Peering & IPv6 (agosto 2026)

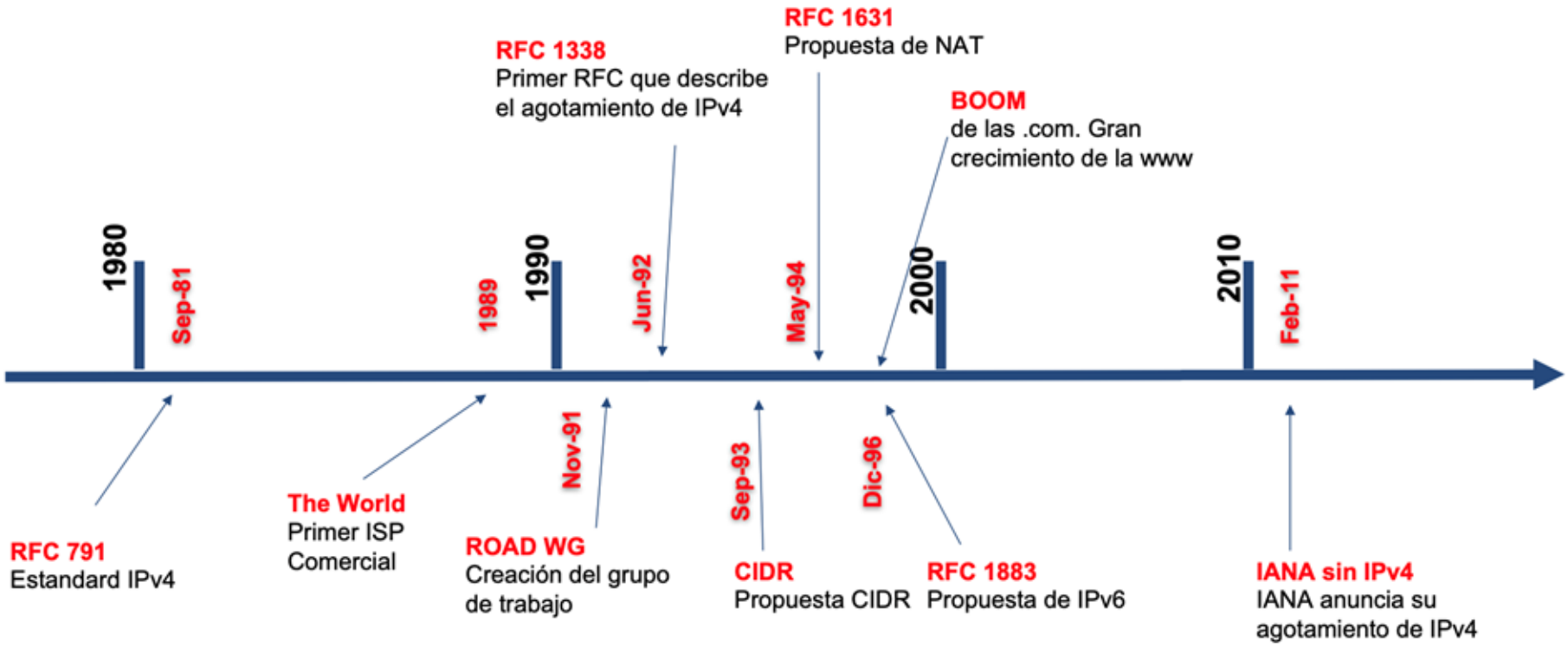
Alejandro Acosta
alejandro@lacnic.net
@ITandNetworking

