Las últimas novedades en la evolución de IPv6

Carlos M. Martínez

@CagnazzoEng

lacnic

www.lacnic.net

Motivación para este análisis

- Los cursos de IPv6 brindados por LACNIC y por otras organizaciones brindan una sólida base de conocimientos generales

- Sin embargo, IPv6 es un tema tecnológico dinámico, tanto en lo que es la definición del protocolo en sí como en la experiencia que se va logrando en temas de operación

- El objetivo de este módulo es complementar la base de conocimientos que se brinda en los cursos tanto básico como avanzado del campus con los últimos temas y las últimas discusiones sobre IPv6, aprovechando la oportunidad para convocar al resto de la comunidad y que sea de utlidad para todos

¿Que está pasando en el IETF?

Grupos de trabajo y eventos analizados

- 6man
  - Mantenimiento del protocolo
- v6ops
  - Consideraciones operativas en redes IPv6
- Eventos:
  - IETF 104: Praga
  - IETF 105: Montreal
  - IETF 106: Singapur

Acerca del proceso en IETF

- En un WG del IETF pueden discutirse documentos que son ya adoptados por el grupo, o que todavía son contribuciones independientes
- ¿Cómo me puedo dar cuenta?
  - Para darnos cuenta fácil miramos el nombre del draft, si el mismo incluye ‘ietf’ y el nombre del WG, es un documento adoptado
    - draft-ietf-v6ops-xxxx
- Fuente: https://www.ietf.org/standards/ids/guidelines/

Grupo v6ops

- Charter: https://datatracker.ietf.org/group/v6ops/about/
- *“The global deployment of IPv6 is underway, creating an Internet consisting of IPv4-only, IPv6-only, IPv4-IPv6 dual-stack, and IPv6+translation networks and nodes. This deployment must be properly handled to avoid the division of the Internet into separate IPv4 and IPv6 networks, ensuring addressing and connectivity for all IPv4 and IPv6 nodes. IPv6 deployment has resulted in the shutdown of IPv4 in some networks.”*

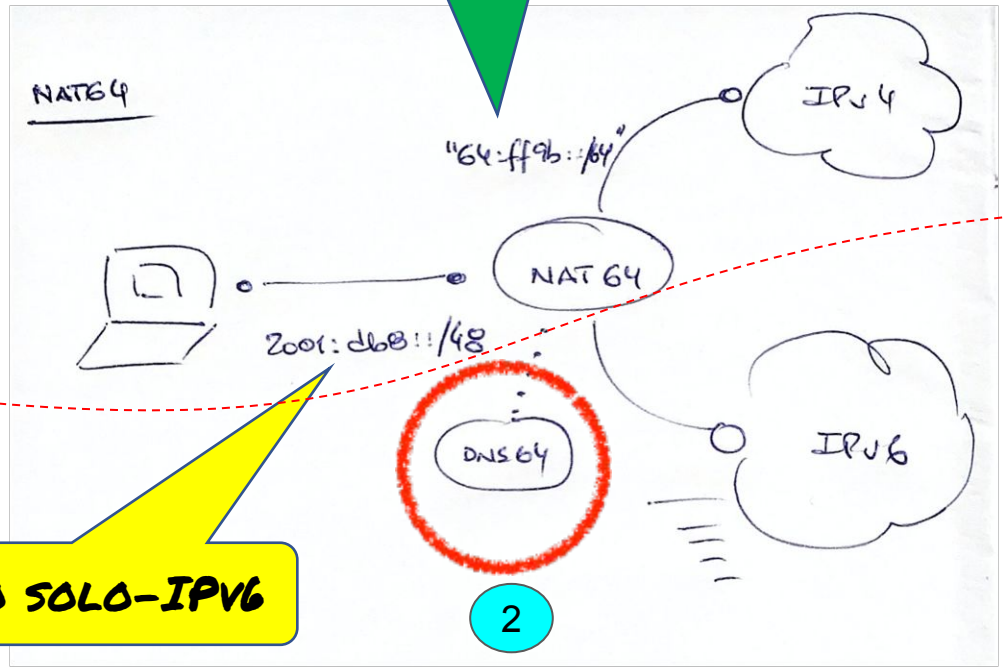
Grupo v6ops

Temas:

