Colaborando con la seguridad y la estabilidad de Internet en América Latina y el Caribe

Ing. Carlos Martínez

A.C. Graciela Martínez

Esp. Guillermo Cicileo

Agenda

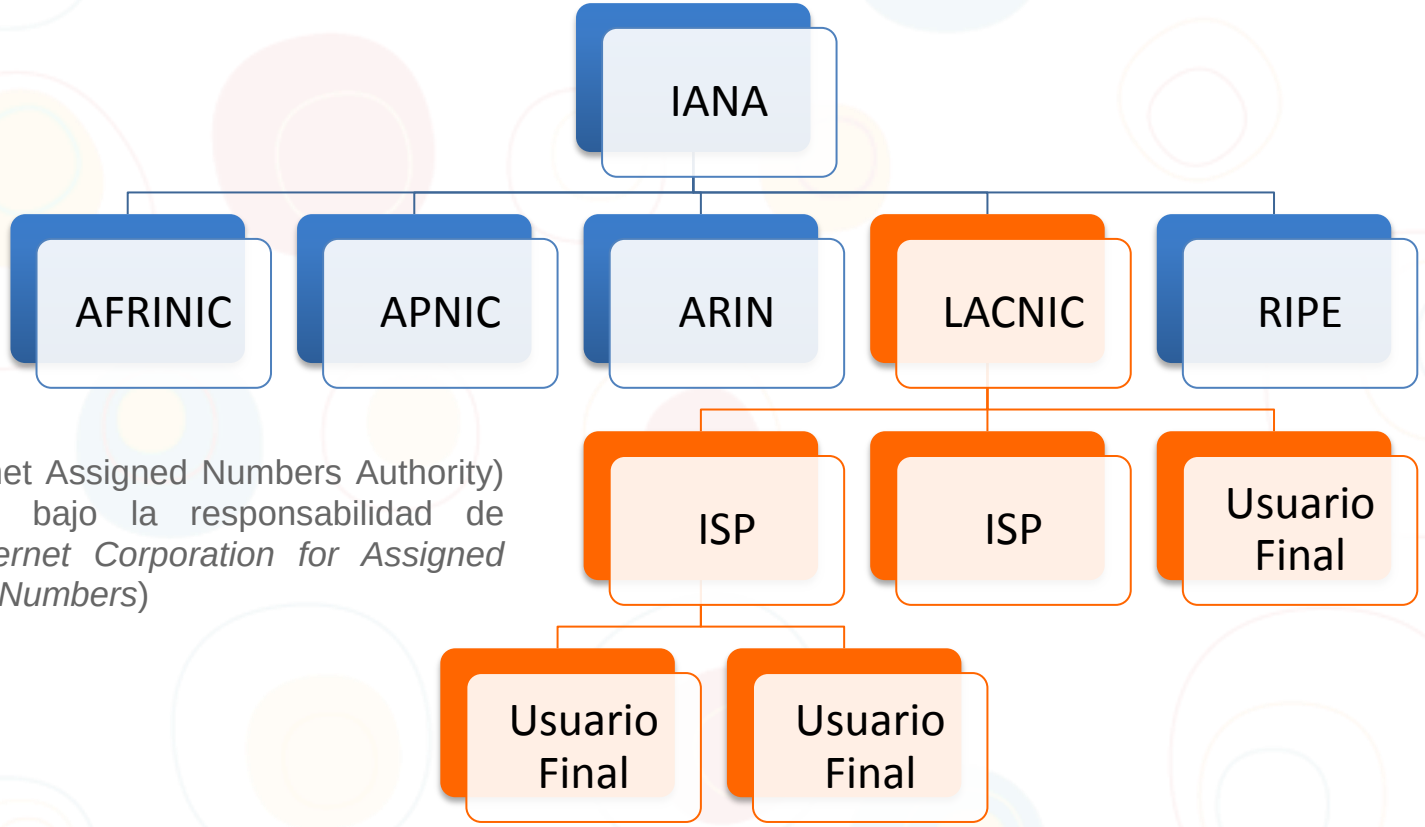
- Administración de los recursos numéricos de Internet, marco global y regional
- Actividades de LACNIC para contribuir a la estabilidad y seguridad de Internet en la región
- LACNIC WARP Respuesta a incidentes de seguridad
- Información útil a la hora de gestionar incidentes de seguridad

