Resultados de un análisis de seguridad de IPv6

Fernando Gont

(UTN/FRH, Argentina)

CONATEL 2011

20 de Mayo de 2011. Arequipa, Perú

Agenda

- Objetivos de este tutorial
- Breve comparación de IPv6/IPv4
- Discusión de aspectos de seguridad de IPv6
- Seguridad de los mecanismos de transición/co-existencia
- Implicancias de seguridad de IPv6 en redes IPv4
- Áreas en las que se necesita progreso
- Conclusiones
- Preguntas y respuestas

Consideraciones generales sobre seguridad IPv6

Aspectos interesantes sobre seguridad IPv6

- Se cuenta con mucha menos experiencia que con IPv4
- Las implementaciones de IPv6 son menos maduras que las de IPv4
- Los productos de seguridad (firewalls, NIDS, etc.) tienen menos soporte para IPv4 que para IPv6
- La complejidad de las redes se incrementará durante el periodo de transición/co-existencia:
  - Dos protocolos de red (IPv4 e IPv6)
  - Mayor uso de NATs
  - Mayor uso de túneles
  - Uso de otras tecnologías de transición
- Pocos recursos humanos bien capacitados

…y así y todo IPv6 será en muchos casos la única opción disponible para continuar en el negocio de Internet

Comparación entre IPv6 e IPv4

Breve comparación de IPv4 e IPv6

- IPv4 e IPv6 son muy similares en términos de *funcionalidad* (no así de *mecanismos*)

	IPv4	IPv6
Direccionamiento	32 bits	128 bits
Resolución de direcciones	ARP	ICMPv6 NS/NA (+ MLD)
Auto-configuración	DHCP & ICMP RS/RA	ICMPv6 RS/RA & DHCPv6 (recomendado) (+ MLD)
Aislamiento de fallas	ICMP	ICMPv6
Soporte de IPsec	Opcional	Recomendado (**no** mandatorio)
Fragmentación	Tanto en hosts como routers	Sólo en hosts

Implicancias de Seguridad de IPv6

Direccionamiento

Breve reseña

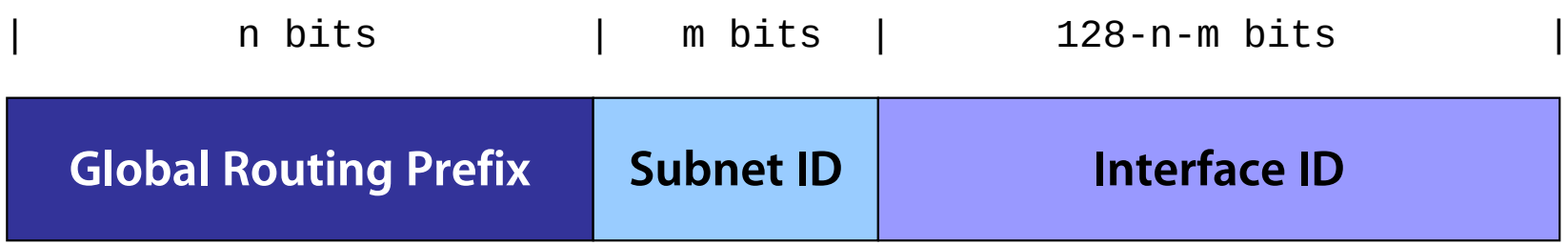
- El principal motivador de IPv6 es su mayor espacio de direcciones
- IPv6 utiliza direcciones de 128 bits
- De manera similar a IPv4,
  - Las direcciones se “agregan” en prefijos para su ruteo
  - Se definen distintos tipos de direcciones (unicast, anycast, y multicast)
  - Se definen distintos alcances para las direcciones (link-local, global, etc.)
- Lo usual es que en un determinado instante, un nodo use varias direcciones, de distintos tipos y alcances. Por ej.,
  - Una o mas direcciones link-local unicast
  - Una o mas direcciones global unicast
  - Una o mas direcciones link-local multicast

Direccionamiento

Implicancias en scanning

Direcciones Global Unicast

- Formato de las direcciones IPv6 unicast globales:



- El Interface ID es típicamente de 64 bits
- Las direcciones unicast globales pueden "generarse" con distintos criterios:
  - Formato EUI-64 modificado (embebiendo direcciones de capa de enlace)
  - Direcciones "temporales" (o sus variantes)
  - Patrones predeterminados por el administrador (por ej., 2001:db8::1)
  - De acuerdo a lo especificado por una tecnología de transición/co-existencia

Implicancias en “brute-force scanning”

- Asumiendo que las direcciones de los hosts están uniformemente distribuídas en la subred, sería muy difícil realizar un “escaneo por fuerza bruta”
- Sin embargo, estudios realizados (*) indican que este no es necesariamente el caso: las direcciones suelen generarse con patrones predeterminados. Basicamente,
  - SLAAC (Interface-ID derivado de la MAC address)
  - Basadas en IPv4 (por ej., 2001:db8::192.168.10.1)
  - “Low byte” (por ej., 2001:db8::1, 2001:db8::2, etc.)
  - Privacy Addresses (Interface-ID aleatorio)
  - “Wordy” (por ej., 2001:db8::dead:beef)
  - Relacionadas con tecnologías de transición (por ej., Teredo)

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Algunos datos reales….