- Reacción a los eventos de renumeración (F. Gont)
- Optimizaciones para 464XLAT (J. Palet)
- Descubrimiento del prefijo para NAT64
- Consideraciones operativas de seguridad para redes IPv6

Refresco NAT64

La internet IPv4 se mapea en un prefijo IPv6



1

www.example.com

192.0.2.1

3

64:ff9b::C000:0201

Segmento solo-IPv6

2

v6ops: Descubrimiento del prefijo para NAT64

- El problema:
  - Hay que elegir un prefijo para hacer la traducción de 6 a 4
    - El prefijo “well known” reservado para esto es 64:ff9b::/96
  - Sin embargo, poder descubrir el prefijo puede ser importante (ver RFC7050)
    - Detectar la presencia o no de NAT64
    - Detectar un cambio en el prefijo de mapeo
    - … otros

v6ops: Consideraciones seguridad operacional

- Ultimo draft: https://tools.ietf.org/html/draft-ietf-opsec-v6-21

- Secciones para:
  - Direccionamiento
  - ULAs, p2p, NDP, seguridad en el plano de control
  - Seguridad en entornos “enterprise”
  - Seguridad en entornos “service provider”
  - Usuarios residenciales

v6ops: Consideraciones seguridad operacional

- Algunas citas:
  - *Interfaces de loopback: asignar un único /64 y usar un /128 por dispositivo. De esa forma es sencillo identificar loopbacks y crear ACLs*
  - *Una ACL al ingreso de la red que va a ser aplicada a todas las interfaces de un router DEBERÍA ser configurada de la siguiente manera:*
    - *descartar paquetes OSPFv3 (identificado por el valor del next-header en 89) y paquetes RIPng (identificado por el puerto UDP 21) con dirección de origen en cualquier dirección que no sea link-local*
    - *permitir paquetes BGP (identificados por el puerto TCP 179) con dirección de origen en todos los vecinos BGP y descartar todos los demás orígenes*
    - *permitir todos los paquetes ICMP (en tránsito y dirigidos a las interfaces del propio router)*

v6ops: Consideraciones seguridad operacional (ii)

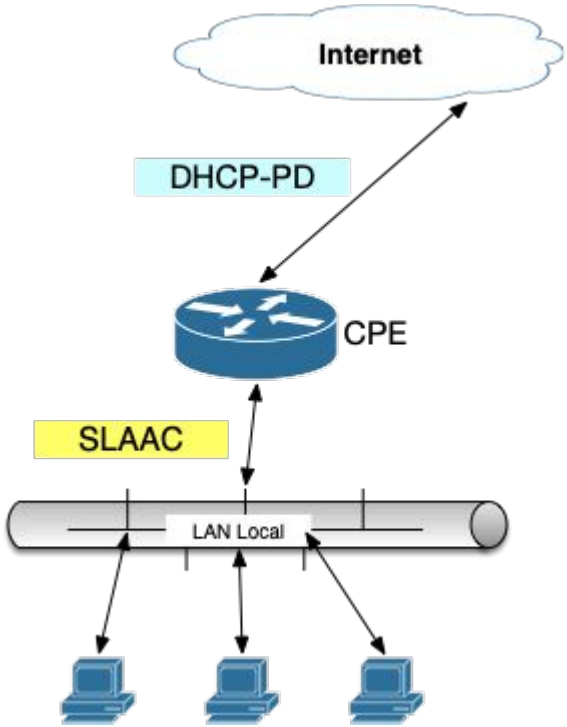
- Algunas citas:
  - *Interfaces punto a punto, se toma la recomendación de la RFC 6164 en cuanto a utilizar /127s para los punto a punto para evitar ataques de ping-pong y de agotamiento del neighbor caché.*
    - [Comentario del relator] se puede tomar un /127 de un /64 y de esa manera aprovechar las ventajas “prácticas” de usar el /64
  - *[hablando de mecanismos de transición] se recomienda bloquear todos los túneles en sus configuraciones por defecto mediante denegar paquetes IPv4 que cumplan con:*
    - *Paquetes con protocol 41*
    - *Paquetes con protocol 47*
    - *Paquetes UDP con puerto 3544*

