Seguridad en el DNS y en el sistema de ruteo de Internet

Seguridad, estabilidad y resiliencia en la región

Guillermo Cicileo

lacnic 15 años 2002•2017 CONSTRUYENDO COMUNIDAD

Visión de LACNIC

Liderar el fortalecimiento de Una Internet, Abierta, Estable y Segura al servicio del desarrollo de América Latina y el Caribe, impulsando el modelo colaborativo de Internet.

lacnic 15 años 2002•2017 CONSTRUYENDO COMUNIDAD

Estrategia de LACNIC

- Consideramos que una Internet segura y estable es un factor clave para el desarrollo social y económico de la nuestra región
- Entendemos que los aspectos de seguridad y estabilidad tienen una fuerte interrelación
  - Muchas medidas que contribuyen a uno también lo hacen al otro.

Estrategia de LACNIC

- En nuestra visión, la seguridad y estabilidad de Internet no puede ser lograda por una única organización, es necesariamente un objetivo compartido
  - Trabajo conjunto con otras entidades como LAC-IX, LACTLD, ICANN, ISOC, ITU, etc, que convergen en estos objetivos

Programa de Seguridad y Estabilidad

- **Seguridad:**
  - Libre de riesgo y peligro
  - Toma de medidas que prevengan riesgos y peligros
- **Estabilidad:**
  - Permanencia, continuidad en el tiempo
  - Funcionamiento con las mismas características en ausencia de estímulos extraordinaros
- **Resiliencia:**
  - La capacidad de auto-repararse (***self restoration***)

Programa de Seguridad y Estabilidad

Ejes principales:

- Fortalecimiento y protección de infraestructura
- Creación de capacidades humanas
- Difusión, cooperación e investigación

Fortalecimiento de Infraestructura

- SSR en enrutamiento
  - Proyecto de Certificación de Recursos (RPKI)
  - Apoyo a los puntos de intercambio de tráfico (IXP)
- Seguridad en el DNS
  - Despliegue de DNSSEC a nivel de la resolución **reversa**
  - Programa +Raíces, despliegue de copias de servidores raíz del DNS en nuestra región
- Despliegue de IPv6
  - Una Internet estable debe poder crecer sin restricciones técnicas

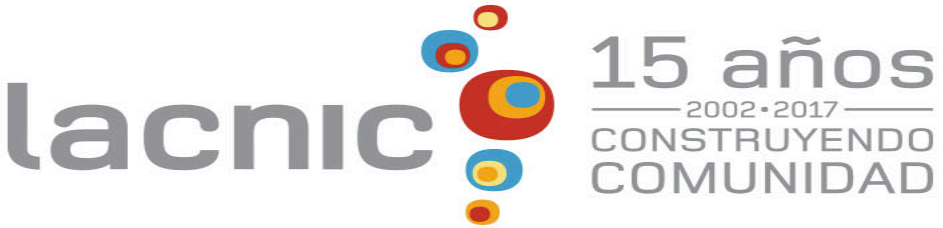
Creación de capacidades humanas

- Cursos de capacitación virtuales y presenciales
  - DNSSEC
  - Enrutamiento con BGP y RPKI
  - Despliegue de IPv6
  - Talleres para IXPs
- Talleres sobre creación de grupos de respuesta a incidentes de seguridad (CSIRTs)
  - Talleres AMPARO

Difusión, cooperación e investigación

- Colaboración con otras organizaciones en diferentes actividades
- Generación de reportes y estadísticas
- LACNIC WARP, http://warp.lacnic.net
  - Servicio de mediación de incidentes *(incident brokering)*
  - Nos apoyamos en la fuerte relación que tenemos con nuestros miembros para hacerles llegar información sobre potenciales incidentes de seguridad que LACNIC recibe por otras vías

Conceptos de DNSSEC



La importancia del DNS

- En cada comunicación entre aplicaciones TCP/IP es necesario obtener la dirección IP del extremo remoto
- Los seres humanos no podemos memorizar millones de direcciones IP (especialmente direcciones IPv6)
- A grandes rasgos: El Sistema de Nombres de Dominio provee a las aplicaciones distintos tipos de recursos (domain name servers, mail exchangers, reverse lookups, …)

DNS

- Permite asociar direcciones IP con nombres de dominio
  - 192.0.2.3 a www.example.net
- Inversamente:
  - www.example.net ---> 192.0.2.3
- Trabaja a traves de consultas y respuestas a traves de "Registros"