Contenido

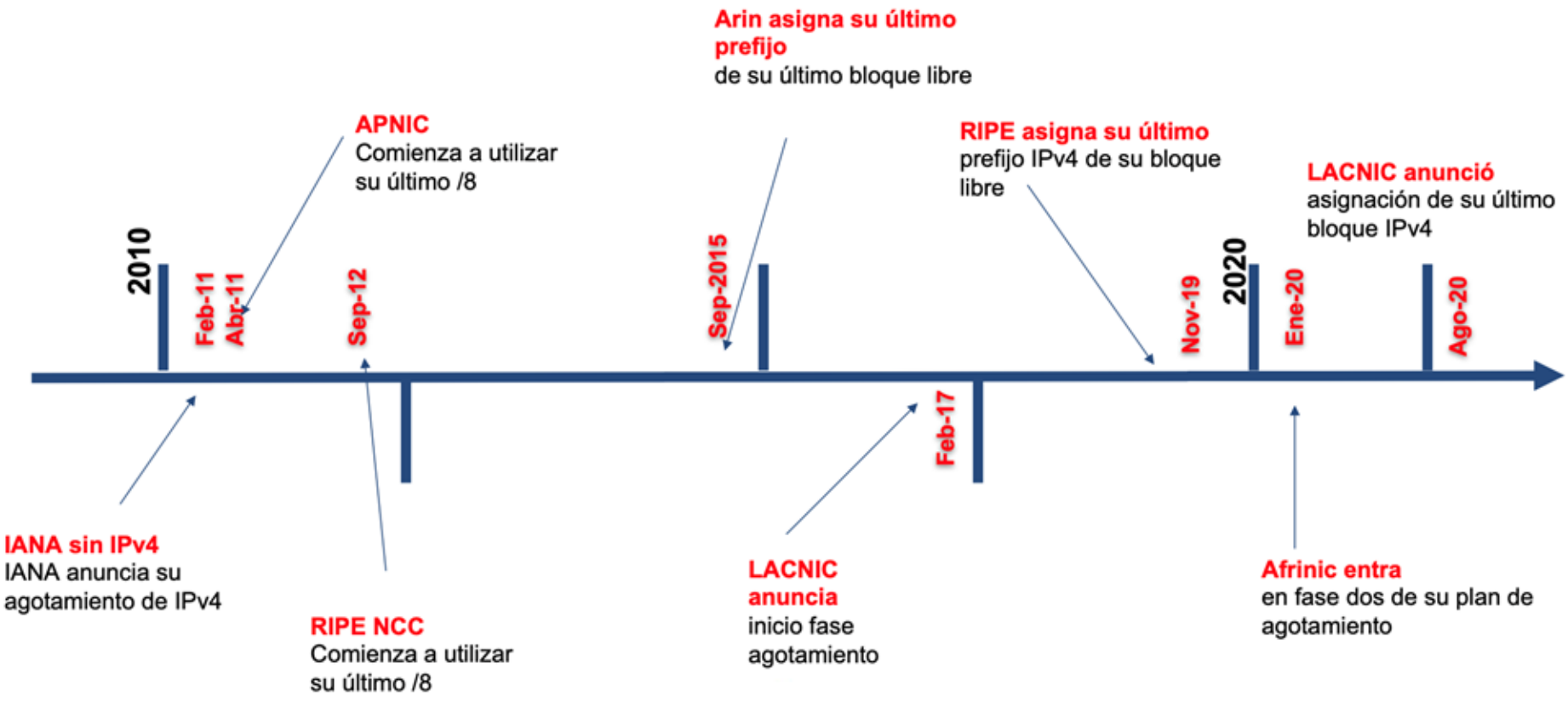
1. Adiós IPv4
    1. CGNAT es costoso; IPv6 es eficiencia directa.
2. MP-BGP: El Motor Técnico
    1. /48s
3. El Rol de los IXPs
    1. NDP
4. Bogons
5. RFC 8950

Adios a IPv4

Línea de tiempo - Agotamiento IPv4 (1/2)



Línea de tiempo - Agotamiento IPv4 (2/2)



(solo referencia, tipo casi parodia y de manera de chiste)

lacnic

MP-BGP

NOC
¡El peering debe ser con BGP!
Optimizando la conectividad global e
intercambio de tráfico en Internet.
NOC
BGP
BGP
BGP

BGP Multiprotolo

- La RFC 4760 define extensiones para BGP multiprotocolo
- Esto permite extender el uso de BGP4 a otras familias de direcciones: vpnv4, IPv6, unicast, multicast, etc.
- Se define un identificador de address family, llamado AFI y subsequent address family: SAFI
- AFI = 1, IPv4
  - SAFI = 1 unicast, SAFI = 2 multicast
- AFI = 2, IPv6
  - SAFI = 1 unicast, SAFI = 2 multicast

lacnic

IPv6 en un IXP

IPv6 en un IXP

- NDP
  - - Suprimir RAs
  - - Utilizar RA Guard
  - - Deshabilitar auto-configuración
  - - Anuncio más chico /48
  - - /64 en VLANs de peerings
  - - Rate-limiting NDP

