Seguridad IPv6

Fernando Gont

6 de Julio de 2022

Consideraciones generales sobre seguridad IPv6

Aspectos interesantes sobre seguridad IPv6

- IPv6 afecta transversalmente a la organización
- Tenemos menos experiencia con IPv6 que con IPv4
- Falta de recursos humanos bien capacitados en seguridad IPv6
- Muchos dispositivos tienen el soporte IPv6 habilitado por defecto
- Las implementaciones de IPv6 son menos maduras que las de IPv4
- Productos de seguridad tienen menos soporte para IPv6
- Aumenta la complejidad de la red Internet:
  - Dos protocolos de internet (IPv4 e IPv6)
  - Mayor uso de NATs (NAT64, CGNAT) y tùneles

Breve comparación entre IPv6 e IPv4

Breve comparación entre IPv6 e IPv4

- Similares en *funcionalidad*, pero **no** en *mecanismos*

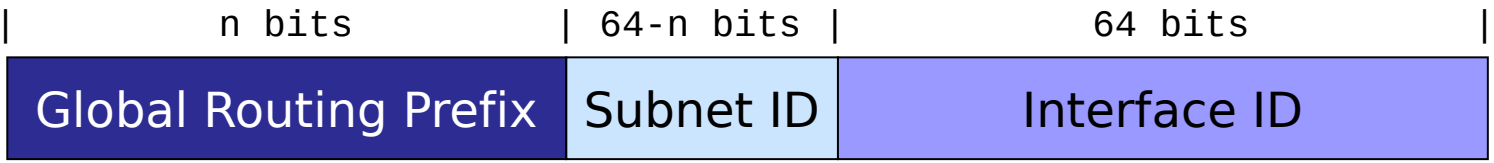
	IPv4	IPv6
Direccionamiento	32 bits	128 bits
Extensibilidad	Limitada	Ilimitada
Resolución de Direcc.	ARP	ND (+ MLD)
Config. automática	DHCP	SLAAC & DHCPv6 (+MLD)
Aislamiento de fallos	ICMPv4	ICMPv6
Soporte IPsec	Opcional	Opcional
Fragmentación	En hosts y en routers	Sólo en hosts

Direccionamiento

Breve reseña

- De manera similar a IPv4,
  - Las direcciones se “agregan” en prefijos con el propósito de ruteo
  - Existen distintos tipos de direcciones (unicast, anycast, y multicast)
  - Existen distintos tipos de “alcances” (link-local, global, etc.)
- Se utilizan simultanteamente múltiples direcciones de:
  - Distinto alcance (link-local, global, etc.)
  - Distinto tipo (unicast, multicast, etc.)
  - Distinta estabilidad (estables vs. temporales)
- La sub-red por defecto es un /64
- Los sistemas normalmente autoconfiguran sus direcciones (SLAAC)

IPv6 Global Unicast Addresses



- Donde:
  - GRP: Prefijo global de ruteo, delegado por el upstream o por un RIR
  - Subnet ID: Igual que IPv4
  - Interface ID (IID): Análogo al Host-ID de IPv4

¿Qué está afectado por el direccionamiento IPv6?

- Todo sistema que utilice direcciones:
  - Servers y Workstations
  - Aplicaciones de red
  - Infraestructura de red
- Todo sistema/aplicación que procese direcciones:
  - SIEM
  - IPAM
  - Aplicaciónes de marketing con GeoIP
- Recursos humanos involucrados en los anteriores items

Correlación de actividad

- En el caso usual (SLAAC) no existe una bitácora que almacene:

  Nodo ↔ Dirección IP ↔ Direccion MAC

- Si preciso tal cosa, puede que tenga que:
  - Correr software en la red
  - Obtener esta información de dispositivos de red
  - Extraer esta información periódicamente con un agente de SIEM
  - Forzar el uso de DHCPv6 (de ser posible)

Mitigación de ataques

- Se suele mitigar ataques bloqueando direcciones IP
  - Ejemplo: fail2ban
- En IPv6, el atacante tiene un /64 (al menos) a disposicón
  - Puede tener que cambiarse la granularidad de bloqueo a un /64
- Pero potencialmente también podría obtener un /56 o /48
  - Por lo que puede tener que escalarse la granularidad de bloqueo
  - Probablemente las herramientas actuales no puedan hacerlo automáticamente