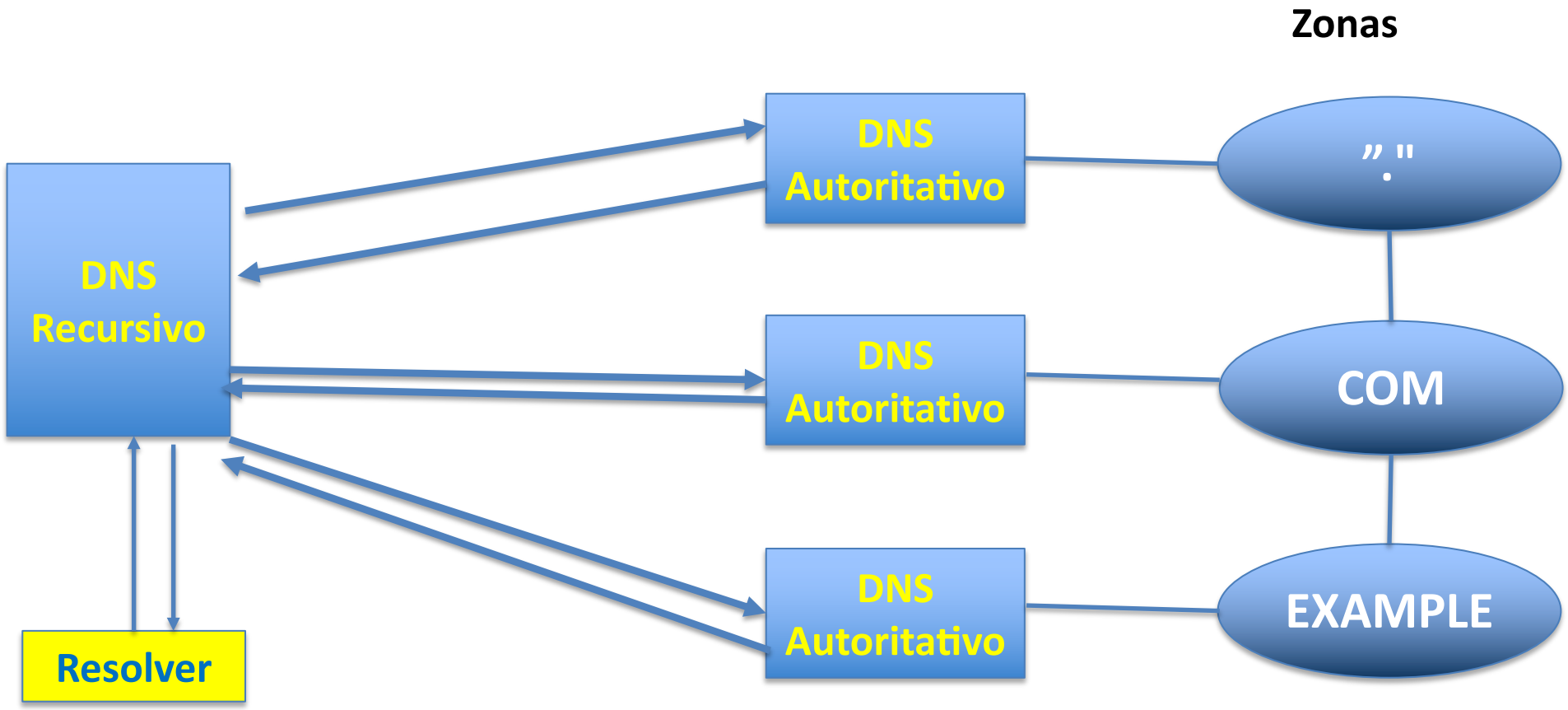
Registros del Servidor de DNS

- Tipos de Resource Records – RR:
  - A : Mapean un nombre a una dirección IPv4
  - AAAA: Mapean un nombre a una dirección IPv6
  - NS : Indican qué servidor responde por qué dominio
  - PTR : Mapean una representación de dirección IPv4 a un nombre (in-addr.arpa)
  - Entre otros..