Administración de los recursos numéricos de Internet, marco global y regional

Registros Regionales de Internet (RIRs)

lacnic

Distribución de Recursos de Numeración de Internet



IANA (Internet Assigned Numbers Authority) actualmente bajo la responsabilidad de ICANN (*Internet Corporation for Assigned Names and Numbers*)

Evolución del sistema de los Registros de Internet Regionales (RIR)

- Antes de 1992 – Sistema Centralizado (*registro único)*
  - 1992 – RIPE NCC en Europa
  - 1994 – APNIC en Asia y Pacífico
  - 1997 – ARIN comienza a operar como registro para América del Norte
- El sistema de los RIRs es global desde 1997
  - 2002 – Se reconoce a LACNIC como registro regional
  - 2004 – Se crea oficialmente AfriNIC, el último RIR en crearse

Registros de Internet Regionales (RIR)

Organizaciones

- Sin fines de lucro
- Sistema de membresía
- Bottom up

Con la función de:

- Administrar el espacio de direcciones y otros recursos de Internet para una región determinada
- Apoyar la Internet abierta como herramienta de desarrollo

¿Cuáles Recursos de Internet?

Hay tres recursos numéricos fundamentales para el crecimiento y despliegue de la red:

- Direcciones IPv4
- Direcciones IPv6
- Números de Sistema Autónomo

Servicios

- Directorio WHOIS
- DNS reverso
- RPKI (certificación de recursos)

lacnic

Servicios y Actividades

Asignación de Direcciones IP y recursos relacionados / Certificación de recursos / Capacitación y entrenamiento de expertos / Coordinación y apoyo de foros técnicos, encuentros regionales y grupos de trabajo / Coordinación y participación en proyectos de cooperación

- Argentina
- Aruba
- Belize
- Bolivia
- Bonaire
- Brasil
- Chile
- Colombia
- Costa Rica
- Cuba
- Curaçao
- Ecuador
- El Salvador
- Falkland Islands
- Guyana
- Guayanne Française
- Guatemala
- Haiti
- Honduras
- México
- El Salvador
- Nicaragua
- Panamá
- Paraguay
- Perú
- República Dominicana
- Saba
- Sint Eustatius
- Sint Maarten
- South Georgia ande the South Sandwich Islands
- Suriname
- Trindad and Tobago
- Uruguay
- Venezuela

LACNIC es una organización internacional sin fines de lucro establecida en Uruguay en el año 2002. Es administrada y dirigida por un Directorio de siete miembros elegidos por sus asociados, un conjunto de más de 2500 entidades que operan las redes y brindan servicios en 33 territorios de América Latina y el Caribe.

¿Que rol cumple LACNIC?

Qué no hace LACNIC

- No tiene poder de policía en Internet
- No puede filtrar redes, ni armar listas de acceso
- No cancela la posesión de recursos por mal uso
- No sanciona a los ISP s

¿Que rol cumple LACNIC?

Qué sí hace LACNIC

- Mantiene un WHOIS actualizado
- Sirve como organismo de coordinación en la región
- Brinda capacitaciones y formación a los ISP s
- Aconseja sobre mejores prácticas
- Decide políticas en base a propuestas de sus miembros

Actividades de LACNIC para contribuir a la estabilidad y seguridad de Internet en la región

Actividades

Nosotros creemos que la seguridad es responsabilidad de todos los involucrados de alguna manera con Internet.

En particular LACNIC en este sentido realiza una serie de actividades:

- En los dos eventos anuales LACNIC brinda un espacio para que pueda llevarse a cabo una reunión de CSIRTS de la región
- Una vez al año y durante el segundo evento anual, LACNIC oficia de sponsor para realizar un FIRST TECHNICAL COLLOQUIUM
- LACNIC brinda la plataforma de correo y webex para el forum de LAC-CSIRT, que es la mailing list que integran los involucrados de distintos centros de respuesta de la región
  - **Sin coordinación todos nuestros esfuerzos son inútiles**
  - **Procedimiento de ingreso**

lacnic

Actividades

- Tenemos acuerdos con algunas organizaciones para el intercambio de información
- Brindamos talleres para nuestros miembros, como por ejemplo:
  - Amparo – cuyo objetivo es contribuir a la creación de la función de respuesta a incidentes de seguridad entre los miembros de LACNIC
  - RPKI – para la certificación de recursos

