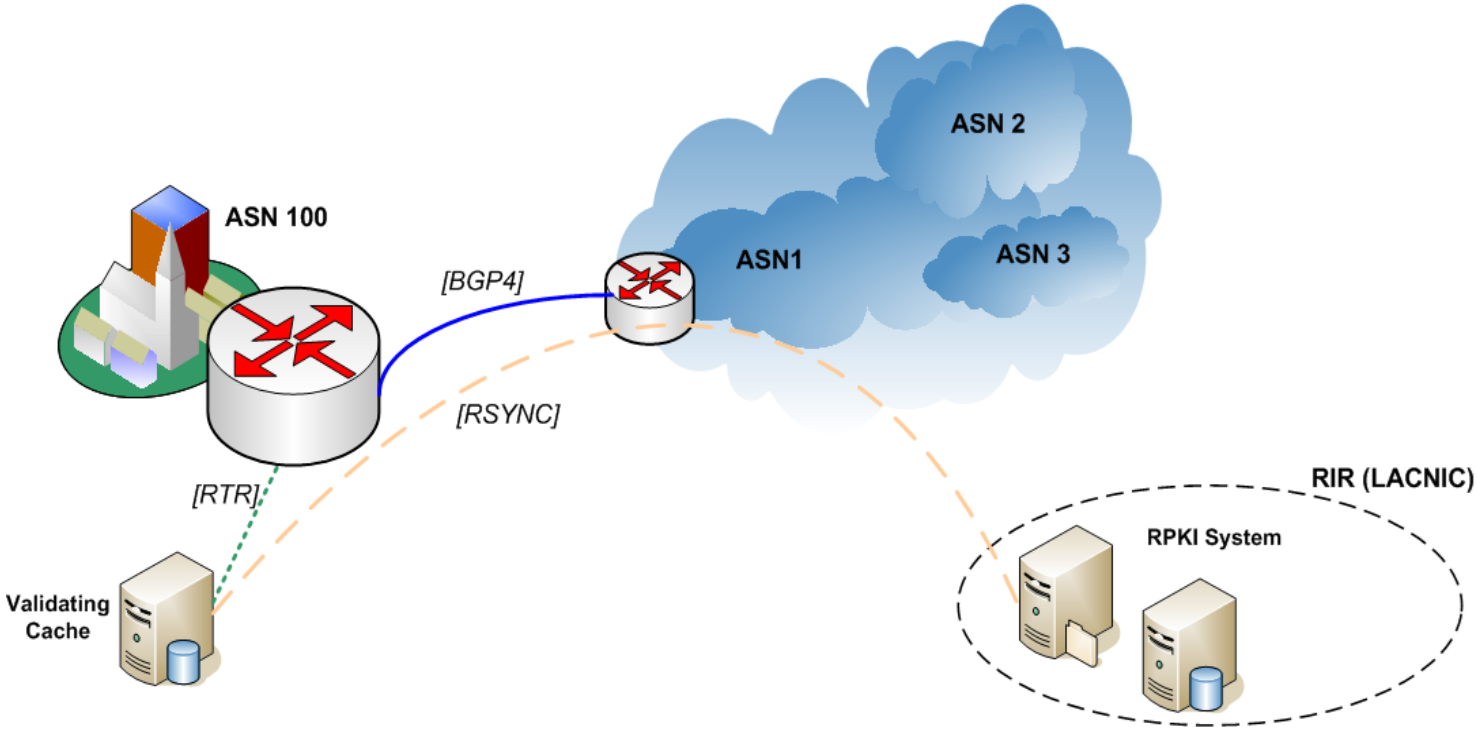
Infraestructura de clave pública para recursos de numeración de Internet