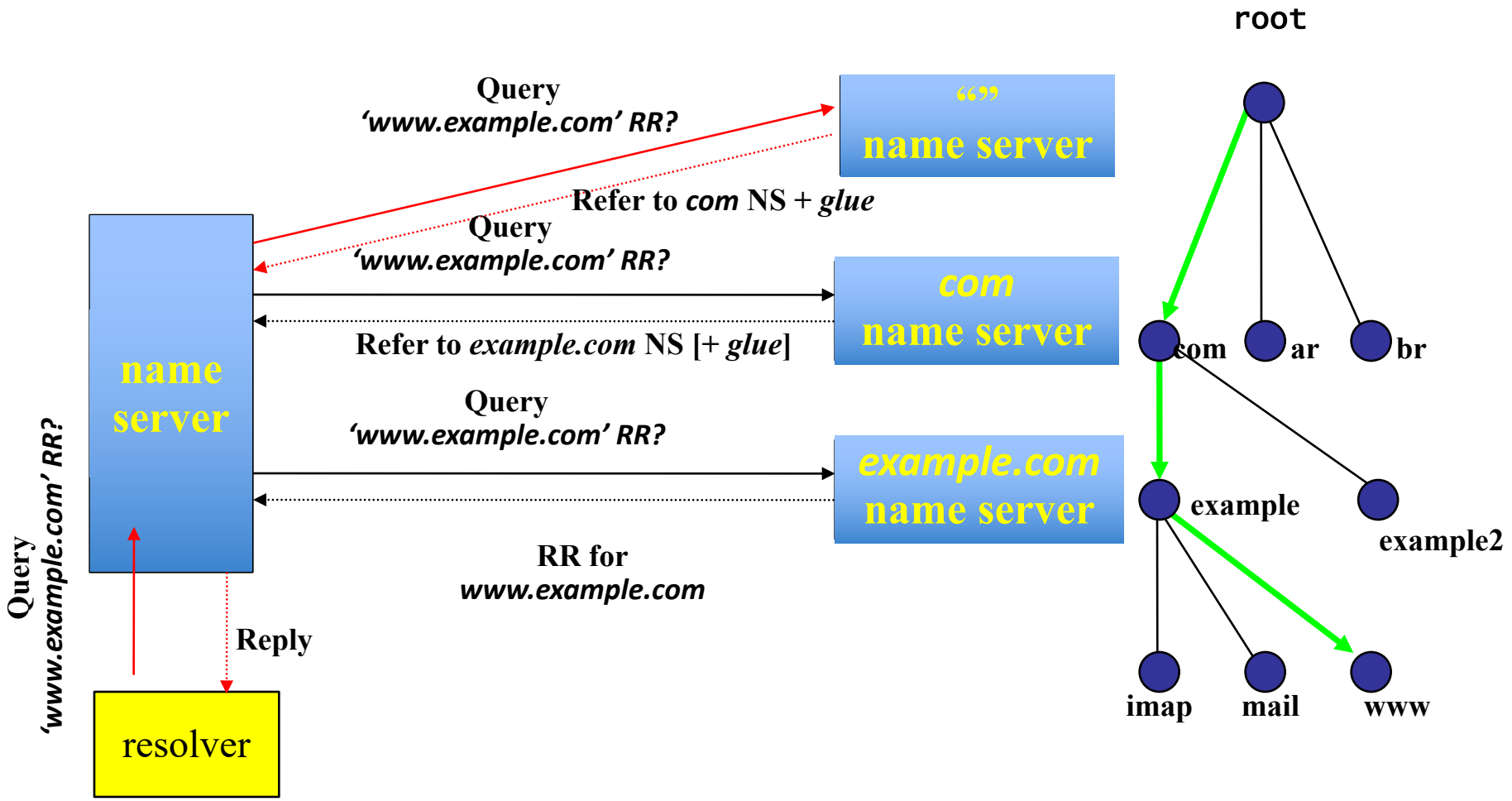
Tipos de name server

- RFC7719:
  - **Resolver**: A program "that extract[s] information from name servers in response to client requests." (Quoted from [RFC1034], Section 2.4) "The resolver is located on the same machine as the program that requests the resolver's services, but it may need to consult name servers on other hosts." (Quoted from [RFC1034], Section 5.1) A resolver performs queries for a name, type, and class, and receives answers. The logical function is called "resolution". In practice, the term is usually referring to some specific type of resolver (some of which are defined below), and understanding the use of the term depends on understanding the context.
  - **Recursive mode:** A resolution mode of a server that receives DNS queries and either responds to those queries from a local cache or sends queries to other servers in order to get the final answers to the original queries. Section 2.3 of [RFC1034] describes this as "The first server pursues the query for the client at another server". A server operating in recursive mode may be thought of as having a name server side (which is what answers the query) and a resolver side (which performs the resolution function). Systems operating in this mode are commonly called "recursive servers". Sometimes they are called "recursive resolvers". While strictly the difference between these is that one of them sends queries to another recursive server and the other does not, in practice it is not possible to know in advance whether the server that one is querying will also perform recursion; both terms can be observed in use interchangeably.
  - **Authoritative server:** "A server that knows the content of a DNS zone from local knowledge, and thus can answer queries about that zone without needing to query other servers." (Quoted from [RFC2182], Section 2.) It is a system that responds to DNS queries with information about zones for which it has been configured to answer with the AA flag in the response header set to 1. It is a server that has authority over one or more DNS zones. Note that it is possible for an authoritative server to respond to a query without the parent zone delegating authority to that server. Authoritative servers also provide "referrals", usually to child zones delegated from them; these referrals have the AA bit set to 0 and come with referral data in the Authority and (if needed) the Additional sections.

Resolver, recursivo y autoritativo



Búsqueda DNS



Vulnerabilidades del DNS

- La información transmitida puede ser falsificada
  - Entre master y slave (AXFR)
  - Entre el master y los resolvers clientes
- El protocolo DNS no permite validar la información contenida en una respuesta
  - Es por lo tanto vulnerable a ataques de ”poisoning” y ”spoofing”
  - Los datos ”envenenados” seguirán causando problemas por un tiempo (TTL)
- Tampoco los secundarios tienen forma de autenticar al primario con el que están hablando

¿Qué protección brinda DNSSEC?

- Proporciona un mecanismo para poder validar la autenticidad y la integridad de los datos contenidos en una zona DNS
  - **DNSKEY/RRSIG/NSEC**
- Proporciona un mecanismo para establecer cadenas de confianza
  - **DS**
- Proporciona un mecanismo para autenticar las transferencias de zona entre primarios y secundarios
  - **TSIG**

DNSSEC

- Es un conjunto de extensiones al protocolo DNS tal como lo conocemos
- Cambios en el "*wire protocol*" (EDNS0)
  - Extensión del tamaño máximo de una respuesta UDP de 512 a 4096 bytes
- Agregado de nuevos *resource records*
  - RRSIG, DNSKEY, DS, NSEC (3)
- Agregado de nuevos flags
  - Checking Disabled (CD)
  - Authenticated Data (AD)

DNSSEC

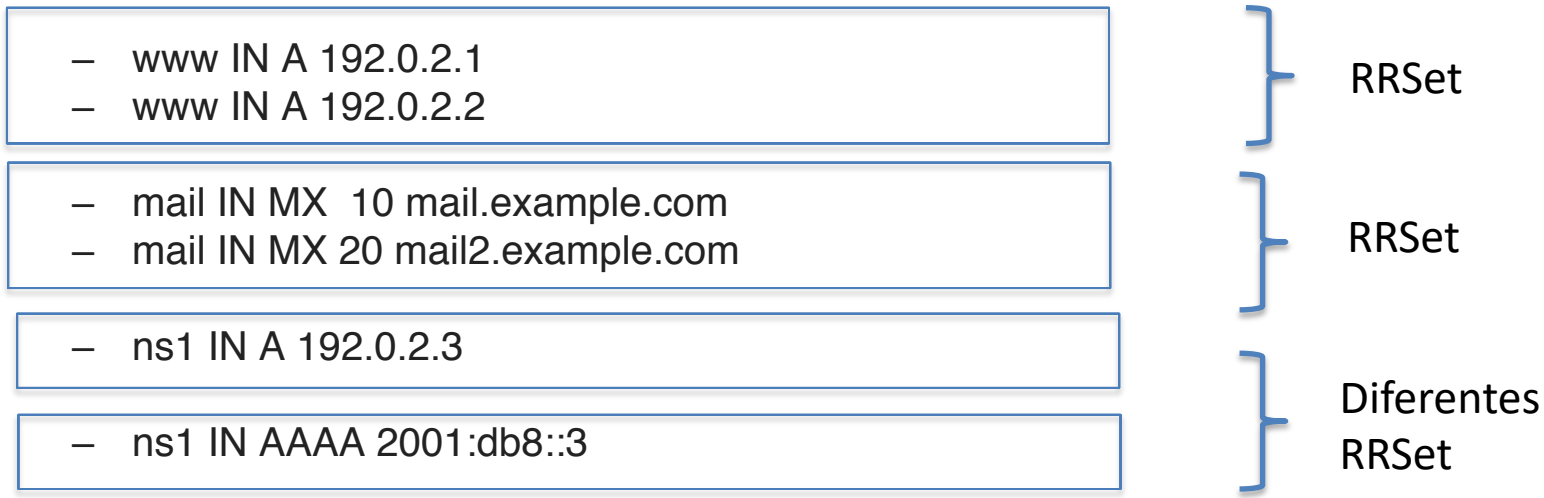
- Nuevos RR
  - RRSIG: *Resource Record Signature*
  - DNSKEY: *DNS Public Key*
  - DS: *Delegation Signer*
  - NSEC/NSEC3: *Next Secure*

