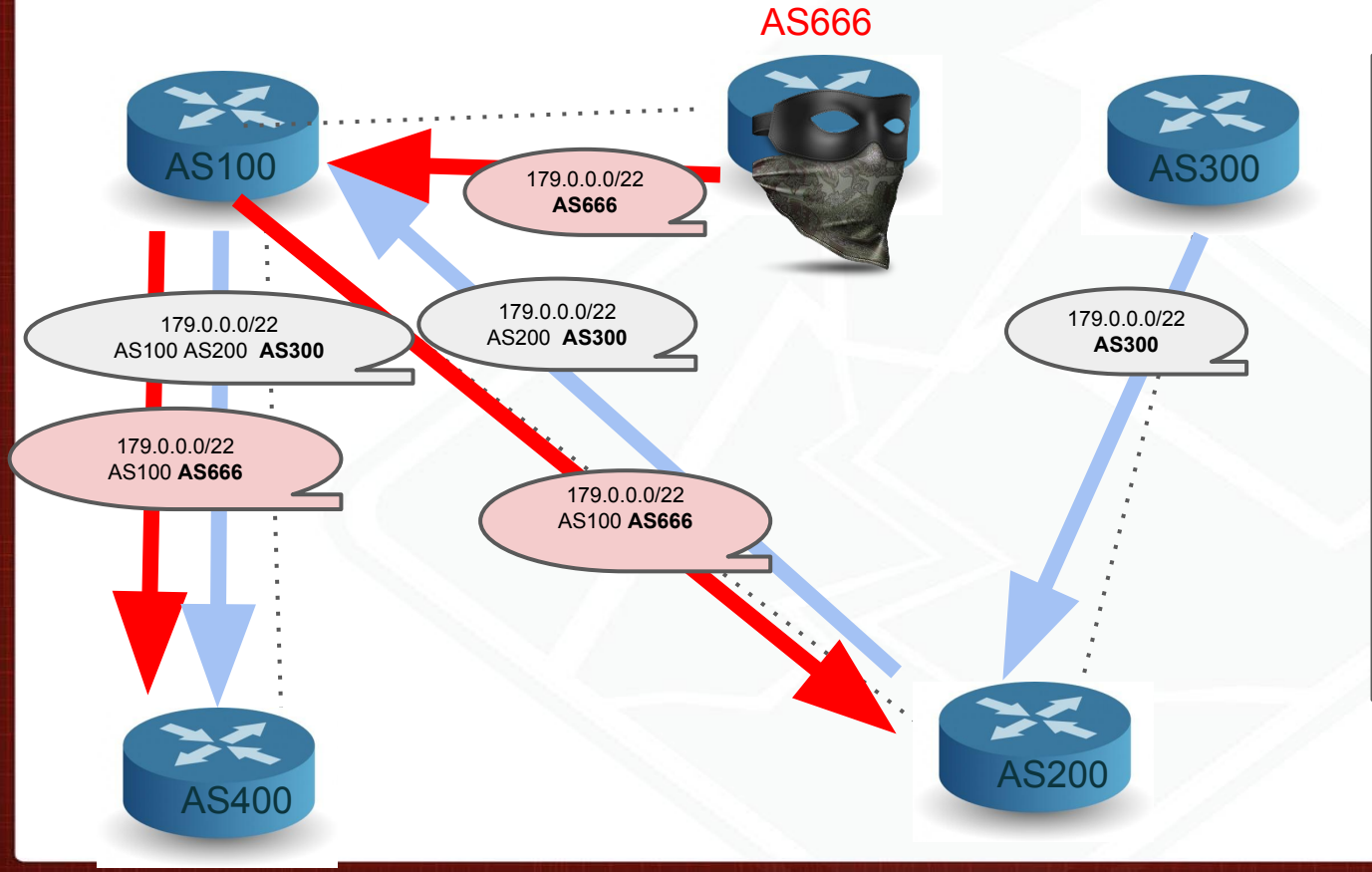
RPKI de LACNIC

Se utiliza rsync
El repositorio de LACNIC es:
rsync://repository.lacnic.net/rpki/

RPKI & HIJACKING

Práctica - Quien se vio afectado?