- [Malone, 2008] (*) midió las direcciones asignadas a clientes y routers:

Clientes

Tipo de dirección	Porcentaje
SLAAC	50%
Basada en IPv4	20%
Teredo	10%
Low-byte	8%
Privacy	6%
wordy	<1%
Otras	<1%

Routers

Tipo de dirección	Porcentaje
Low-byte	70%
Basada en IPv4	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Otras	<1%

(*) Malone, D. 2008. *Observations of IPv6 Addresses*. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

Algunas recomendaciones

- Para servidores, la política de generación de direcciones es generalmente irrelevante
- Para clientes, en escenarios generales es deseable el uso de extensiones de privacidad:
  - Algunas variantes implementan las extensiones especificadas en RFC 4941
  - Otras implementaciones generan el Interface-ID a partir de un hash sobre el prefijo de autoconfiguración, la MAC address de la interfaz, y un secreto)
- Para nodos que no necesiten ser “alcanzables”, es deseable la asignación de direcciones “no previsibles”
- En todos los casos anteriores, se debe considerar si es deseable implementar una política de filtrado de paquetes

Conclusiones

- IPv6 incrementa la dificultad de realizar "brute force scanning"
- Sin embargo, es esperable las herramientas utilizadas por atacantes evolucionen, permitiendo reducir el espacio de búsqueda.
- Asimismo, es probable que se exploren otros métodos de scanning:
  - Direcciones expuestas por protocolos de aplicación (P2P, e-mail, etc.)
  - Direcciones multicast (por ej., all-nodes multicast address)
  - Protocolos de descubrimiento de vecinos (por ej., mDNS)

Direccionamiento

Conectividad “extremo a extremo” (“end-to-end”)

Breve reseña

- Dado que IPv6 posee un gran espacio de direcciones, se espera que cada dispositivo conectado a la red cuente con una dirección IPv6 global unica.
- Es usual asumir que esto “devolverá” a la Internet el principio conocido como “end-to-end”:
  - La comunicación entre sistemas es transparente (por ej., los nodos intermedios no modifican los paquetes)
  - Cualquier sistema de la red es capaz de establecer una comunicación con cualquier otro sistema de la red
  - Usualmente se argumenta que esto permitiría la “innovación” en la red

Consideraciones varias

- El hecho de que cada sistema posea una dirección global única no garantiza la posibilidad de comunicación “extremo a extremo”
  - Esta no es necesariamente una propiedad “deseable” en una red de producción
  - Por tal motivo, es de esperar que una subred IPv6 típica (como ser una red hogareña) esté protegida por un firewall stateful que solo permita el tráfico “de retorno” (aquél en respuesta a comunicaciones iniciadas desde el interiore de la red)
- La realidad es que la mayoría de las redes de hoy en día no tienen como fin la innovación, sino que son un medio para trabajar o recrearse
- Y los servicios esperados por los usuarios son aquellos mismos que hoy se brindan en IPv4 sin conectividad “end-to-end” (web, email, redes sociales, etc.)

ICMPv6

(Internet Control Protocol version 6)

Internet Control Message Protocol version 6

- ICMPv6 es un componente fundamental de la suite IPv6 suite, y se utiliza para:
  - Aislamiento de fallas (errores ICMPv6)
  - Troubleshooting (ICMPv6 echo request/response, etc.)
  - Resolución de direccíones
  - StateLess Address Auto-Configuration (SLAAC)

Mensajes de error ICMPv6

- El RFC 4443 define una variedad de mensajes de error:
  - Destination Unreachable
    - No route to destination
    - Beyond scope of source address
    - Port Unreachable, etc.
  - Packet Too Big
  - Time Exceeded
    - Hop Limit Exceeded in Transit
    - Fragment reassembly time exceeded
  - Parameter Problem
    - Erroneous header field encountered
    - Unrecognized Nect Header type encountered
    - Unrecognized IPv6 option encountered
- Claramente, la mayoría de ellos tienen un análogo en IPv4.

Mensajes de error ICMPv6

- Los mensajes de error ICMPv6 podrían utilizarse para realizar ataques de denegación de servicio (ver RFC 5927)
- En general, filtrar dichos mensajes trae aparejado:
  - Incremento en la dificultad para hacer troubleshooting
  - Posibles penalidades de performance (por ej., delays a a hora de establecer nuevas conexiones TCP)
- De manera análoga a ICMPv4, lo mensajes ICMPv6 “Packet Too Big” **no** deben ser filtrados
  - Hacerlo rompería el mecanismo PMTUD

ICMPv6 Redirect

- Los mensajes ICMPv6 Redirect son muy similares a sus homónimos en IPv4.
- Permiten especificar, para una dirección destino determinada, un mejor “receptor” de los paquetes.
- Los ICMPv6 redirect son una optimización –- pueden ser deshabilitados sin que esto tega implicancias de interoperabilidad.
- De cualquier modo, dado que la especificación exige que los mensajes recibidos tengan un Hop Limit de 255, estos mensajes solo pueden ser explotados en al red local.