Recordemos

- Un *resource record* en DNS es una tupla de cinco valores:
  - (*nombre, clase, tipo, TTL, valor)*
- *Ejemplo:*
  - www.example.com. 86400 IN A 192.0.2.1
- Esta representado por la tupla:
  - Nombre (www.example.com)
  - Clase (IN)
  - Tipo (A)
  - TTL (86400 segundos)
  - Valor (192.0.2.1)

DNSSEC y RRSets

- *Resource Record Sets (*RRSets)
  - DNSSEC opera firmando *RRSet*s (no RR individuales)
  - Un RRSet es un conjunto de resource records que comparten igual:
    - Clase
    - Tipo
    - Nombre
- Ejemplo de RRSet (TTL omitido):



Firma de zonas

- Se genera un par de claves (publica y su correspondiente privada) para cada **zona**
  - El par de claves es propio de cada zona y no del servidor autoritativo
- La parte privada se debe mantener bajo custodia
  - La privada firma los RRSets de la zona
- La publica se debe publicar en DNS mediante un registro DNSKEY
  - La pública permite verificar las firmas de los RRSets
- Un RRSet puede tener multiples firmas generadas con diferentes claves

Registros firmados

- La firma digital de un RRSet se devuelve en forma de un registro RRSIG que es parte de la respuesta
- Ejemplo:

dig +dnssec www.lacnic.net

;; ANSWER SECTION:

www.LACNIC.NET. 7200 IN A 200.3.14.147

www.LACNIC.NET. 7200 IN RRSIG A 5 3 7200 20160506051612 20160406042508 48072 lacnic.net.
RIiO6s9b95wgLK4H8ORMbR9PXWp0Rpb6huaoNySASQiZr32TldnMkNaN bvK0Dwl/hdwtIoz7yLjirNeaWTIloaokO6OHbooPBdfV/RF/T5KNeBYF
SqQpKO34AXQ3nEVmw6OgHFVJT/EVvLghxGR5VUY6qRRMAJ1K6TqpPPn knjmMsDQ/RWLtuhWQRiOshuygp0GpMqdRH8W3I3nE0HqL43WBoYHti03
2/01NB59SWgbHV0C5wclNkXIFIVV45sXKNz7cXX9oc+CQy/xLrTRgegR 0HvlwGLVZeeVRq3qPzAX3/sGDErkZi3pBEepXqzcGN/T5IPdoLlbZq3g A68vSg==

;; AUTHORITY SECTION:

LACNIC.NET. 7200 IN NS SEC3.APNIC.NET.

LACNIC.NET. 7200 IN NS NS.LACNIC.NET.

LACNIC.NET. 7200 IN NS TINNIE.ARIN.NET.

LACNIC.NET. 7200 IN NS dns.anycast.lacnic.net.

LACNIC.NET. 7200 IN NS NS2.LACNIC.NET.

LACNIC.NET. 7200 IN NS ns2.dns.br.

LACNIC.NET. 7200 IN RRSIG NS 5 2 7200 20160506053320 20160406043943 48072 lacnic.net.
b6Au9BEdOqHG8V4vBwbqfEMYNUtdivOJoyy6ER0KSN3xsbY7GOZHwkxF m5StPUgOV8PXhzV/i0faqjpoTBJmQxRZbkW6KH2KuMRG8wA8KF/kbYfK
rL15lQzNsJmv69iUjP5JuXdCE2v8RPrtlhIDOoyCA4cmSLxrZNAhZETM YR5uz7yegcEXEHwMf1OZCzBQZdXglZ5zwfhxCwEO4mjzMKGPnfHsnxmH
S5eQu5l71xAa+D7xvV0nyREk+qt/h/FyZeehazy5tGiVTH+Goht4pUoa DhQTqRdx1CJiu3XYJINE6jatGtPEKO0tDvx9EW6R27jmULFOyanvEkfF iZHpvA==

Cadena de confianza

- ¿Como puede un cliente verificar un RRSet de una cierta zona?
  - Hace una consulta por el DNSKEY correspondiente
  - Realiza los calculos correspondientes y los compara con el RRSIG
    - Si coinciden, la firma verifica, de lo contrario, no
- Pero ¿como se puede confiar en la DNSKEY si sale de la misma zona que queremos verificar?
  - Necesitamos verificar la **cadena de confianza**

Cadena de confianza

- Registro DS "*Delegation Signature*"
  - Los registros DS "firman" claves de zonas **hijas**
  - De esta forma uno puede verificar el DNSKEY de una zona buscando un registro DS en la zona padre
- El registro DS contiene un hash de la una clave pública
  - Es decir, del contenido de un registro DNSKEY
- Los registros DS en la zona padre están firmados con la(s) claves de esa zona
- Parecidos a los NS, pero son authoritativos en el padre, no el hijo
- Para completar la cadena de confianza tiene que estar firmada la **raíz del DNS**

Cadena de confianza

- Pero ¿que pasa con la zona raíz?
  - La zona raíz no tiene “padre” a quien ir a pedirle un registro DS
- La raíz del DNS esta firmada desde julio de 2010
  - *[http://www.root-dnssec.org]*
- El registro DS para “.” se puede obtener fuera de banda
  - [http://data.iana.org/root-anchors/root-anchors.xml]
  - . IN DS 49AAC11D7B6F6446702E54A1607371607A1A41855200F D2CE1CDDE32F24E8FB5

Firma de la raíz

- ¿Cómo se verifica la autenticidad del root trust-anchor?
- El TA de la zona raíz se publica fuera de banda, por ello la validación debe ser diferente
  - Se puede bajar por HTTP/HTTPS
  - Se puede verificar por otros mecanismos (certificados, firmas PGP)
  - Similar a lo que pasa con la zona raíz misma, se debe cargar manualmente

Negación de existencia

- Respuestas con “NXDOMAIN”
  - Niegan la existencia de un nombre
  - Son respuestas “cacheables” a pesar de ser negativas
- ¿Como firmar la no-existencia?
  - Necesito tener un RRSet para firmar
    - Recordar que en DNSSEC lo que se firma siempre son RRSets
  - Técnicas propuestas:
    - NSEC
    - NSEC3

NSEC/NSEC3

- NSEC provee un puntero al próximo registro seguro según orden alfabético
- Ej: consulta por mail.example.com ?