LACNIC WARP
Respuesta a Incidentes de Seguridad

Misión y Comunidad objetivo de LACNIC WARP

- Llevar a cabo las funciones de coordinación necesarias para el fortalecimiento de las capacidades de respuesta a incidentes vinculados a las direcciones de Internet de América Latina y el Caribe, en el marco de las metas específicas establecidas por la misión de LACNIC tendientes a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento
- La comunidad objetivo está constituida por todas las organizaciones miembros de LACNIC

Autoridad

- LACNIC WARP no tiene autoridad para actuar sobre las operaciones de los sistemas de su comunidad, a excepción de los sistemas internos propios de LACNIC, por lo que no brindará asistencia directa remota ni in situ para la atención de incidentes de seguridad, aun cuando éstos involucren direcciones de Internet de Latinoamérica y el Caribe.

Servicios definidos de LACNIC WARP (I)

- Servicios a prestar por LACNIC WARP
  - Alertas de Seguridad a medida (Filtered Warnings): envío de advertencias de seguridad relevantes para la comunidad
  - Intermediación (Advice brokering): LACNIC WARP provee a sus miembros un ambiente seguro y anónimo de intermediación para la búsqueda, discusión e intercambio de información de incidentes de seguridad y buenas prácticas

Servicios definidos de LACNIC WARP (II)

- Reporte de incidentes (Reporting Point)
  - LACNIC WARP provee a los miembros un punto de confianza para el reporte de incidentes de seguridad u otra información sensible sin el temor de que la misma puede ser divulgada ni utilizada en su contra
  - Las organizaciones no miembros también podrán reportar incidentes, LACNIC WARP colaborará para redirigirlos según convenga
  - El reporte de incidentes podrá realizarse a través de
    - Correo electrónico a la casilla: info-warp@lacnic.net
    - Formulario web: www.lacnic.net/web/warp/form

lacnic

Camino recorrido

- Desde octubre llevamos considerados mas de 30.000 correos electrónicos (casilla abuse fundamentalmente).
- Se han gestionado mas de 90 incidentes.
- Se realizaron acuerdos con algunas organizaciones para el intercambio de datos.

Tipos de incidentes reportados

Algunos de los tipos de incidentes que se han gestionado:

- Ataques de DDOS utilizando varios tipos de protocolo
  - Open resolvers, Open SNMP
- Phishing
- Ataques de fuerza bruta para intentos de acceso no autorizado
- Anuncios indebidos de rutas de Internet
- SPAM