6man

- Temas:
  - Descubrimiento del prefijo NAT64
    - ¿Les suena?
  - Path MTU Discovery
  - IPv6-Only RA Option

Descubrimiento prefijo NAT64

- Draft: https://tools.ietf.org/html/draft-pref64folks-6man-ra-pref64-02
- Propone una opción para RA donde el router del segmento informe el prefijo NAT64
- Ventajas:
  - No es afectado por los problemas del “DNS externo” (es decir nodos locales que usan *resolvers* externos, como el 8.8.8.8 o los resovers DoH)



Descubrimiento del path MTU

Draft:
https://tools.ietf.org/html/draft-hinden-6man-mtu-option-02

Opción hop by hop

```
ReportedMTU | ReturnPMTU
```

El MTU del camino es el menor de todos los MTU

El draft nuevo propone utilizar un encabezado hop by hop, sin utilizar ICMP

Descubrimiento del path MTU

Opción hop by hop

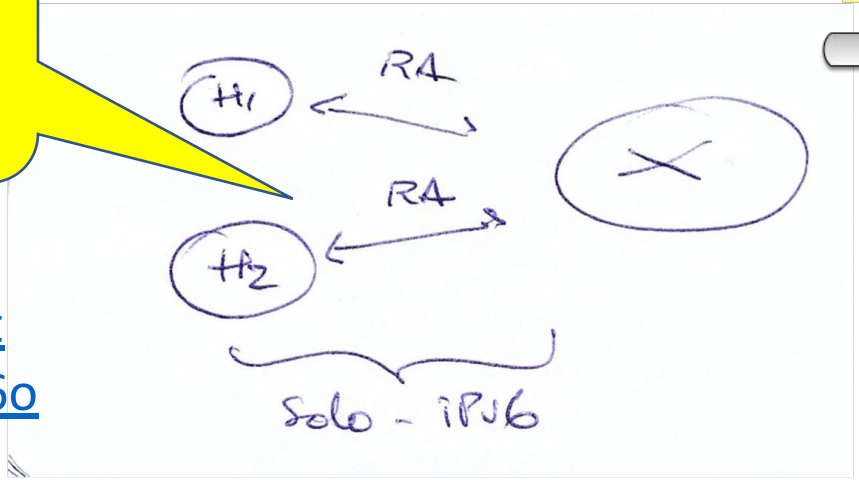
`ReportedMTU | ReturnPMTU`

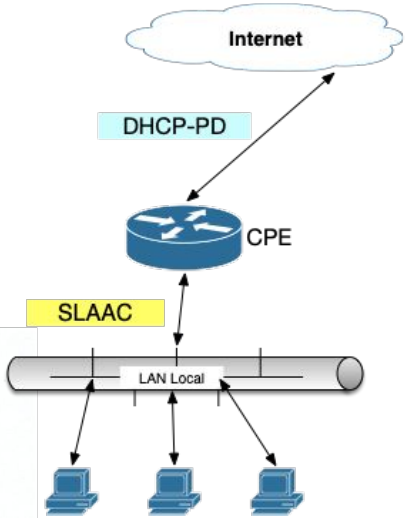
En cada salto el router "reporta" su MTU en caso de ser menor que el valor anterior