Mensajes ICMPv6 Informational

- Echo Request/Echo response:
  - Utilizados por “ping6”, con propositos de troubleshooting
  - Puede ser explotado apra network reconnaissance
  - Algunas implementaciones para clientes “ignoran” los “echo request” recibidos
- Node Information Query/Response
  - Especificados en el RFC 4620 como “Experimentales”, pero con soporte (y habilitado por defecto) en KAME.
  - Se envían peticiones sobre un nombre o dirección de red (IPv4 or IPv6), solicitando el nombre del nodo, direcciones IPv4, o direcciones IPv6.
  - El comando ping6 permite enviar mensajes de tipo Node Information Queries (mediante las opciones “-a” y “-b”)
  - Dado que no son ampliamente soportados, ni tampoco útiles en la práctica, es recomendable deshabilitar el soporte en cuestión

Resolución de Direcciones

Breve reseña

- Para resolver direcciones IPv6 en direcciones de capa de enlace se utiliza el mecanismo denominado “Neighbor Discovery”
- El mismo se basa en el protocolo ICMPv6
- Los mensajes ICMPv6 Neighbor Solicitation y Neighbor Advertisement cumplen una función análoga a la de ARP request y ARP reply en IPv4

Implicancias de seguridad

- Como era de esperar, en IPv6 pueden realizarse ataques análogos a los de “ARP spoofing” de IPv4
- Por ejemplo, el atacante falsifica mensajes “Neighbor Advertisement” cuando recibe un “Neighbor Solicitation”
- Este tipo de ataque puede ser utilizado con el el fin de:
  - Man In The Middle (MITM)
  - Denegación de Servicio (DoS)
- Desde hace bastante tiempo que existen herramientas para realizar este ataque (por ej., THC’s IPv6 Attack Suite)

Posibles contramedidas

- Algunas técnicas de “mitigación” posibles son:
  - Desplegar SEND (SEcure Neighbor Discovery)
  - Monitorear el tráfico de Neighbor Discovery (por ej. con NDPMon)
  - Usar entradas estáticas en el Neighbor Cache
  - Restringir el acceso a la red
- Lamentablemente,
  - SEND es difícil de desplegar (requiere de una PKI)
  - Las herramientas de monitoreo son posibles de evadir
  - El uso de entradas estáticas “no escala” para el caso general
  - No siempre es posible restringir el uso a una red
- En síntesis, la situación no es tan diferente a la de IPv4

Autoconfiguración (SLAAC)

Breve reseña

- Existen en IPv6 básicamente dos mecanismos para la autoconfiguración de hosts
  - Stateless: SLAAC (Stateless Address Auto-Configuration), basado en mensajes ICMPv6 (Router Solicitation y Router Advertisement)
  - Stateful: DHCPv6
- SLAAC es mandatorio, mientras que DHCPv6 es “recomendado”
- En SLAAC, los router envían mensajes “Router Advertisement”, comunicando información de configuración a los “hosts” del segmento de red en cuestión, como ser:
  - Prefijos a utilizar
  - Rutas
  - Valores para distintos parámetros (Hop Limit, MTU, etc.)
  - Tiempos recomendados para la utilización de las direcciones generadas
  - etc.

Implicancias de seguridad

- Un atacante podría falsificar mensajes “Router Advertisement” cuando recibe un “Router Solicitation” y/o enviar estos mensajes periodicamente
- Este tipo de ataque puede ser utilizado con el el fin de:
  - Man In The Middle (MITM)
  - Denegación de Servicio (DoS)
- Desde hace bastante tiempo que existen herramientas para realizar este ataque (por ej., THC’s IPv6 Attack Suite)

Posibles contramedidas

- Algunas técnicas de “mitigación” posibles son:
  - Desplegar SEND (SEcure Neighbor Discovery)
  - Monitorear el tráfico de Neighbor Discovery (por ej. con NDPMon)
  - Utilizar RA guard (Router Advertisement guard)
  - Restringir el acceso a la red
- Lamentablemente,
  - SEND es difícil de desplegar (requiere de una PKI)
  - Las herramientas de monitoreo son posibles de evadir
  - Es posible evadir RA guard
  - No siempre es posible restringir el uso a una red
- En síntesis, la situación no es tan diferente a la de IPv4

Soporte de IPsec

Breve reseña y consideraciones

- Actualmente, se el soporte de IPsec es mandatorio en toda implementación de IPv6 (y opcional en IPv4) – aunque la IETF está en proceso de cambiar este requerimiento
- Sin embargo, a los fines prácticos, esto es completamente irrelevante:
  - Es/era mandatorío el *soporte* de IPv6 – no así su *utilización*
  - Así y todo, existen muchas implementaciones IPv4 con soporte IPsec, como también implementaciones IPv6 sin soporte IPsec
- Existen en IPv6 básicamente los mismos problemas para el despliegue de IPsec que en IPv4
- Por tal motivo, no existen motivos para esperar más uso de IPsec con IPv6 que el que se tiene con IPv4

Seguridad de los Mecanismos de Transición/Co-existencia

Breve reseña

- El plan original de transición era el uso de dual-stack (*si, este plan falló*)
- La estrategia actual es un plan de transición/co-existencia basado en un grupo de herramientas:
  - Dual Stack
  - Túneles “configurados”
  - Túneles automáticos (ISATAP, 6to4, Teredo, etc.)
  - Traducción (por ej., NAT64)
- Algunas variantes de túneles automáticos (como Teredo e ISATAP) están habilitados por defecto en Windows Vista y Windows 7