alejandro @ lacnic .net

RPKI

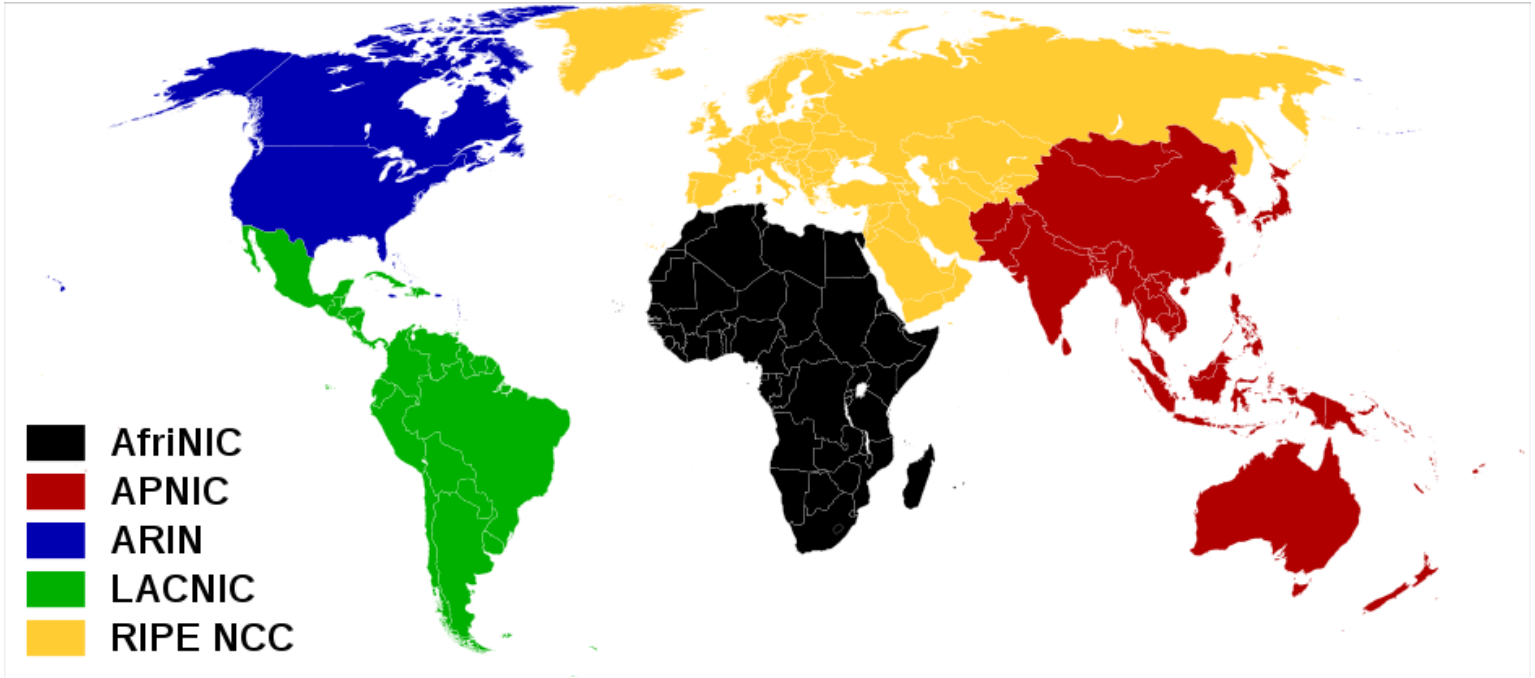
Infraestructura de clave pública para recursos de numeración de Internet

Introducción

RPKI=Resource Public Key Infrastructure

Plataforma tecnológica que permite la implementación de mejoras de seguridad en el sistema de enrutamiento global.