Al llegar a destino, el destino devuelve otro mensaje informando el último valor de MTU en el campo ReturnPMTU

IPv6-Only flag para RA

La presencia de este flag indica que no hay otras versiones de IP en uso _intencional_ en este segmento de red





Draft:
https://tools.ietf.org/html/draft-ietf-6man-ipv6only-flag-05

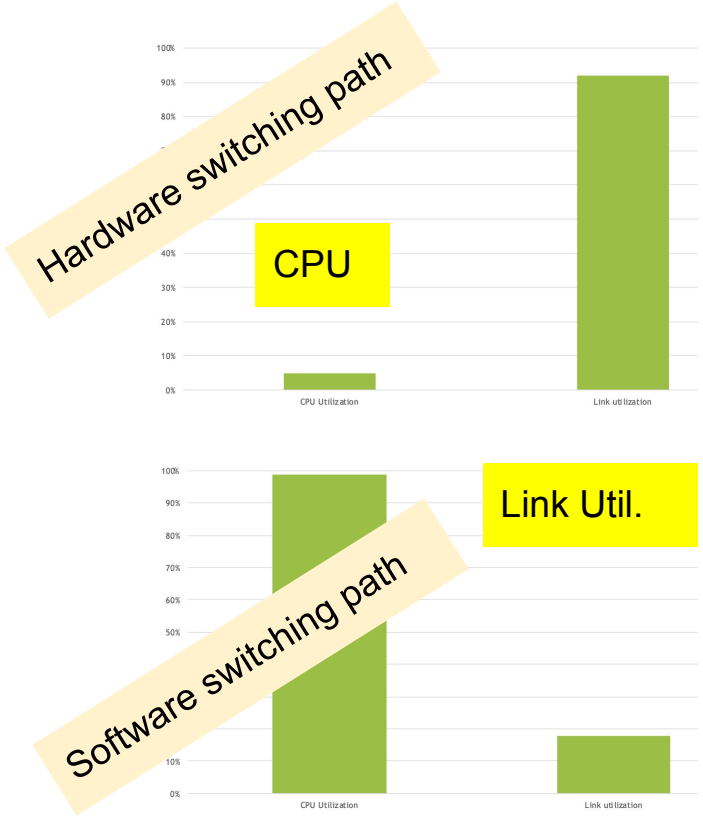
¿Qué está pasando en los NOGs?

NANOG

- NANOG: North American Network Operators Group
  - https://www.nanog.org/, dos eventos por año, en 2019 fueron el 76 y 77
- *IPv6 Adoption is Killing my Throughput*
  - Crítica al uso de DHCP option 82
- *Segment Routing with mapped IPv6*
- MPLS como estrategia de migración y de interconexión de nubes IPv6 sobre redes IPv4

NANOG: *IPv6 Adoption is Killing my Throughput*

- ¡IPv6 está matando mi performance!
- El problema que se describe, afecta a servicios hogareños:
  - Todo router tiene dos “caminos” para conmutar paquetes: uno acelerado por hardware y el otro procesado enteramente por software.
  - El camino de hardware es de mucha mejor performance que el de software
  - En ciertos casos, la combinación de método de despliegue de IPv6 (DHCP opción 82) con el tipo de CPE usado hace que el tráfico IPv6 vaya por el camino de conmutación lento.



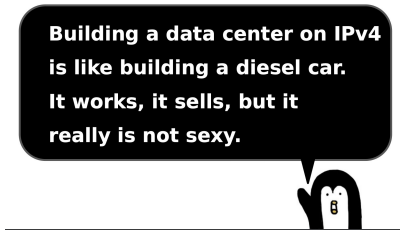
RIPE

- RIPE es el registro de direcciones para la región de Europa y Oriente Medio
  - Realiza dos eventos técnicos al año, en 2019 fueron RIPE 79 (https://ripe79.ripe.net/archives/) y RIPE 78 (https://ripe78.ripe.net/archives/)