- NSEC: www.example.com

KSK vs ZSK

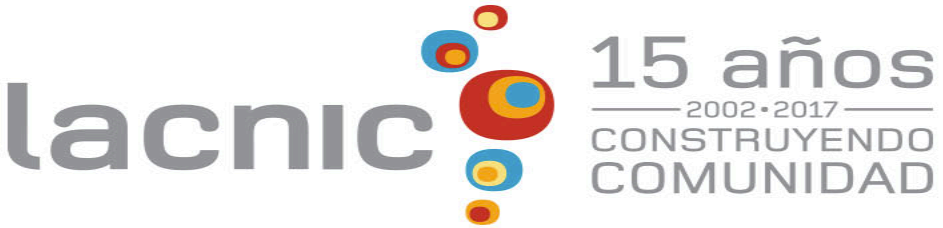
- Usamos 2 pares de claves pública-privada:
  - ZSK: usada para firmar las zonas
  - KSK: usada para firmar la ZSK
    - Es la apuntada por el registro DS de la zona padre
- Ventaja: no es necesario actualizar el registro DS en la zona padre cuando se cambia la clave de una zona
- Evita una mayor complejidad administrativa

DANE: DNS-Based Authentication of Named Entities

- Protocolo para poder codificar certificados X.509 en DNS
- DANE permite publicar y firmar las claves/certificados TLS de un dominio usando la estructura del DNS
  - Para que el modelo funcione, es necesario usar DNSSEC
- De esta forma, se pueden usar certificados auto-firmados (no es necesaria una CA externa) para los distintos servicios
- Se agrega un nuevo RR: TLSA
- Especificado en las RFC6698 y RFC7671

Secuestro de rutas y medidas de protección

RPKI – Resource Public Key Infrastructure

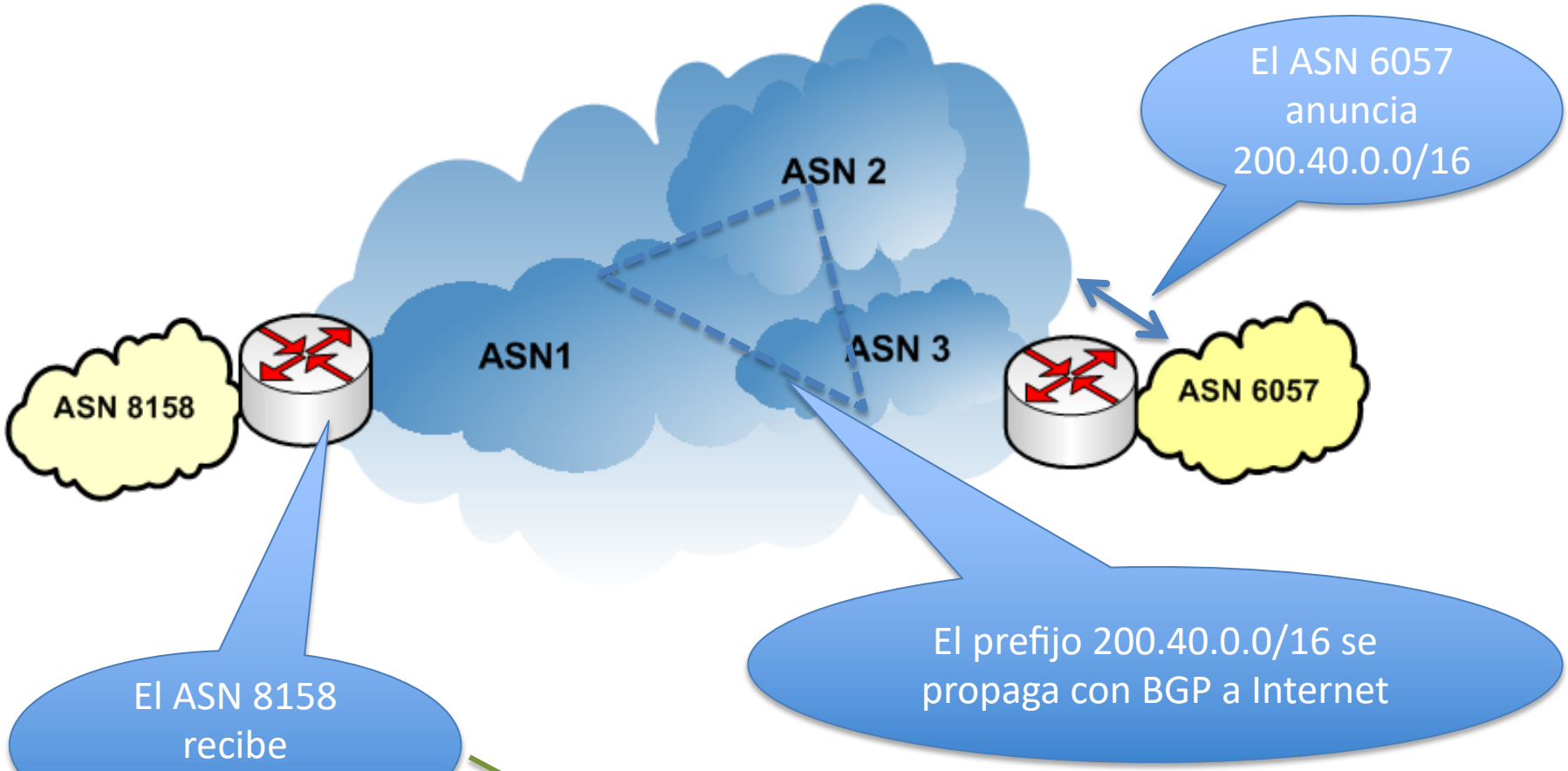


CÓMO FUNCIONA INTERNET?