Información útil a la hora de gestionar incidentes de seguridad

Sistemas Autónomos - AS

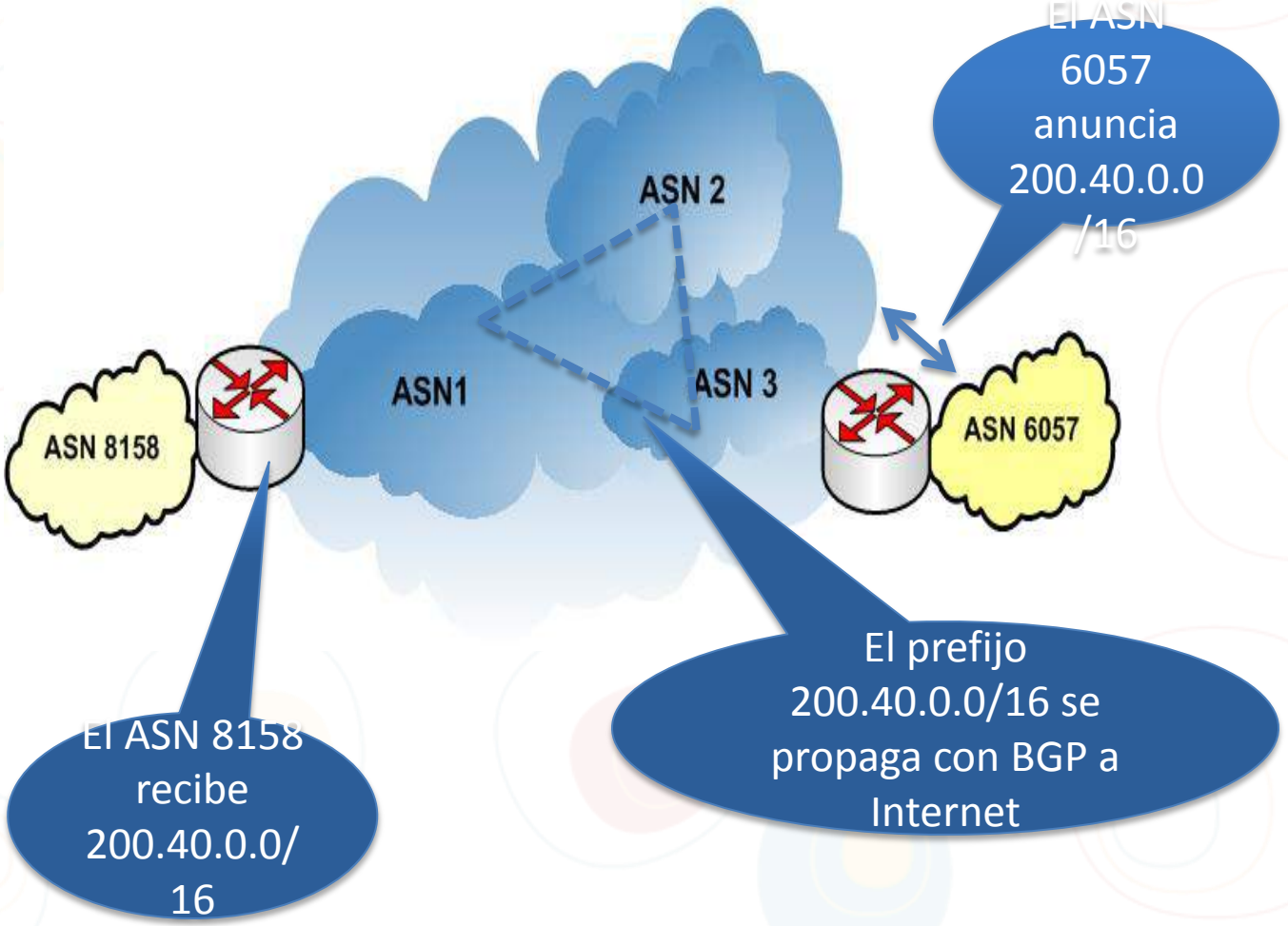
- Normalmente, para poder utilizar una dirección IP, ésta debe ser publicada en Internet mediante un anuncio de ruta
- Una organización que publica rutas en Internet, necesita un número de sistema autónomo
- Sistema autónomo: se denomina así a una organización que controla un conjunto de redes bajo su administración
- Los sistemas autónomos reciben un número: ASN que también es asignado por los RIRs
- Esta información es única a nivel mundial