- Temas IPv6:
  - IPv6-only Datacenters

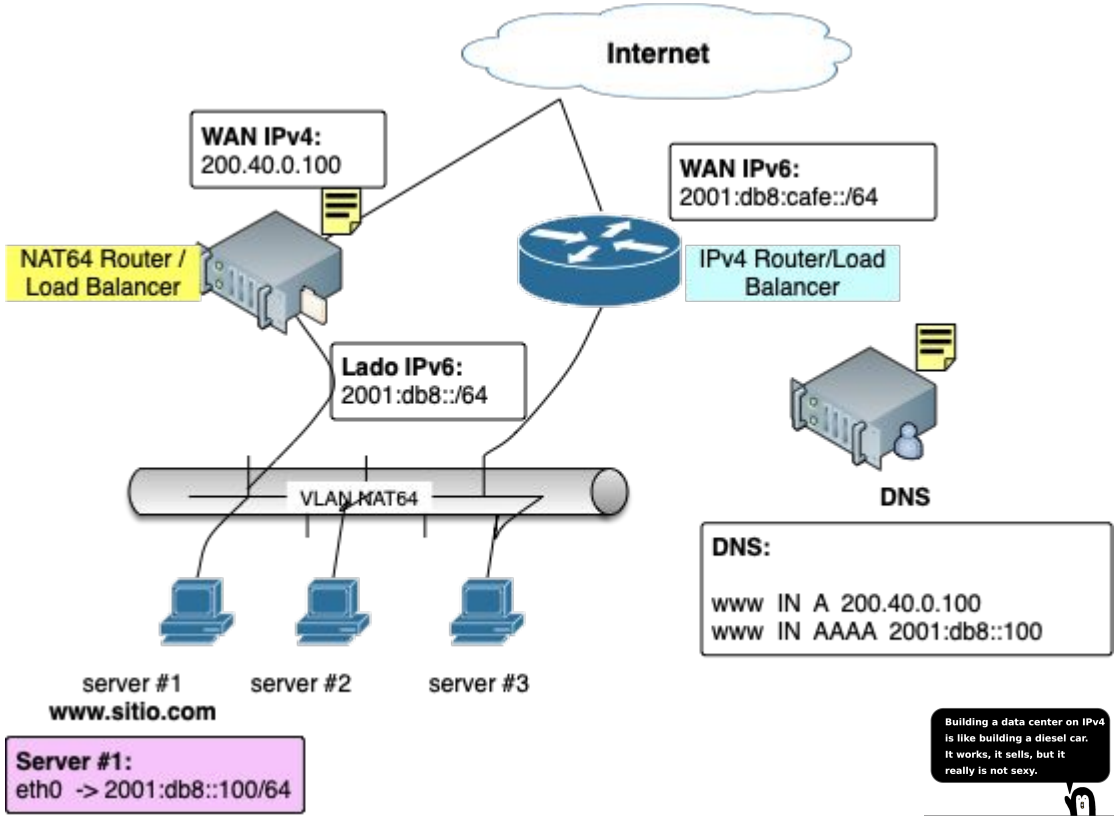
RIPE - IPv6 Only Datacenters

- Presentación original
  - https://ripe79.ripe.net/presentations/19-How-to-Build-Maintain-and-Market-an-IPv6-only-Data-Center-RIPE79.pdf
- Motivación:
  - Los datacenters son grandes consumidores de direcciones IP, existe una oportunidad para reciclar IPs públicas de ellos
- Técnicas posibles:
  - NAT64 en el borde del datacenter, todos los servidores utilizan IPv6 solamente
- Desafíos:
  - Servicios que solo escuchan en la “0.0.0.0”, uso de literales IPv4 en aplicaciones web
  - Limitaciones del hardware (IPv4-only pxe boot!)