SEGURIDAD

Mitos de Seguridad IPv6

- Mitos de Seguridad
  - Yo solo uso IPv4, no tengo que preocuparme de IPv6
  - IPv6 es más seguro que IPv4
  - Estoy expuesto: sin NAT ni direcciones privadas
  - IPv6 es algo muy nuevo para ser atacado

Clasificación Amenazas IPv6 (I)

- Tres categorías para amenazas seguridad IPv6:
- Ya existían con IPv4 y se comportan similar con IPv6
  - Ejemplos: sniffing, ataques a otras capas, flooding
- Ya existían con IPv4 y se comportan distinto con IPv6
  - Ejemplos: escaneo de red, amplificación (smurf)
- Nuevas amenazas que aparecen con IPv6
  - Ejemplos: amenazas a NDP, Routing Header tipo 0, cabeceras de extensión

Recomendaciones de seguridad

Algunos consejos en IXPs/ISP/SPs

- Limitar RA (Router Advertisement) en enlaces no directamente conectado clientes
- Habilitar RA Guard en los LAN Switch del IXP
- BGP Maximum Prefixes
- RPKI + IRR
- Utilizar password en las sesiones BGP
- No permitir nuestros propios prefijos
- BCPs
  - 38 (anti-spoofing)
  - 84 (urpf)

Bye bye NAT

¿Qué tiene de malo el NAT (Network Address Translation?

R: Caro y lo peor: rompe la conectividad end-end

¿Qué tanto NAT existe?

En IPv4: 80 %

En IPv6: 0,05 %

¿Por qué ir a IPv6?

En IPv6 la tendencia es no utilizar NAT

→ Gran mejoría en el performance de los DC / Head

Ends

https://natmeter.labs.lacnic.net/

lacnic

PREFIJOS BOGONS

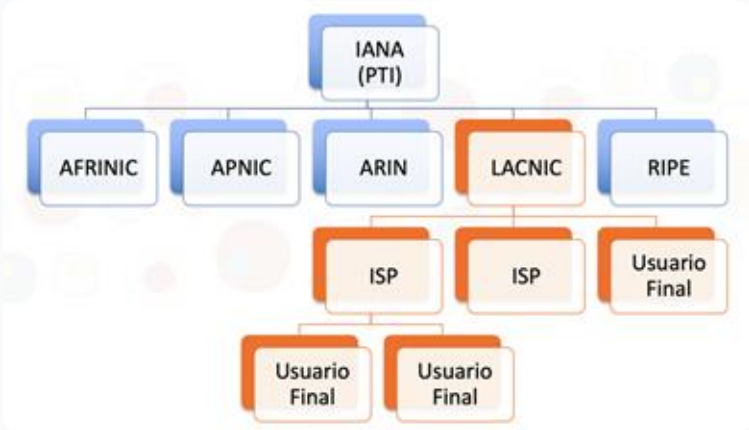
¿Qué son los prefijos Bogons?

Los **prefijos bogons** (o simplemente *bogons*) son direcciones IP y rangos de red que **no deberían verse transitando por el Internet público (DFZ y otros)**.

Tipos de prefijos bogons

Direcciones Marcianas (Martians)

Rangos IP reservados por RFCs para propósitos especiales (como redes privadas o pruebas), que por definición no son enrutables en el internet público.



Espacio no asignado

Bloques de direcciones IP que aún no han sido delegados o asignados por la IANA o por los Registros Regionales de Internet (RIR) a ningún operador.

lacnic

Ejemplo de prefijos IPv4 Bogons

Redes Privadas (RFC 1918)

No son enrutables en el Internet público y se usan para redes de área local (LAN):

- **`10.0.0.0/8`**: Bloque completo Clase A (desde `10.0.0.0` hasta `10.255.255.255`).
- **`172.16.0.0/12`**: Bloque Clase B (desde `172.16.0.0` hasta `172.31.255.255`).
- **`192.168.0.0/16`**: Bloque Clase C habitual de hogares (desde `192.168.0.0` hasta `192.168.255.255`)

Direcciones Locales y de Enlace

- **`127.0.0.0/8`**: Rango de **Loopback**. Se usa para pruebas internas del propio host (la más famosa es `127.0.0.1`).
- **`169.254.0.0/16`**: Rango **Link-Local** (APIPA). Las asignan los sistemas operativos automáticamente cuando no consiguen un servidor DHCP.

