

Resultados de un análisis de seguridad de IPv6

Fernando Gont



CIICT 2011

Tunja, Colombia. Octubre 25-28, 2011

Breve reseña de IPv6

- Las direcciones IPv4 están próximas a agotarse, limitando el crecimiento de Internet
- IPv6 se desarrolló para solucionar el problema de escasez de direcciones IPv4
- Todavía no ha sido amplia/globalmente desplegado/utilizado (se estima que el tráfico IPv6 es menos del 1% del tráfico total)
- Sin embargo, la mayoría de los SO de propósito general poseen soporte IPv6 – al menos parte de tu red ya utiliza IPv6!
- Asimismo, los ISP y otras organizaciones están pensando en IPv6 mas seriamente, en parte debido a:
 - Agotamiento del pool central de direcciones IPv4 de IANA
 - El inminente agotamiento de direcciones IPv4 en los RIR
 - Actividades de concientización como el “World IPv6 Day”
- Pareciera que finalmente IPv6 empieza a despegar...

Motivación de esta presentación

- Se han creado muchos mitos sobre “seguridad IPv6”:
 - La seguridad fue considerada durante el desarrollo del mismo
 - El paradigma de seguridad cambiará de network-centric a host-centric
 - Se incrementará el uso de IPsec
 - etc.
- Estos mitos han llevado a concepciones erróneas sobre IPv6, con un consecuente impacto negativo en la seguridad de las redes emergentes (o ya existentes)
- Esta presentación intentará separar “mito” de “realidad”, y ofrecer una visión realista sobre el tema
- Más que discutir vulnerabilidades específicas, esta presentación intentará influenciar la manera en la cual piensas sobre “Seguridad IPv6”



Agenda

- Consideraciones generales sobre seguridad IPv6
- 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

(qué cambia, y qué no)


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 (opcional) (+ MLD)
Aislamiento de fallas	ICMP	ICMPv6
Soporte de IPsec	Opcional	Recomendado (<u>no</u> mandatorio)
Fragmentación	Tanto en hosts como routers	Sólo en hosts



Implicancias de Seguridad de IPv6



Direccionamiento

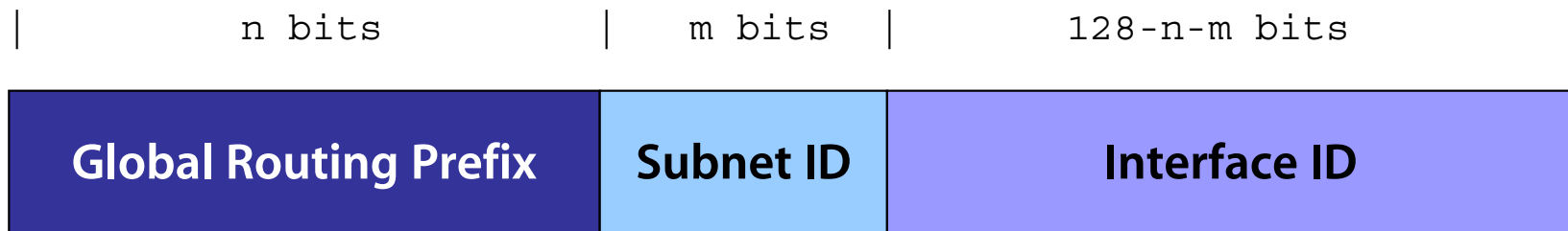
Implicancias en “host scanning”

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

Breve reseña (II)

- 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., PREFIJO::1)
 - De acuerdo a lo especificado por una tecnología de transición/co-existencia

Consideraciones de seguridad

Mito: "Es imposible realizar un ataque de 'host scanning' en IPv6, ya que el espacio de direcciones es muy grande. Hacerlo llevaría una eternidad!"

- Esta aseveración asume que las direcciones se asignan aleatoriamente.
- [Malone, 2008] (*) investigó los patrones de asignación de direcciones:
 - Para hosts: 50% autoconf, 20% IPv4-based, 10% Teredo, 8% "low-byte"
 - Para routers: 70% "low-byte", 5% IPv4-based
- Conclusiones:
 - Las direcciones IPv6 no se asignan de manera aleatoria
 - El mayor espacio de direcciones no necesariamente significa mayor resistencia a escaneo de direcciones
 - Es esperable que estos ataques utilicen mayor "inteligencia" en el caso de IPv6.

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



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

Breve reseña

- Uno de los principios fundamentales de la Arquitectura de Internet es el llamado “principio de extremo a extremo” (end to end):
 - Red “tonta”, hosts inteligentes -- la red se limita a reenviar paquetes
 - Cualquier sistema de la red es capaz de establecer una comunicación con cualquier otro sistema de la red
 - Usualmente se argumenta que esto permite la “innovación” en la red
- Este principio fue “abandonado” principalmente debido al despliegue de tecnologías como NAT.
- Usualmente se asume que IPv6 brindará a cada dispositivo una dirección IPv6 global única, eliminando la necesidad de dispositivos como NAT.