RIRs - Mapa del mundo



DATOS IMPORTANTES PARA RPKI

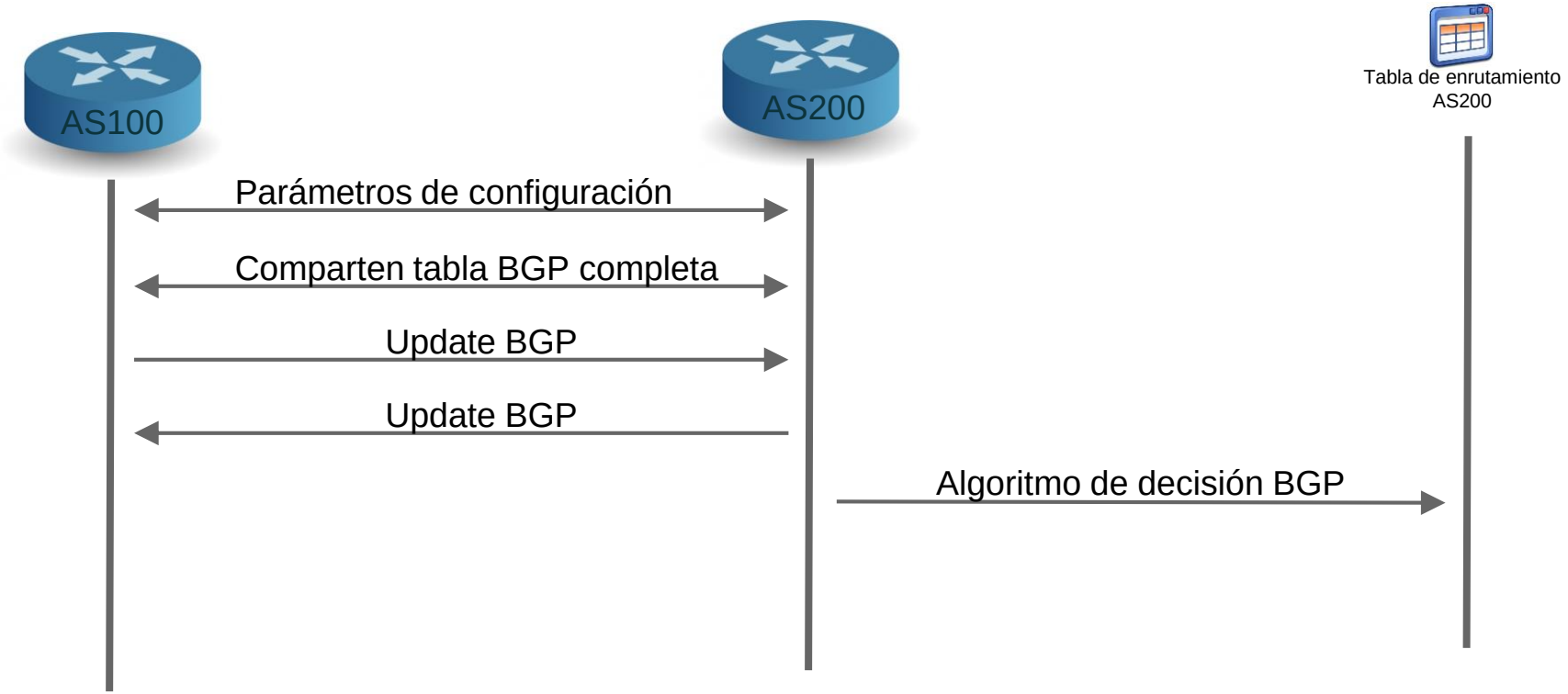
- Estructura jerárquica
- Sub-asignaciones
- RIRs almacenan toda esta información

DATOS IMPORTANTES PARA RPKI

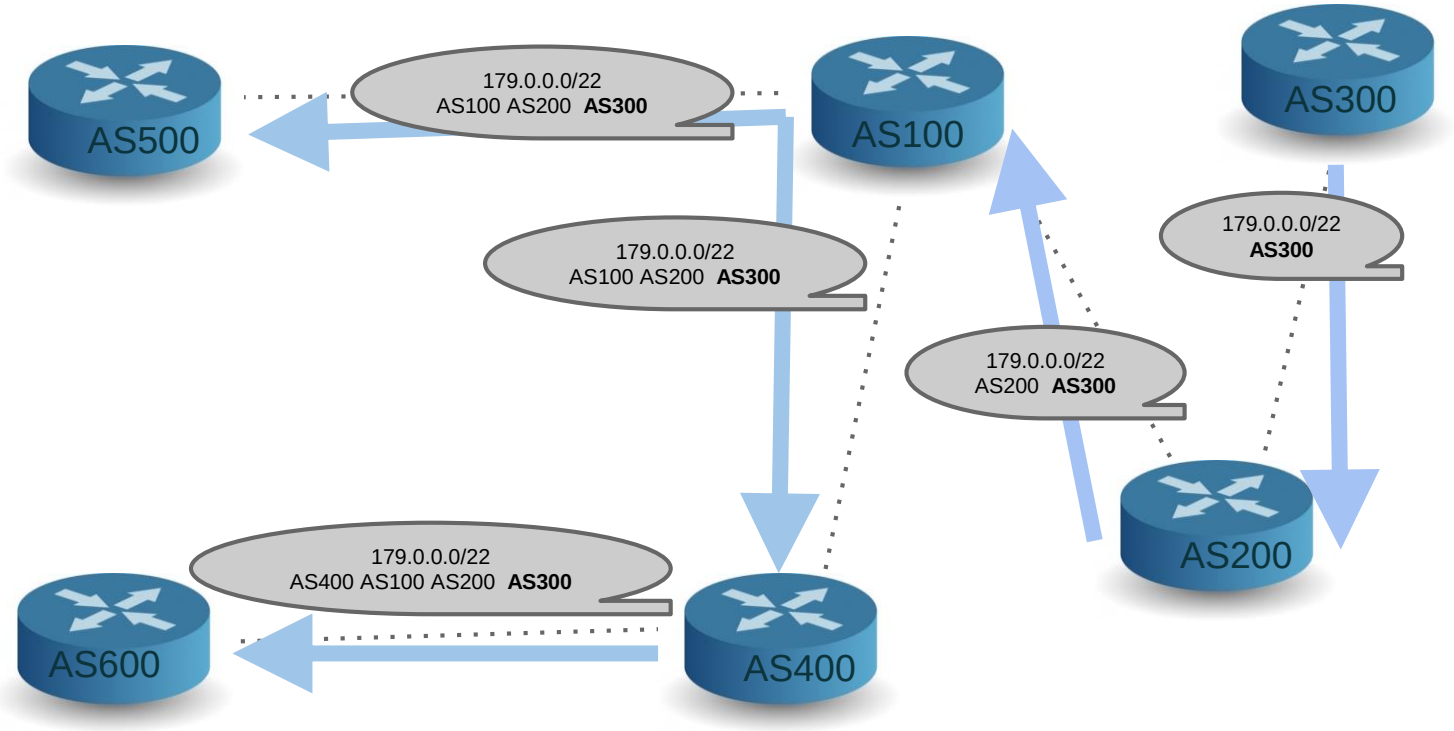
- Esto no es un problema teorico http://bgp.he.net/report/bogons#_bogonsv4asn
- Al desplegar esta tecnologia los clientes y proveedores estarán protegidos contra este tipo de ataques