HIJACKING “CAMINO MÁS CORTO”



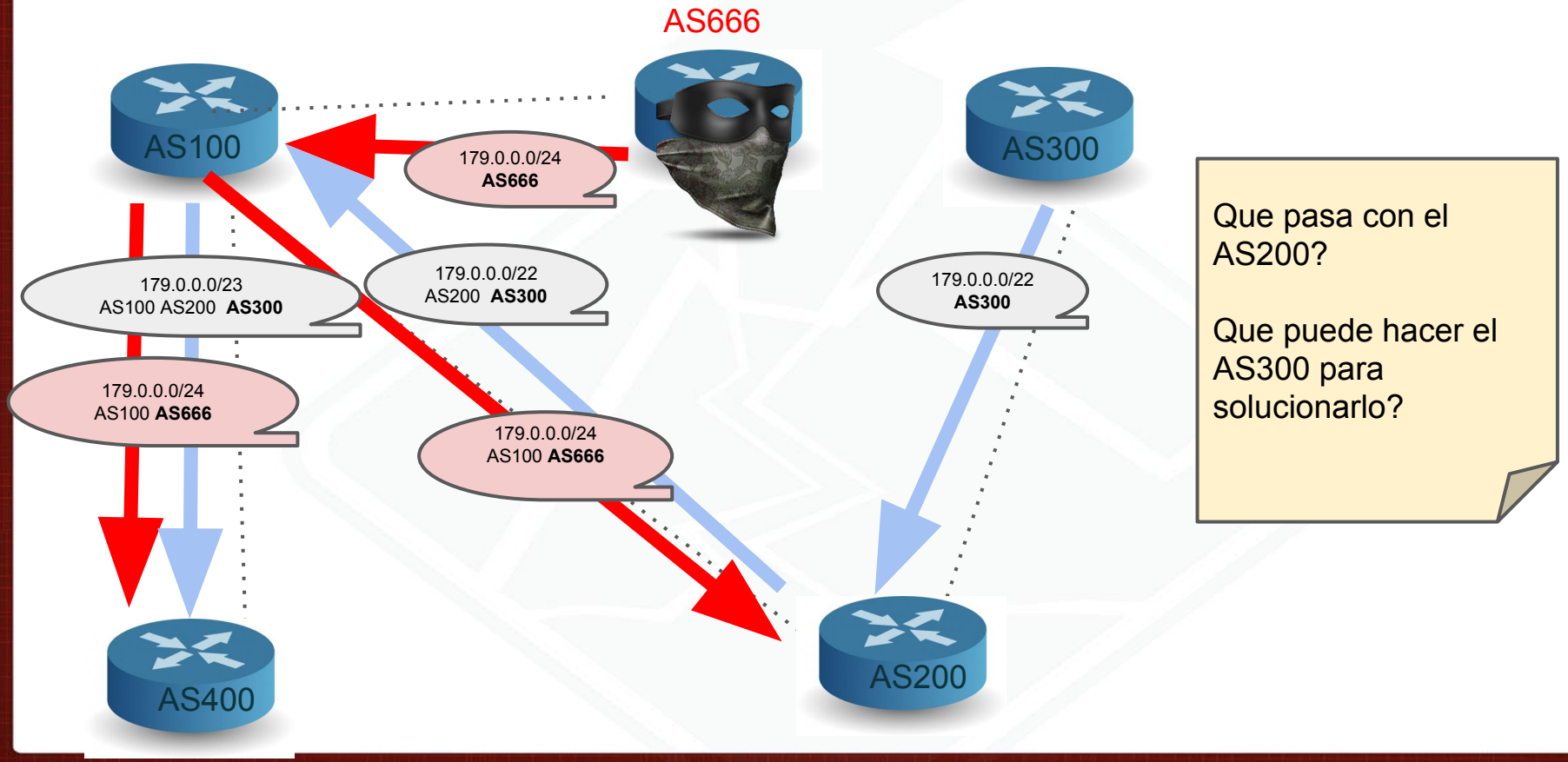
Que pasa con los AS100y AS400?

Que pasa con el AS200?

Como se da cuenta el AS300 que hay un problema?

Que puede hacer el AS300 para solucionarlo?

HIJACKING “RUTA MÁS ESPECÍFICA”



Que pasa con el AS200?

Que puede hacer el AS300 para solucionarlo?

RPKI & CERTIFICADOS

Práctica -Encuentre las diferencias?

CERTIFICADOS DIGITALES

Archivo de texto plano que contiene como principales datos:

- Emisor: Ente certificador
- Receptor: Empresa X
- Serial
- Fechas de validez
- Clave pública del receptor

CERTIFICADOS EN RPKI

Emisor: Certificadora RADA
Receptor: Cliente 1
Serial 123
Fechas de validez XY
Clave pública del receptor: ab
CA: OFF

Emisor: lksndklskndknskls
Receptor: oiuewioewyeuw
Serial 123
Fechas de validez XY
Clave pública del receptor: ab
CA: ON
200.7.85.0/24, AS28000

DIFERENCIAS DE LOS CERT EN RPKI

- No tiene información de identidad
- Posee extensiones específicas donde se pueden incluir direcciones IPv4, IPv6 y ASNs
- BIT CA = ON

RPKI & CERTIFICADOS

Práctica - Veamos un certificado de rpki?