RIPE - IPv6 Only Datacenters

- El **server#1** solo tiene numeración IPv6
- En DNS el www tiene tanto A como AAAA
- La dirección IPv4 está en el lado público del NAT64



Foro Técnico de LACNIC - LACNOG

Temas discutidos recientemente:

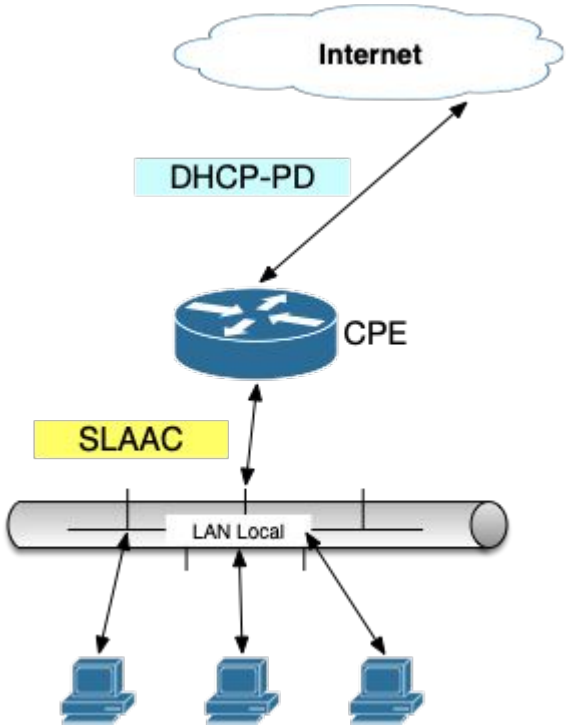
- Foro Técnico de LACNIC
  - 464XLAT en Redes de Cable (Alejandro D'Egidio)
  - Identificando Open Resolvers en IPv6 (Alejandro Acosta)

- LACNOG:
  - Reacción de SLAAC a eventos de renumeración (Fernando Gont)
  - Consideraciones para el despliegue de 464XLAT en redes de operadores (J. Palet)

SLAAC: Reacción frente a eventos de renumeración

¿Cuál es el problema?

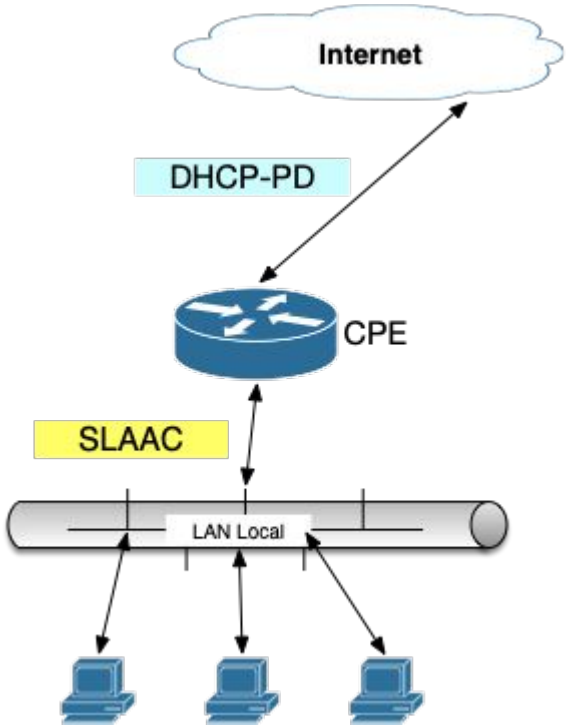
- El CPE recibe un prefijo por DHCP-PD y lo publica hacia la LAN por SLAAC
  - Los anuncios de SLAAC incluyen un “time to live” del prefijo
- Si por alguna razón el CPE se reinicia, pide un nuevo prefijo, y lo anuncia
- ¡Pero el viejo persiste en los clientes!
- Esto puede crear situaciones donde hay inestabilidad en la conectividad o fallas



SLAAC: Reacción frente a eventos de renumeración

¿Cuáles pueden ser las posibles soluciones?