¿ 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



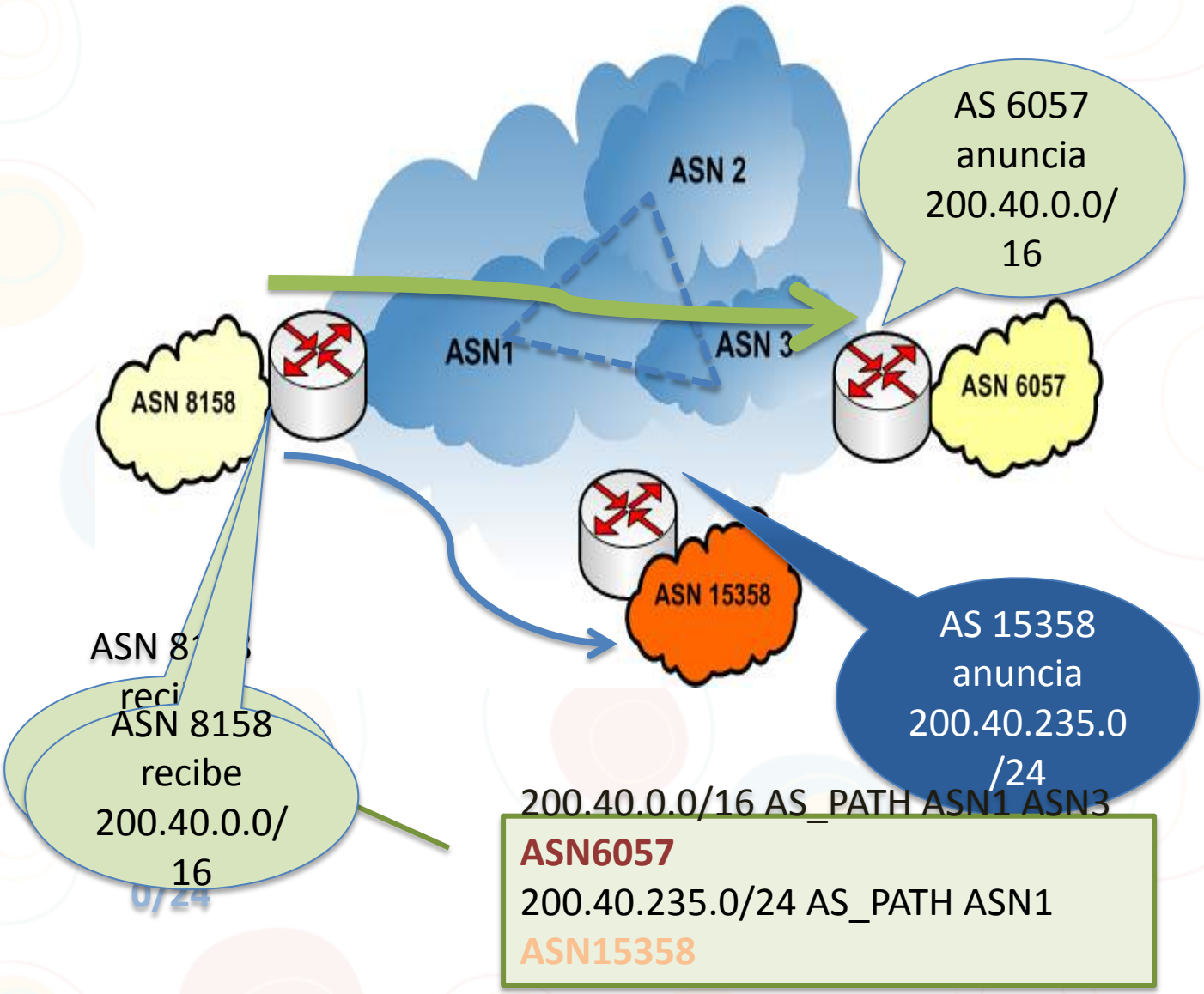
Enrutamiento en Internet

- 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

Secuestro de rutas



Secuestro de rutas

Se recomienda que se analicen algunos casos de estudio, por ejemplo:

- Pakistan Telecom vs. You Tube - 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 por algunas horas. 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

Secuestro de rutas

- 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: dell.com, cnn.com, www.amazon.de , www.rapidshare.com y www.geocities.jp, además de muchos sitios chinos
  - Tambien 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
- La solución involucra:
  - 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

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 (***permiten agrupar bloques de direcciones en una sola entrada de tabla de rutas)*
- Se impide entonces que terceros falsifiquen la información de enrutamiento o las firmas

Herramientas de información

Para la gestión de incidentes recordemos que tenemos herramientas muy valiosas que nos pueden colaborar para identificar a una organización:

- DNS
- Resolucion DNS reversa
- WHOIS – IP y ASN
- ASN de origen y upstream (tablas de ruteo, traceroute)
- Ping – podríamos saber si un servicio está activo
- Looking glass, es un servicio que permite obtener una vista de la tabla de ruteo de BGP, normalmente son provistos por ISPs o IXPs

Agotamiento de IPV4

Fechas de agotamiento:

- IANA agotó su espacio /8 en Enero de 2011
- APNIC fue el primer RIR en quedarse sin espacio IPv4 a fines de 2011
- RIPE NCC agotó su espacio IPv4 en 2012
- LACNIC agotó su espacio IPv4 en Jun-2014
- ARIN agotó su espacio en Junio 2015
- AFRINIC – Feb/2019

NAT – Problemas

- Al compartir una misma dirección IPv4 se modifica el modelo de comunicación IP punto a punto
- ACLs (Listas de control de acceso) para evitar ciertos ataques tienen importantes efectos colaterales, al bloquear el tráfico de un cliente “malo”, también bloqueamos el tráfico de muchos clientes “buenos”
- Para identificar quién accedió a un servicio, no solo hay que guardar la dirección IP sino también el puerto
- Clientes de distintos países salen a Internet a través de una misma dirección IP

Muchas Gracias...

A.C. Graciela Martínez
Head of LACNI WARP
Security Incident Response
gmartinez@lacnic.net