BGP
HIJACKING
RIR
INTERNET
ORIGEN
DE
RPKI
DE
ASN
ORIGEN
VALIDACION
PKI
PATH

BGP - Funcionamiento de Internet



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 aprendieron la ruta

TODOS

RECORDEMOS QUE:

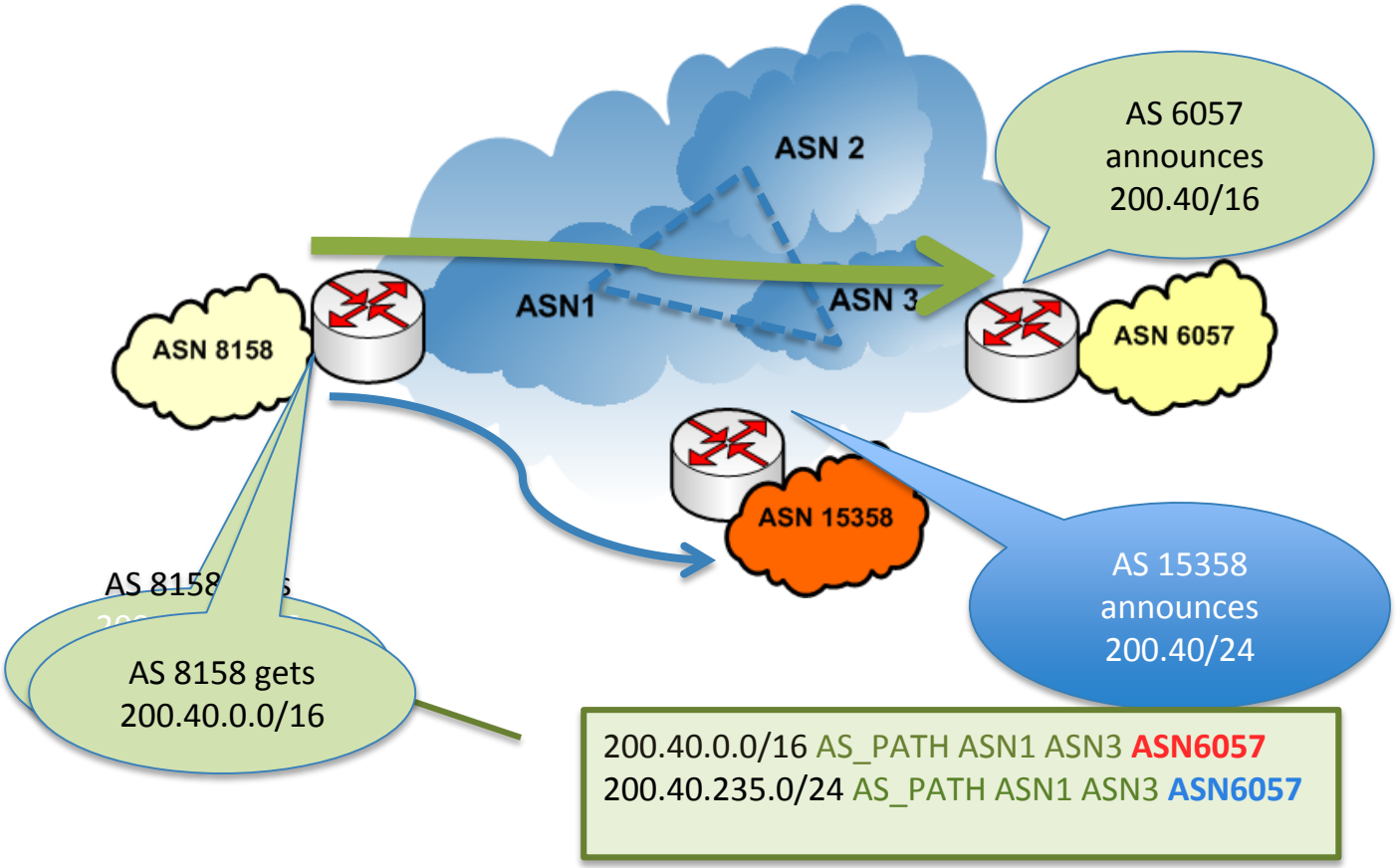
- Los **pares** se tienen **confianza**
- Concepto de **ASN de origen**
- Concepto de **ASN PATH**
- En la tabla de enrutamiento se prefieren las **rutas** más **específicas**
- Aparece un ***misterioso*** atributo nuevo "**Estado de validez**"