Consideraciones varias

Mito: *“IPv6 devolverá a Internet la conectividad extremo a extremo”*

- Es usual asumir que el mayor espacio de direcciones “devolverá” a la Internet el principio conocido como “end-to-end”.
- Sin embargo,
 - La disponibilidad de direcciones no garantiza la posibilidad de comunicación “extremo a extremo”
 - La mayoría de las redes de hoy en día no tienen como fin la innovación
 - Los servicios esperados por los usuarios son aquellos mismos que hoy se brindan en IPv4 sin conectividad “end-to-end” (web, email, etc.)
 - La conectividad “extremo a extremo” no es necesariamente una propiedad “deseable” en una red de producción
- En conclusión,
 - IPv6 no nos devolverá el principio de “extremo a extremo”
 - La subred IPv6 típica (como ser una red hogareña) esté protegida por un firewall stateful que solo permita el tráfico “originado en el interior de la red”



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 utiliza mensajes ICMPv6
- Los mensajes ICMPv6 Neighbor Solicitation y Neighbor Advertisement cumplen una función análoga a la de ARP request y ARP reply en IPv4

Consideraciones de seguridad

- Como es de esperarse, en IPv6 se pueden realizar ataques análogos a los ataques “ARP spoofing” de IPv4
- 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 (en realidad, tal vez algo mas complicada)



Autoconfiguración

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 opcional
- Mediante el envío de mensajes “Router Advertisement”, los routers comunican información de configuración a los “hosts” del segmento de red en cuestión
 - Prefijos a utilizar
 - Rutas
 - Valores para distintos parámetros (Hop Limit, MTU, etc.)
 - Tiempos recomendados para la utilización de las direcciones generadas
 - etc.

Consideraciones de Seguridad

- Básicamente, mediante la falsificación de dichos mensajes el atacante puede realizar:
 - Ataques de denegación de servicio (DoS)
 - Ataques de tipo “Man in the Middle” (MITM)
- Algunas técnicas de “mitigación” disponibles 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...

Mito: *"IPv6 es mas seguro que IPv4 porque tiene soporte mandatorio de IPsec"*

- Actualmente, 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 mandatorio 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

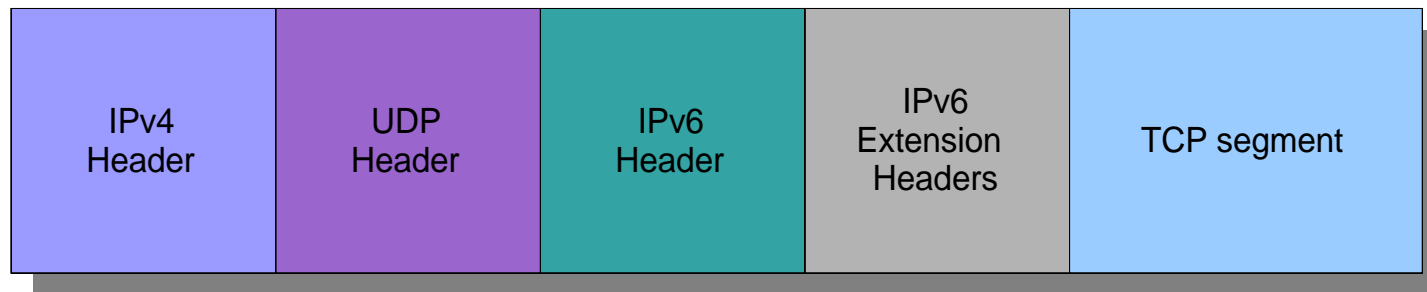
- El plan original de transición a IPv6 era el uso de dual-stack (*este plan falló*)
- La estrategia actual es un plan de transición/co-existencia basado en un grupo de herramientas:
 - Dual Stack
 - Túneles “configurados”
 - Túneles automáticos (ISATAP, 6to4, Teredo, etc.)
 - Traducción (por ej., NAT64)
- Algunas variantes de túneles automáticos (como Teredo e ISATAP) están habilitados por defecto en Windows Vista y Windows 7

Consideraciones 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.
- Algunos de estos mecanismos merecen consideraciones de privacidad:
 - ¿Por dónde circula su tráfico Teredo y 6to4?
 - Esto puede (o no) ser importante para su red

Consideraciones de seguridad (II)

- Los paquetes resultantes de la utilización de 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:



- Es sabido que algunas de estas tecnologías han sido utilizadas por atacantes para violar políticas de seguridad



Implicancias de seguridad de IPv6 en redes IPv4

Breve reseña

- La mayoría de los sistemas de uso general tienen algún tipo de soporte IPv6 habilitado “por defecto”
 - Soporte IPv6 nativo
 - Mecanismos de transición/co-existencia
- Incluso si una red supone ser IPv4-only, este soporte existe, y está a la espera de ser utilizado.

Consideraciones de seguridad

- Un atacante podría habilitar la conectividad IPv6 nativa, falsificando RAs
- Esto podría permitir que se evadan controles de filtrado de tráfico y/o NIDS
- El uso de tecnologías como Teredo podría resultar en que incluso hosts que están detrás de NATs quedaran expuestos a la red pública (Internet)
- Por tales motivos,
 - Incluso si una red no espera utilizar IPv6, debe tener en cuenta las implicancias de seguridad del mismo
 - Si se espera que en una red IPv4 no se utilicen mecanismos de transición/coexistencia, se deberían aplicar las políticas de filtrado correspondientes



Trabajo a futuro

Algunas 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.
 - Existen muy pocas herramientas de ataque disponibles públicamente
- Soporte de IPv6 en dispositivos de seguridad
 - IPv6 no tiene el mismo nivel de soporte que IPv4 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 entrenamiento 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

- IPv6 provee una funcionalidad similar a la de IPv4, pero muchos de los mecanismos utilizados son diferentes. Por tal motivo, se 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 correspondientes
- 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?



Agradecimientos

- Organizadores del CIICT 2011, quienes hicieron posible esta presentación
- A Uds., los asistentes a esta presentación

Gracias!

Fernando Gont

fgont@si6networks.com



www.si6networks.com