Implicancias de seguridad

- La mayoría de estas tecnologías incrementan la complejidad de la red, y así las potenciales vulnerabilidades
- Muchas de estas tecnologías introducen Puntos Únicos de Falla ("Single Point of Failure") en la red.
- Algunas de ellas han sido explotadas para violar políticas de seguridad, ya que en ocasiones no son tenidas en cuenta por firewalls y NIDS
- Algunos de estos mecanismos merecen consideraciones de privacidad:
  - ¿Por dónde circula su tráfico Teredo, 6to4, o Tunnel Broker?
  - Esto puede (o no) ser importante para su red

Implicancias de seguridad de IPv6 en redes IPv4

Breve reseña

- Muchos sistemas tienen IPv6 habilitado “por defecto” – por ej. Linux, *BSD, y Windows Vista/7
- Algunos sistemas como Windows Vista/7 tienen, adicionalmente, soporte de tecnologías de transición/co-existencia habilitadas “por defecto” – por ej. Teredo e ISATAP
- Incluso si una red supone ser “IPv4-only”, este soporte existe, y puede ser utilizado sin la decisión explícita del administrador de red/seguridad

Explotación del soporte IPv6 nativo

- Un atacante con acceso a una red local podría "oficiar" como router IPv6, enviando mensajes Router Advertisement (RA) falsificados. (*)
- Todos los sistemas con soporte IPv6 nativo configurarían direcciones IPv6
- Esto podría permitir que se evadan controles de filtrado de tráfico y/o NIDS
- Posibles contramedidas:
  - Implementar controles de seguridad IPv6, incluso en redes IPv4
  - Deshabilitar el soporte IPv6 nativo en los sistemas de redes IPv4-only

(*) http://resources.infosecinstitute.com/slaac-attack/

Explotación de Tecnologías de transición/co-existencia

- Algunos sistemas incluyen soporte de tecnologías de transición habilitado por defecto.
- Estas tecnologías podrían ser explotadas para evadir controles en la red.
- Tecnologías como Teredo podrían resultar en que incluso hosts que están detrás de NATs quedaran expuestos a la red pública (Internet)
- Posibles contramedidas:
  - Implementar controles de seguridad IPv6 en redes IPv4
  - Deshabilitar el soporte de estas tecnologías
  - Implementar políticas de filtrado que impidan el uso de estas tecnologías

Filtrado de Tecnologías de Transición

Tecnología	Regla de filtrado
Dual-Stack	Automático
IPv6-in-IPv4 tunnels	IPv4 Protocol == 41
6to4	IPv4.Protocol == 41 IPv4.{src,dst} == 192.88.99.0/24
ISATAP	IPv4 Protocol == 41
Teredo	IPv4.dst == known_teredo_servers && UDP.DstPort == 3544
TSP	IPv4.dst == known_teredo_servers && {TCP,UDP}.dst == 3653

Conclusiones

- Incluso si una red no espera utilizar IPv6, debe tener en cuenta las implicancias de seguridad de este protocolo (por ej. en lo que respecta a filtrado y monitoreo)
- Si se espera que en una red IPv4 no se utilicen mecanismos de transición/co-existencia, se deberían aplicar las políticas de filtrado correspondientes