Documentación y Pruebas (Test-Nets)

Rangos reservados para libros, manuales técnicos y pruebas de laboratorio:

- **`192.0.2.0/24`** (TEST-NET-1)
- **`198.51.100.0/24`** (TEST-NET-2)
- **`203.0.113.0/24`** (TEST-NET-3)
- **`198.18.0.0/15`**: Rango para medir rendimiento o *benchmarking* entre dispositivos (RFC 2544).

lacnic

Ejemplo de prefijos IPv6 Bogons

Rangos Reservados Estáticos

- `::/128`: Dirección no especificada. Se utiliza solo como dirección de origen temporal cuando un dispositivo inicia en la red y aún no tiene una IP configurada.
- `::1/128`: Dirección de **Loopback** (equivalente a la `127.0.0.1` de IPv4) para pruebas internas en el propio equipo.
- `::ffff:0:0/96`: Direcciones IPv4 mapeadas en IPv6. Se usan internamente en sistemas operativos para compatibilidad, pero son inválidas en el enrutamiento global.
- `64:ff9b::/96`: Rango para traducción de protocolos **NAT64 well-known prefix** (RFC 6052). Sirve para que redes puras IPv6 se comuniquen con el mundo IPv4.

Redes Locales y ULAs (Equivalentes a RFC 1918)

- `fc00::/7`: Direcciones Locales Únicas (**ULA** o *Unique Local Addresses*). Son el equivalente a las IP privadas de IPv4; se usan dentro de corporaciones u hogares y ningún router de Internet las propaga.
- `fe80::/10`: Direcciones de **Enlace Local** (*Link-Local*). Todo dispositivo IPv6 autogenera una para hablar exclusivamente con los vecinos de su mismo cable físico o red Wi-Fi.

Ejemplo de prefijos IPv6 Bogons

Mecanismos de Transición Obsoletos o Especiales

- `2002::/16`: Bloque reservado para el mecanismo de transición **6to4** (RFC 3068). Aunque se usó mucho en el pasado, hoy está en desuso y suele filtrarse como bogon.
- `2001:10::/28` al `2001:30::/28`: Rangos utilizados para pruebas y protocolos específicos de la IETF (como la subred `2001:20::/28` para benchmarking del RFC 5180).

Documentación y Pruebas

- `2001:db8::/32 y 3fff::/20`: Reservado exclusivamente para **documentación**, ejemplos de libros de texto, guías y manuales técnicos (RFC 3849 y RFC 9637).

lacnic

¿Por qué representan un riesgo de seguridad?

¿Por qué representan un riesgo de seguridad?

Ataques de Spoofing, Spam y DDoS

Los atacantes falsean direcciones IP no asignadas (bogons) para ocultar su identidad real y saturar servidores mediante tráfico malicioso difícil de rastrear.

Infiltración de Redes Internas

El uso no filtrado de rangos privados o reservados permite a intrusos saltar perímetros de seguridad y simular confianza dentro de la red corporativa.

Nula Trazabilidad del Tráfico

Al no estar asignadas a ninguna organización legítima, identificar el origen real de estas conexiones es inviable sin un filtrado proactivo en los routers.

lacnic

RFC 8950

RFC 8950 al rescate

Enrutamiento nativo de IPv4 en redes IPv6-Only

RFC 8950 al rescate

Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop

RFC 8950 al rescate

Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop

¿Y esto que significa?

RFC 8950 al rescate

Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop

¿Y esto que significa?

Puedo anunciar prefijos IPv4 en BGP de manera fácil y sencilla en redes IPv6

¿preguntas?
¿Dudas?

Alejandro Acosta
alejandro@lacnic.net
@ITandNetworking