Auditoría/pentesting

- En muchos escenarios el IID de una dirección es aleatorio
- Esto puede dificultar la tarea de “reconocimiento¨:
  - Los escaneos de direcciones “por fuerza bruta” son imposibles
  - Las herramientas de seguridad suelen tener mal soporte para IPv6
- Algunas técnicas posibles:
  - Escaneos “inteligentes” de direcciones
  - Metodos de reconocimiento alternativos
    - DNS (reverse zone), Certificate Transparency Framework (certificados publicos)
  - Auditorías utilizando fuentes de información
    - Netbox, LIbreNMS, DNS zone configuration

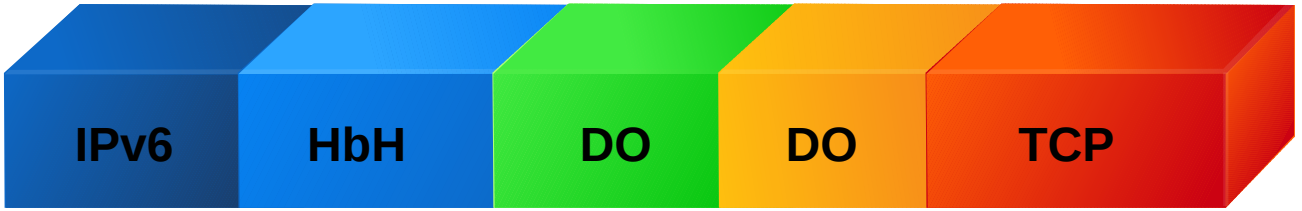
Exposición en Red

- Potencialmente puede aumentar la exposición en red
  - En el caso general, los sistemas contarán con direcciones globales
  - Normalmente no se utiliará NAT en IPv6
  - En principio todo sistema está expuesto a Internet
- Algunas opciones:
  - Desplegar firewalls de red que “solo permitan conexiones salientes”
  - Desplegar firewalls en los hosts
  - Utilizar IPv6-only donde sea posible