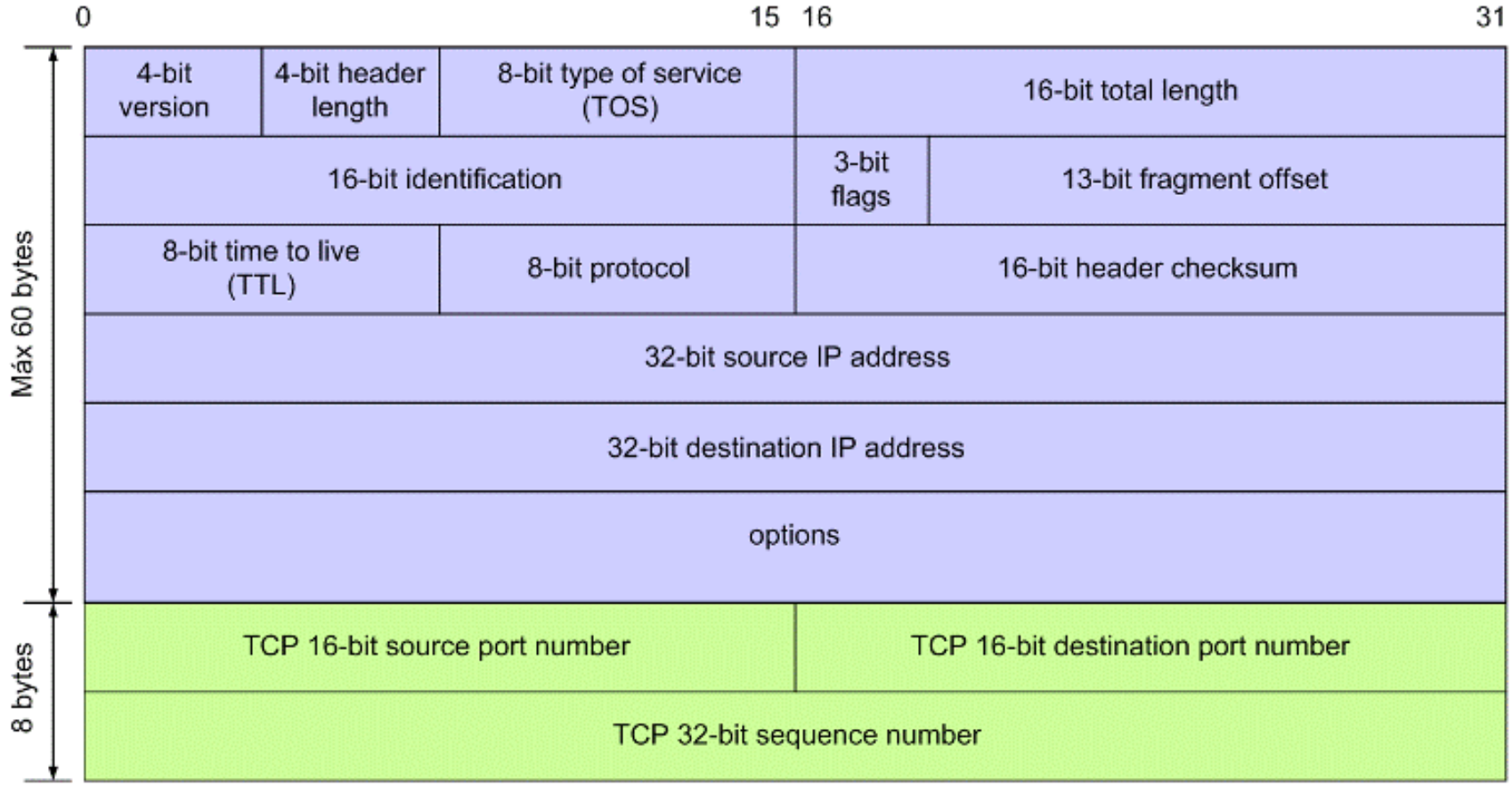
Firewalls en IPv6

Firewalls en IPv6

Desafíos el filtrado básico de paquetes

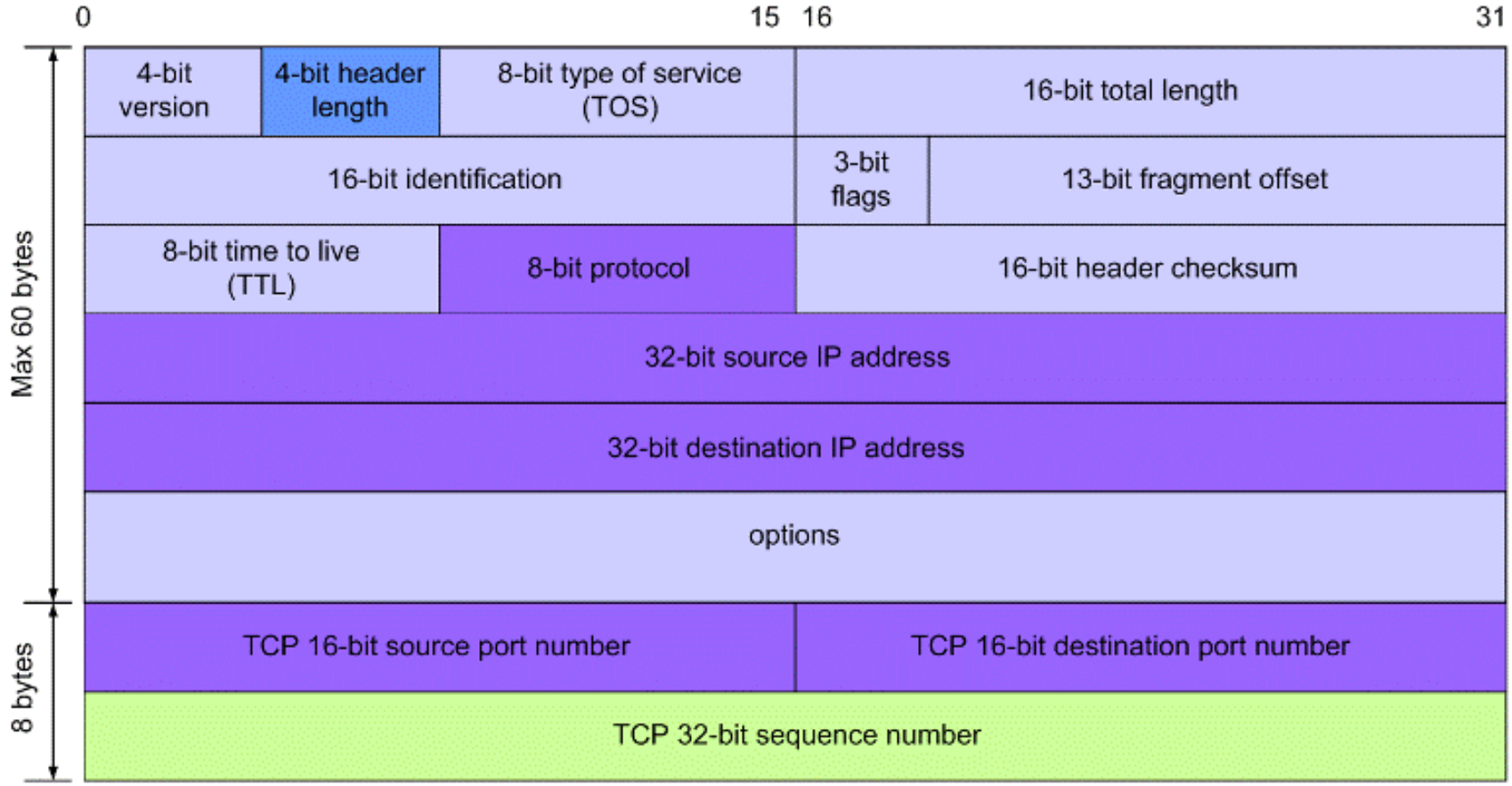
Breve reseña (situación en IPv4)