VISOR DE OBJETOS

http://tools.labs.lacnic.net/visor/set

RPKI & CERTIFICADOS

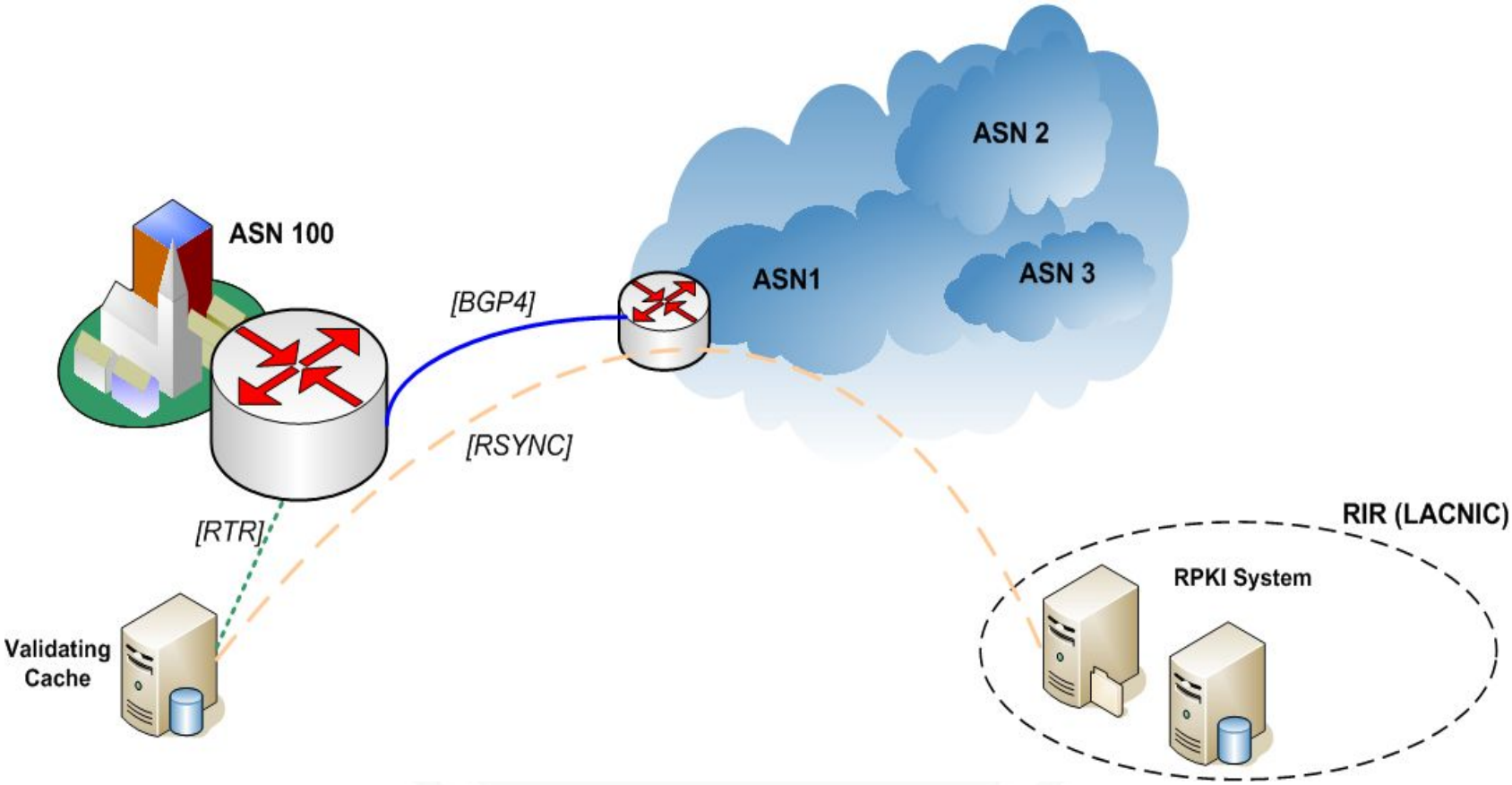
Práctica - Que se valida en un certificado digital?