Extensibilidad

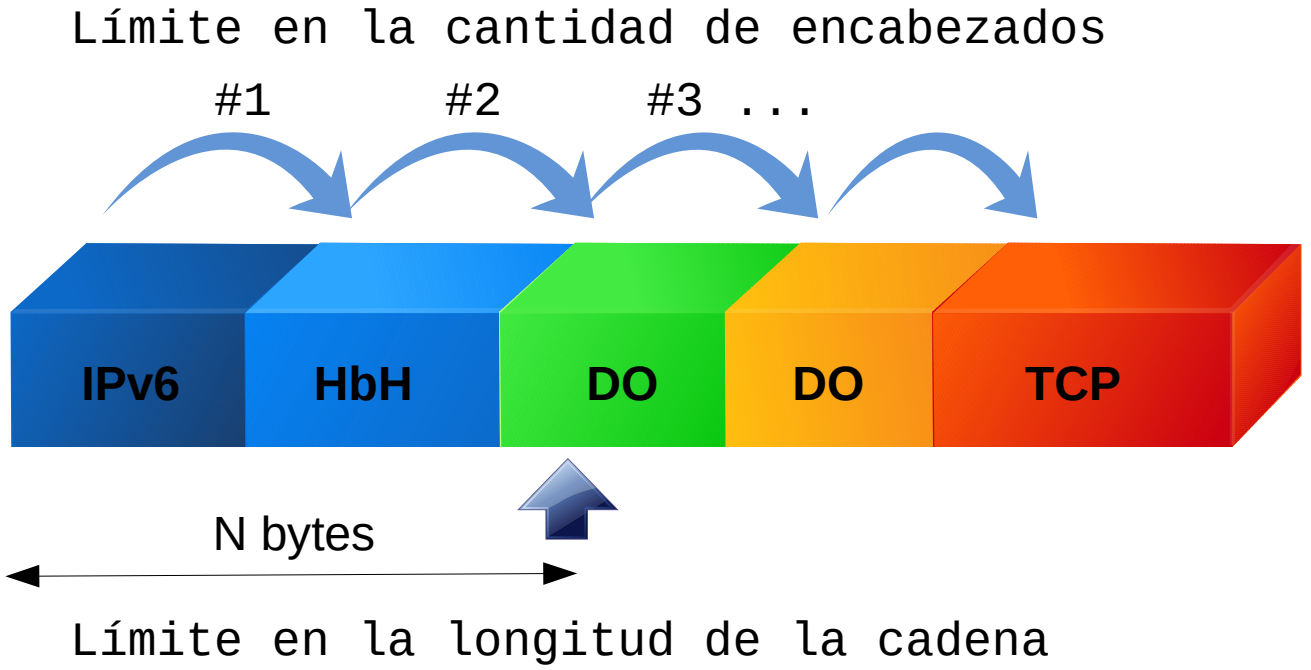
Breve reseña

- Las opciones IPv6 se incluyen en “encabezados de extensión”
  - Estos encabezados se encuentran entre el encabezado IPv6 y el “payload”
  - Pueden haber multiples instancias, de multiples tipos de encabezados, cada uno con multiples opciones
- Estructura de paquete resultante:

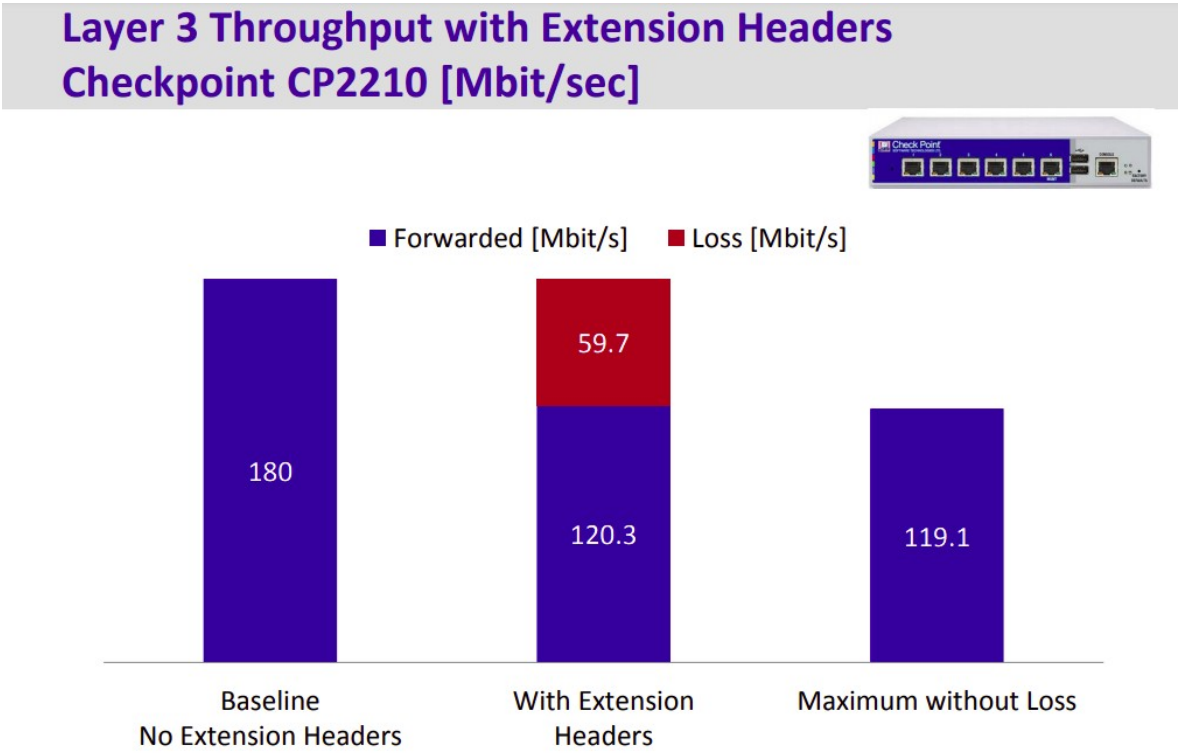


Implicancias generales en seguridad

- Impacto negativo en el funcionamiento de los sistemas

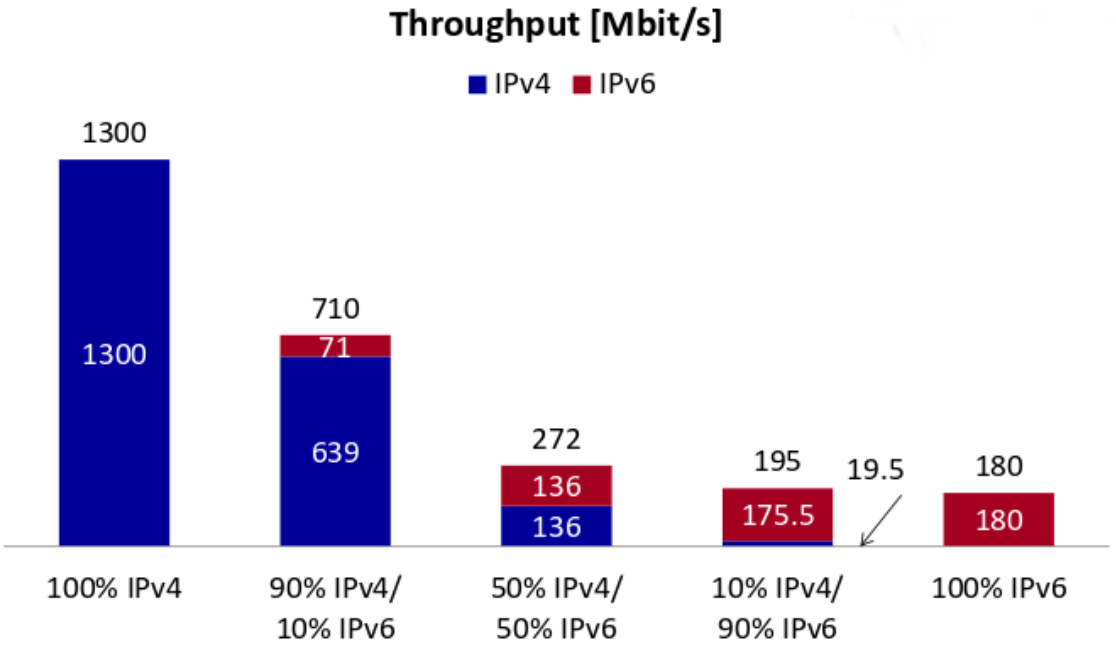


Impacto de los encabezados de extensión



Procesamiento de tráfico IPv6 vs. IPv4

- Muchos productos no tienen paridad de funcionalidad



Zack, E. “Firewall Security Assessment and Benchmarking IPv6 Firewall Load Tests”. IPv6 Hackers meeting #1. Berlin, July 2013. See: https://www.ipv6hackers.org

Implicancias de seguridad de IPv6 en redes IPv4

Paridad de políticas de seguridad

- Politicas para IPv6 e IPv4 se suelen configurar por separado
- Muy usualmente esto lleva a falta de paridad, lo cual es inadecuado
- Opciones:
  - Configuración conjunta en la medida de lo posible
  - Asegurar siempre la paridad de políticas de seguridad

Fugas de tráfico VPN

- Escenario típico:
  - Te conectas a una red insegura
  - Utilizas un cliente VPN para conectarte a tu organización
  - **Tu cliente VPN no soporta IPv6**
- Esto resulta en una fuga de tráfico VPN
  - Puede ocurrir naturalmente (red local con soporte IPv6)
  - Puede ser disparado por un atacante intencionalmente.

Plan de acción

Plan de Acción

- Educación/entrenamiento
- Elaboración de un Plan de Despliegue
  - Considerarando los aspectos de seguridad en el propio Plan
  - Capacitando y conscientizando a todos los afectados
- Es hora de tener un Plan de Despliegue de IPv6!

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com