Protocolo BGP

- Las organizaciones publican sus prefijos de red mediante el protocolo BGP
- Anuncian las redes a las que se puede llegar y el próximo salto (next hop) a través del cual llegar
- Cada organización debería anunciar sólo sus propios recursos (prefijos IP) o los de organizaciones a las que provea tránsito
- Pero este control en BGP no está contemplado
- Se basa en la buena voluntad de los operadores (ISPs)

Enrutamiento en Internet



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**

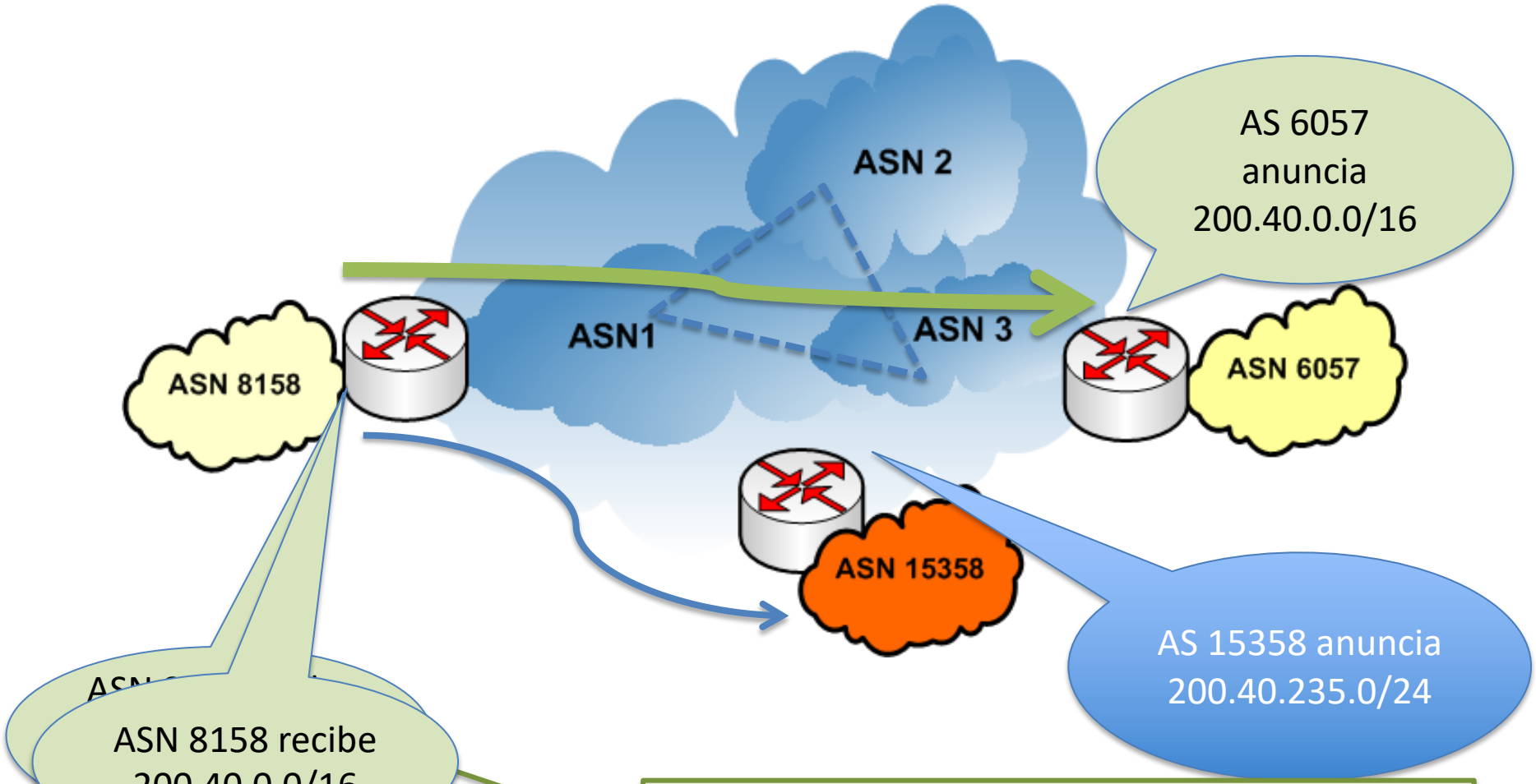
Ruteo en Internet

- Recordemos de BGP:
  - Los anuncios de rutas que recibimos afectan al tráfico ***saliente***
  - Los anuncios de rutas que realizamos afectan al tráfico ***entrante***
- Entonces:
  - Si recibimos un anuncio de ruta incorrecto, nuestro tráfico puede ir hacia sitios distintos de lo esperado
  - Es posible atraer hacia nosotros determinado tráfico haciendo anuncios de rutas específicos