- IPv4 cuenta con un encabezado de tamaño variable (20-60 bytes), y un MTU mínimo de 68 bytes. Esto hace simple identificar la información de utilidad para el filtrado:



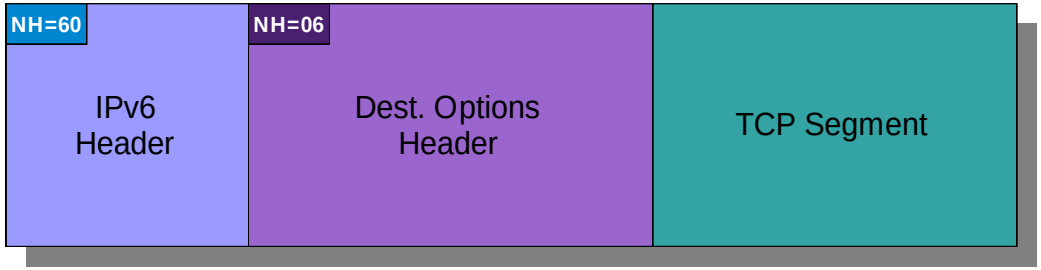
Breve reseña (situación en IPv4)

- IPv4 cuenta con un encabezado de tamaño variable (20-60 bytes), y un MTU mínimo de 68 bytes. Esto hace simple identificar la información de utilidad para el filtrado:



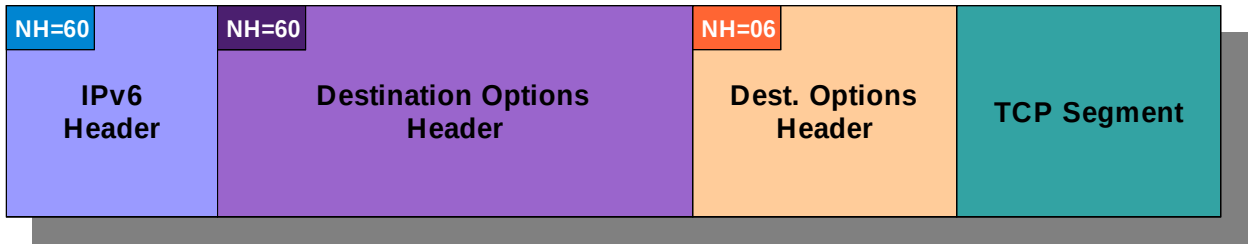
Situación en IPv6

- Se cambió la estructura de encabezamiento variable por una de encabezamiento fijo.
- De necesitarse opciones, las mismas se incluyen en “encabezamientos de extensión” (extension headers), que forman una “cadena de encabezamientos”.
- Por ejemplo,



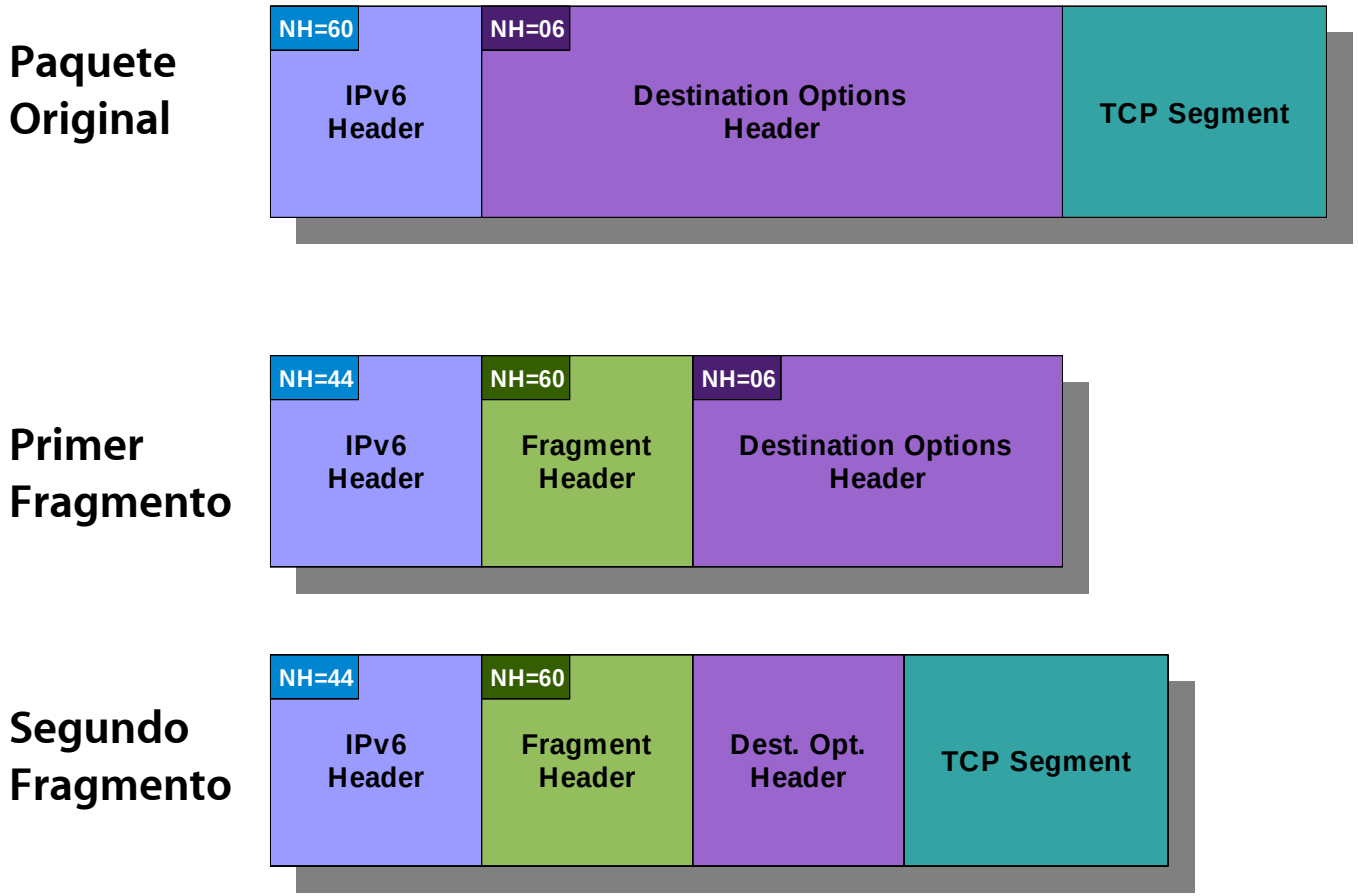
Problemas (I)