CERTIFICADOS DIGITALES

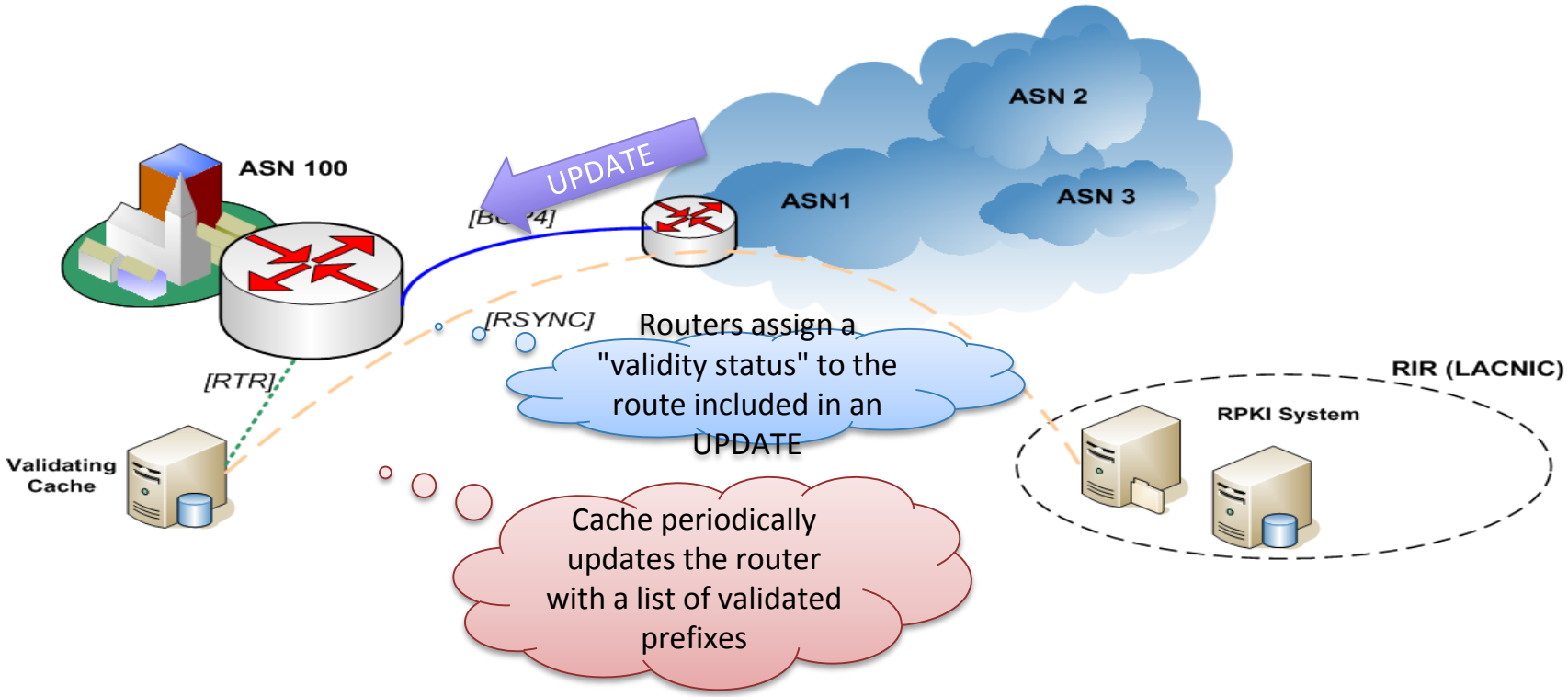
Archivo de texto plano que contiene como principales datos:

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

Route Hijacking (ii)



RPKI in Action



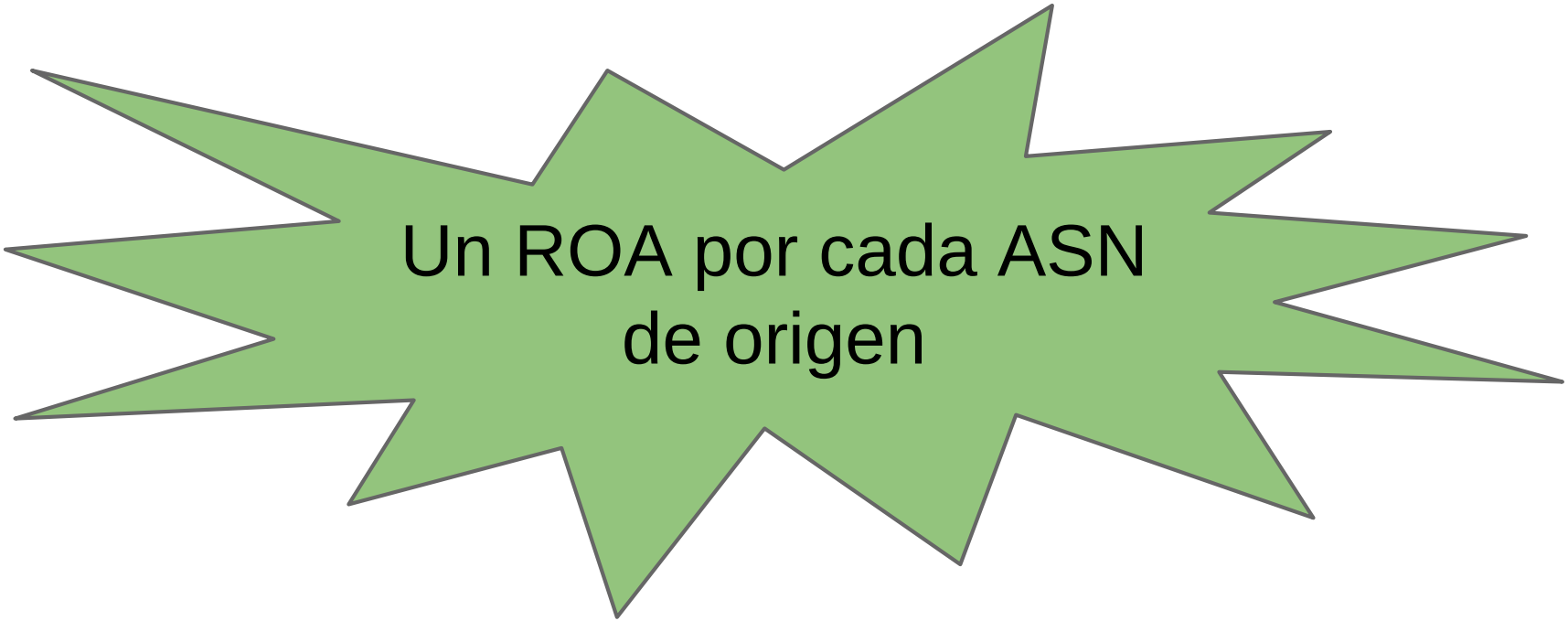
ROA = AUTORIZACIÓN A ORIGINAR RUTAS = TEXTO PLANO CON FORMATO ESPECÍFICO FIRMADO

Es una documento firmado donde se indica cual es ASN autorizado a originar rutas

ROA = TEXTO PLANO CON FORMATO ESPECÍFICO FIRMADO

- ASN
- BLOQUES IP
  - BLOQUE 1 - desagregación máxima
  - BLOQUE 2 - desagregación máxima
  - BLOQUE 3 - desagregación máxima
- FECHA DE VALIDEZ INICIAL
- FECHA DE VALIDEZ FINAL

ROAs - AUTORIZACIÓN A ORIGINAR RUTAS (Route Origin Authorizations)



Q & A