- Operativas:
  - Utilización de prefijos estables por parte de los operadores
  - Utilización de CPEs que guardan estado de cual fue el último prefijo que utilizaron
- Mejoras a nivel de protocolo:
  - Los clientes podrían darse cuenta que el mismo router ahora está anunciando otro prefijo y tomar acciones en consecuencia



GTER

- GTER es el *Grupo de Trabalho de Engenharia e Operacao de Redes*, el grupo de operadores de red (NOG) de Brasil

- Temas relacionados con IPv6 que se han discutido recientemente:

    - Problemas con ciertos proveedores de equipamiento de cliente (CPEs)

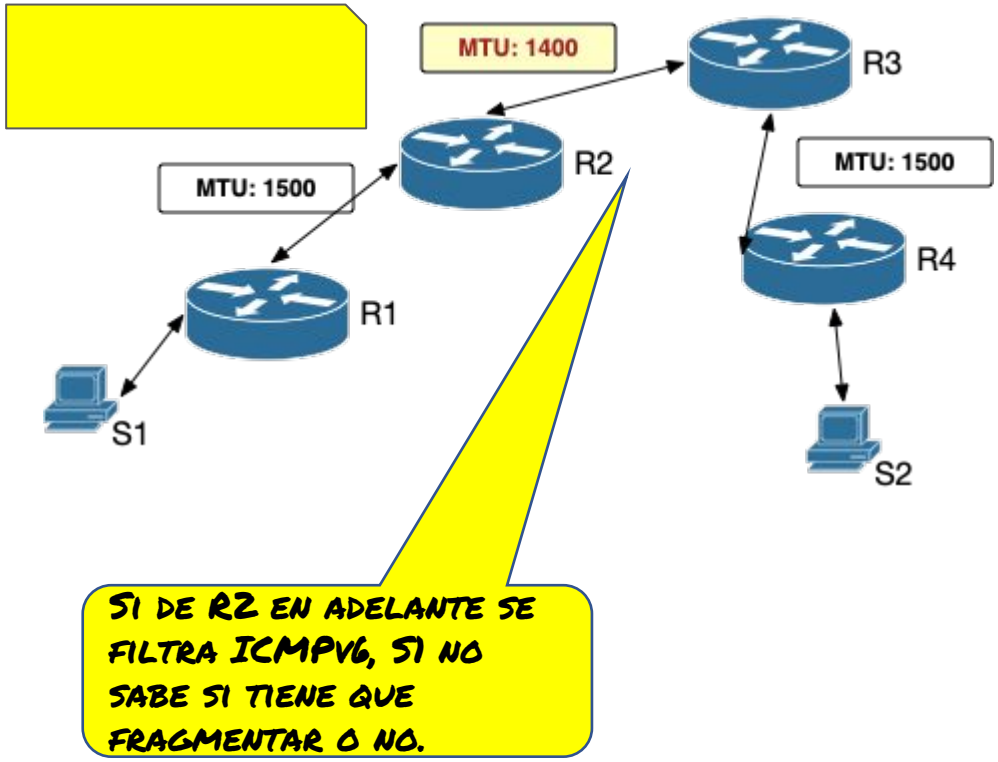
    - Problemas de servicio con algunos sitios que habilitan IPv6 sin tener en cuenta algunos aspectos:

        - El enrutamiento en IPv6 puede tener una topología diferente a la de IPv4
        - La configuración de filtros tiene que acompañar a la de IPv4 y ser equivalente
        - No hay que filtrar irresponsablemente el ICMPv6 (blackhole por falla en la detección de pMTU)

pMTU Blackhole

Recordar:

- en IPv6 solamente los extremos de la comunicación fragmentan
- si los extremos no se enteran que necesitan fragmentar, no lo hacen
- ¿Como se enteran? ***pMTU Discovery***



¡ Muchas gracias !