Secuestro de rutas

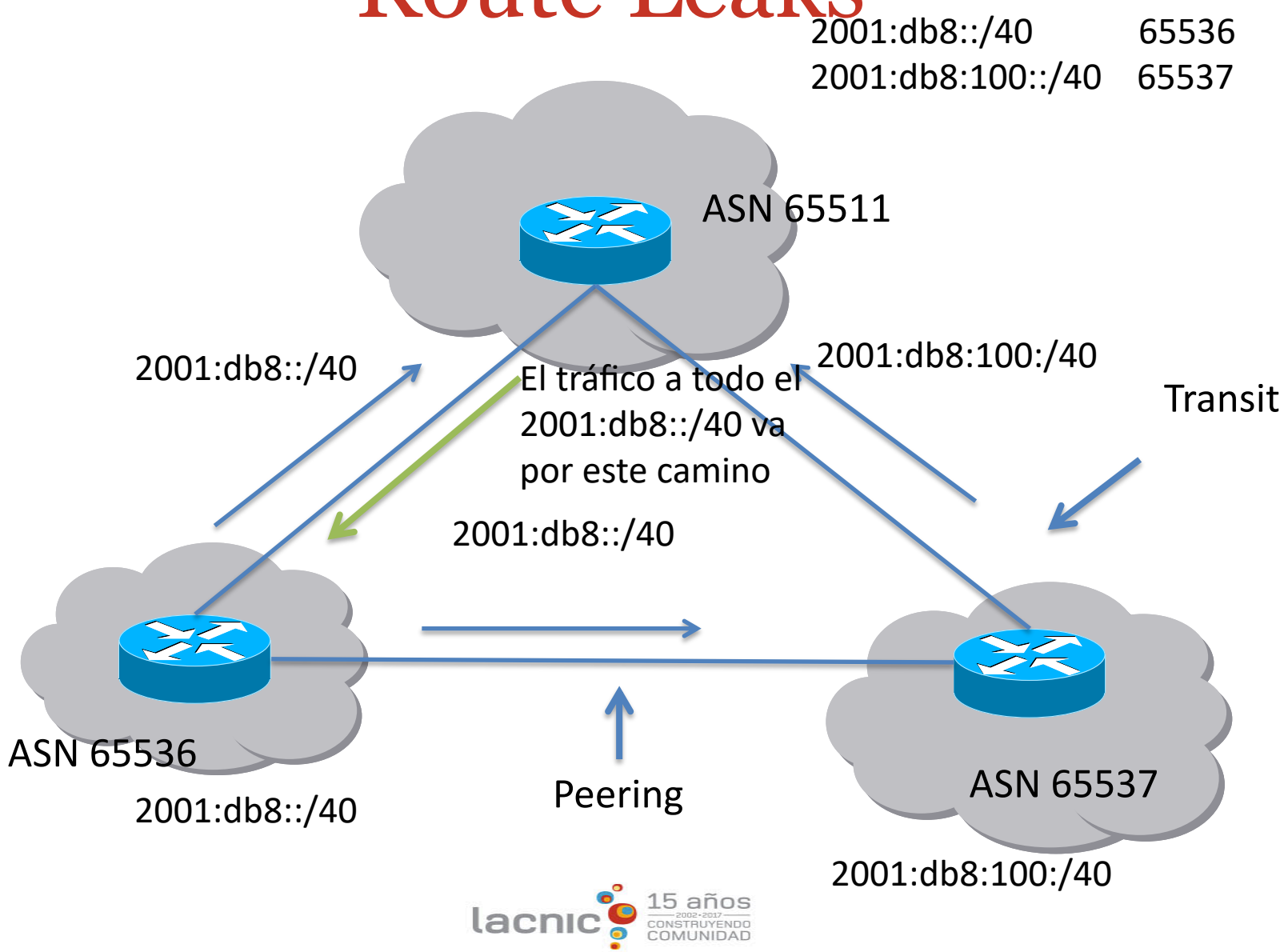
- Cuando un participante en el routing en Internet anuncia un prefijo que no esta autorizado a anunciar se produce un "*secuestro de ruta*" (*route hijacking)*
- Malicioso o causado por error operacionales
- Casos más conocidos:
  - Pakistan Telecom vs. You Tube (2008)
  - China Telecom (2010)
  - Google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