Que se valida

- Firma
- Fechas de validez
- No aparezca en la Lista de Certificados Revocados
- Que la lista de certificado revocados esté vigente.
- *Coherencia entre manifiestos y publicaciones*
- *Inclusión de recursos*

RPKI & ORIGIN VALIDATION

Práctica - Calculemos el estado de validez


ASN 100
[BGP4]
ASN 2
ASN1
ASN 3
[RSYNC]
[RTR]
RIR (LACNIC)
RPKI System
Validating
Cache

Tablas

BGP				
Prefijo	ASPATH	LP	E de Validez	. . .
			INVALID	
			VALID	
			NOTFOUND	

UPDATE BGP
Entradas en la tabla BGP

Tabla Enrutamiento		
Prefijo	...	NEXT H
200.0.0.0/16	..	100
179.0.0.0/22	..	200
....	...	...

Cache Validador		
Prefijo	MAX	ASN
200.0.0.0/16	20	100
179.0.0.0/22	22	200
....	...	...

Estado de Validez

Se asigna cuando recibimos una actualización BGP, aplicando un algoritmo que consulta el cache validador.

Estado de Validez

NOT FOUND: Si **no hay ninguna entrada** en la lista de prefijos del cache validador que incluya el prefijo que viene en el update BGP

VALID: Si hay **al menos una** entrada en la lista de prefijos del cache validador que incluya el prefijo que viene en el update BGP y **además el ASN coincide y el largo del prefijo es igual o menoR al largo máximo permitido**

INVALID: Si se **encuentran entradas** en la lista de prefijos del cache validador que incluyan el prefijo que viene en el update BGP, pero **no se encuentran ASN que coincidan y/o el largo del prefijo es mayor al largo máximo permitido**

Construcción de la tabla BGP

Cache Validador		
Prefijo	M	ASN
200.0.0.0/16	20	100
179.0.0.0/22	22	200
200.0.0.0/24	24	200
85.0.0.0/20	22	300
85.0.0.0/22	22	300
200.0.0.1/24	32	100

Tabla BGP		
Prefijo	origen	E Validez
200.0.0.0/16	100	Valid
200.0.0.0/24	100	Invalid
200.0.0.0/24	200	Valid
35.0.0.0/20	800	Not found
200.0.0.0/15	600	Not found
85.0.0.0/21	300	Valid
85.0.0.0/24	600	Invalid
179.0.0.0/22	300	Invalid

200.0.0.0/16 origen 100

200.0.0.0/24 origen 100

200.0.0.0/15 origen 600

85.0.0.0/21 origen 300

85.0.0.0/24 origen 600

179.0.0.0/22 origen 300

35.0.0.0/20 origen 800

200.0.0.0/24 origen 200

Qué otras cosas puedo hacer con el Estado de Validez

Reportes,
Estadísticas,
Conocer más nuestra red,
Entender en profundidad como funciona RPKI
Monitoreo, Alertas, Etc

Tabla BGP		
Prefijo	origen	E Validez
x	a	VALID
y	b	VALID
z	c	INVALID
x	a	NOT FOUND
y	b	NOT FOUND
z	c	NOT FOUND

Descartar anuncios

Tabla BGP				
Prefijo	origen	E Validez	LP	COMUNIDAD
x	a	VALID	100	C1
y	b	VALID	100	C1
y	c	VALID	100	C1
DESCARTADA		INVALID	DESCARTADA	
x	a	INVALID	20	C2
y	b	NOT FOUND	50	C3
z	c	NOT FOUND	50	C3
z	d	NOT FOUND	50	C3

RPKI & SISTEMA DE LACNIC

Práctica - Quién en mi empresa puede operar en el sistema de LACNIC?

RPKI de LACNIC

Solo accede el contacto administrativo de LACNIC

Quien es el contacto administrativo?

RPKI & LOOKING GLASS

Práctica - En que estado estan mis anuncios?

ANUNCIOS BGP

http://tools.labs.lacnic.net/announcement/set

http://bgp.he.net/net/

https://rrdp.ripe.net/certification/content/static/validator/rpki-validator-app-2.22-dist.tar.gz

RPKI & ROAS

Práctica - Que ROAS tengo que Crear?

CREACIÓN DE ROAS

http://tools.labs.lacnic.net/roa-wizard/set

RPKI & Sistema de LACNIC

Práctica - Como creo los ROAS?

SISTEMA DE LACNIC

PRODUCCIÓN
https://rpki.lacnic.net
DEMO
http://rpkidemo.labs.lacnic.net/

RPKI & ROA PARTY