- Las especificaciones permiten (y las implementaciones adhieren de manera acorde) el uso de varios encabezados de extensión, permitiendo incluso la repetición de los mismos.
- Asi, la estructura del paquete resultante es compleja, y se dificulta notablemente el proceso de filtrado.
- Ejemplo :



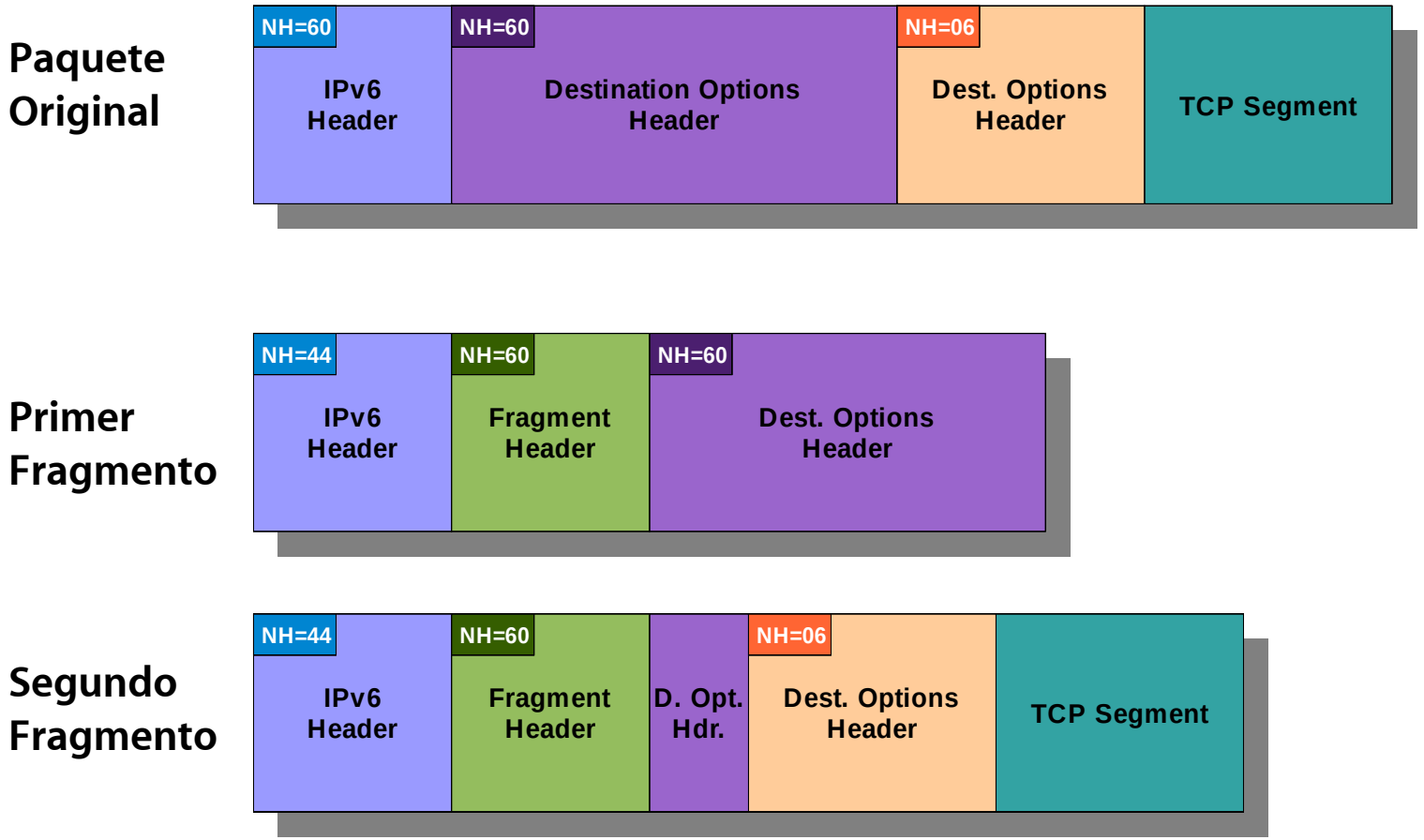
Problemas (II)