Secuestro de rutas



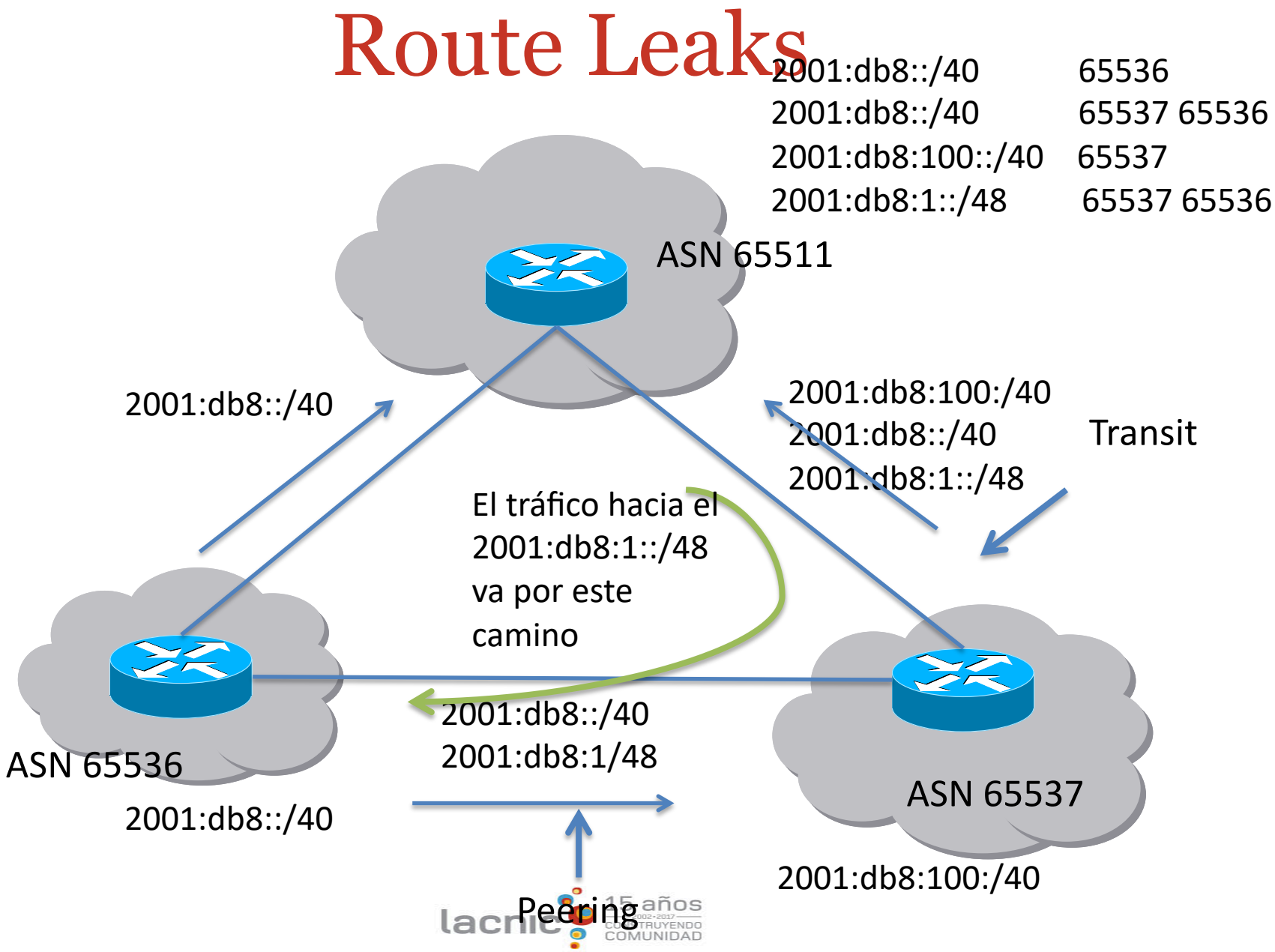
Route Leaks

Cómo esto debería funcionar sin leaks



Route Leaks

Ahora un route leak



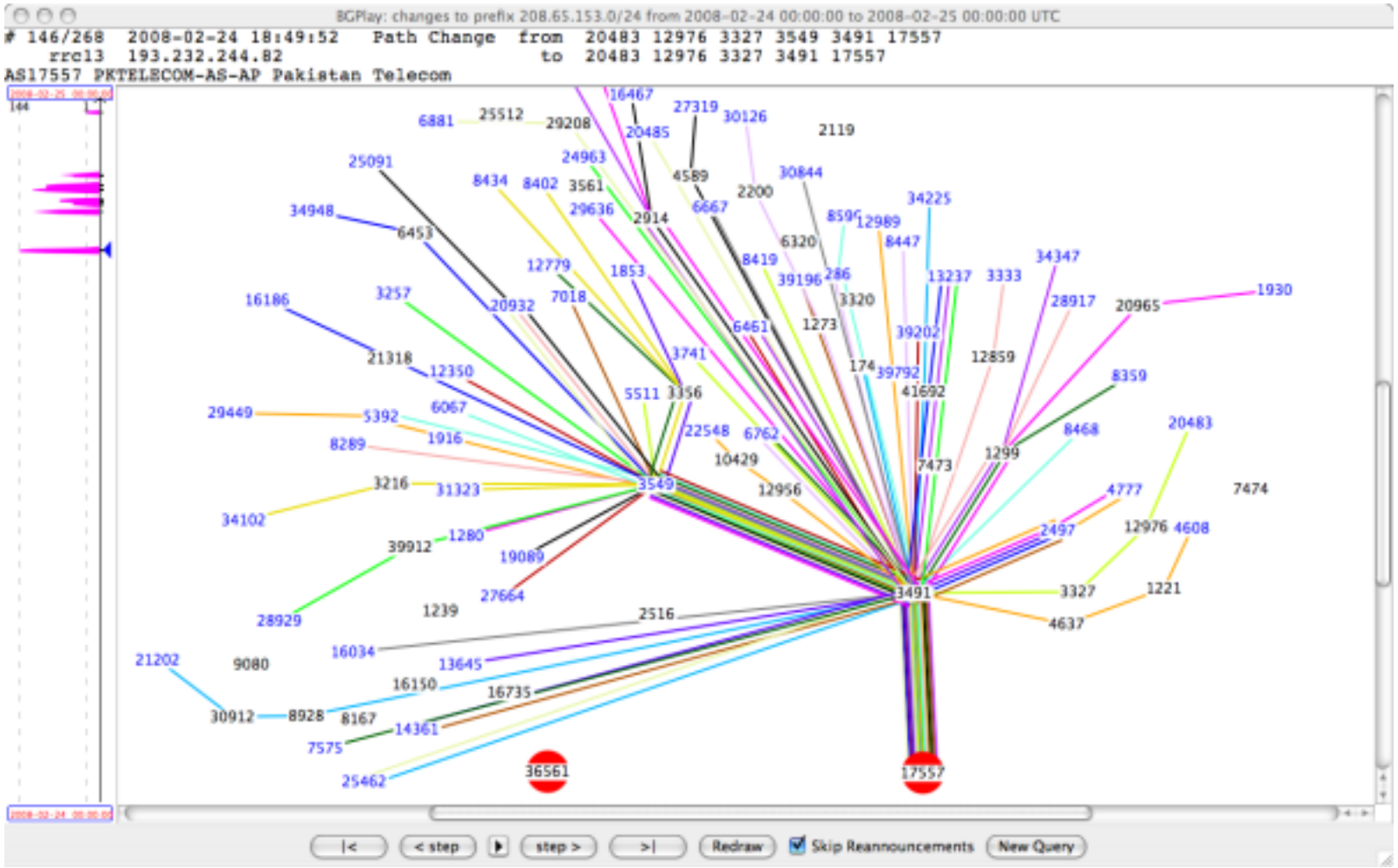
Secuestro de rutas

- 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
- Sin embargo, en un trabajo de 2008, presentado en DEFCON 16, Pilosov-Kapela demuestran la posibilidad de re-enrutar tráfico sin prácticamente dejar evidencias
  - De esa manera, el tráfico puede ser analizado y procesado sin ser notado

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



China Telecom (2010)

- En abril de 2010, AS23724 operado por China Telecom propagó rutas erróneas durante 15 minutos:
  - De un promedio de 40 prefijos pasó a 37.000 anuncios de prefijos no asignados a ellos
  - Muchos sitios populares fueron afectados, como dell.com, cnn.com, www.amazon.de , www.rapidshare.com y www.geocities.jp, además de muchos sitios chinos
  - También sitios .mil y .gov como el Senado, ejército, marina, fuerza aérea y otros de los EEUU
- http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/
- http://www.bgpmon.net/chinese-bgp-hijack-putting-things-in-perspective/

RPKI

- 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

¿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)

ROAs

- Usando certificados podemos firmar 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

Validación 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

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

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

Preguntas?

Muchas gracias…