- Un encabezamiento de extensión, y fragmentación:



Problemas (III)

- Dos encabezamiento de extensión, y fragmentación:



Posibles contramedidas

- Firewall stateful que reensamble los fragmentos y luego aplique la politica de filtrado
- Filtrado (en firewalls y/o hosts) de paquetes que contengan determinadas combinaciones de encabezados de extensión:
  - Paquetes con numerosos encabezados de extensión
  - Paquetes que usen una combinación fragmentación y encabezados de extensión
- Las posibles contramedidas se dificultan aún mas si el filtrado desea hacerse en capa-2 (a la RA-Guard)

Conclusiones

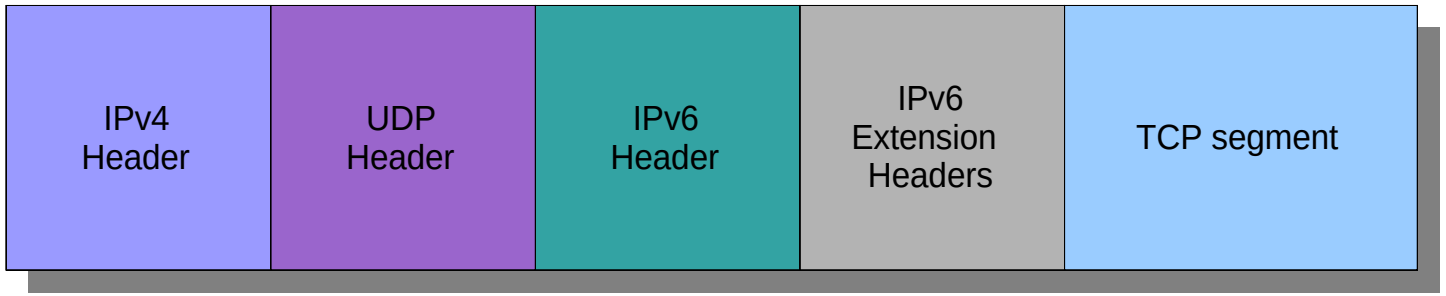
- Los encabezados de extensión son fácilmente explotables para evadir políticas de filtrado
- Es muy probable que se haga común el filtrado (en firewalls) de paquetes que contengan en encabezados de extensión
- El resultado será menor flexibilidad, con el potencial riesgo de inutilizar el uso de los mismos

Firewalls en IPv6

Desafíos en el filtrado de tráfico transición

Breve reseña

- Los paquetes resultantes de la utilización te tecnologías de transición co-existencia pueden tener varias capas de encapsulamiento
- Esto dificulta notablemente la aplicación de políticas de filtrado, a menos que el firewall tenga soporte de dicha tecnología de transición.
- Ejemplo de tráfico Teredo:



- Ejercicio ilustrativo: escribir un filtro para libpcap que “detecte” paquetes TCP/IPv6 transportados sobre Teredo, destinados al host 2001:db8::1, puerto TCP 25.

Trabajo a futuro

Algúnas áreas clave en las que se necesita progreso

- Mejora de implementaciones IPv6
  - Las implementaciones de IPv6 todavía no han estado en el foco de los atacantes. Es muy probable que se descubran muchas vulnerabilidades y bugs en las implementaciones IPv6 actuales.
  - Existen muy pocas herramientas de ataque disponibles públicamente.
- Soporte de IPv6 en dispositivos de seguridad
  - IPv6 no tiene el mismo nivel de soporte que IPv6 en dispositivos tales como firewalls, IDS/IPS, etc.
  - Esto es clave para poder aplicar en IPv6 políticas de seguridad comparables con las aplicadas en IPv4.
- Educación/Entrenamiento
  - Desplegar IPv6 sin un conocimiento aceptable del mismo podría llevar a resultados muy desfavorables.
  - Se necesita entranamiento para ingenieros, técnicos, personal de seguridad, etc., previo al diseño y puesta en funcionamiento de una red IPv6.

20 million engineers need IPv6 training, says IPv6 Forum
The IPv6 Forum - a global consortium of vendors, ISPs and national research & Education networks - has launched an IPv6 education certification programme in a bid to address what it says is an IPv6 training infrastructure that is "way too embryonic to have any critical impact.“ (**http://www.itwire.com**)

Algunas conclusiones

Algunas conclusiones

- Pese a que IPv6 provee una funcionalidad similar a la de IPv4, muchos de los mecanismos utilizados son diferentes. Por tal motivo, requiere de un análisis cuidadoso.
- Las implicancias de seguridad de IPv6 deben ser consideradas previo a su despliegue, para evitar un impacto negativo en las redes correspodientes
- Dado que la mayoría de los sistemas de uso general cuenta con soporte IPv6, incluso los administradores de redes IPv4 deberían conocer las implicancias de seguridad de IPv6
- Incluso si todavía no lo ha planificado, es probable que necesite desplegar IPv6 en el corto plazo.
- Es hora de capacitarse, entrenarse, y experimentar con IPv6!

Preguntas?

Gracias!

Fernando Gont

fernando@gont.com.ar

http://www.gont.com.ar