IPv6: Motivación y Desafíos

Fernando Gont

Campus Party 2012
Quito, Ecuador. Septiembre 19-23, 2012

Acerca de...

- He trabajado en análisis de seguridad de protocolos de comunicaciones para:
  - UK NISCC (National Infrastructure Security Co-ordination Centre)
  - UK CPNI (Centre for the Protection of National Infrastructure)
- Actualmente trabajando para SI6 Networks
- Participante activo de la Internet Engineering Task Force (IETF)
- Más información en: http://www.gont.com.ar

Agenda

- Breve reseña del mundo IPv4
- Agotamiento de direcciones IPv4
- Diseño del nuevo protocolo de Internet: IPv6
- Mecanismos de transición y co-existencia
- Desafíos en el despliegue de IPv6
- Próximos pasos
- Conclusiones
- Preguntas y respuestas

Breve historia del mundo IPv4

Breve historia de IPv4

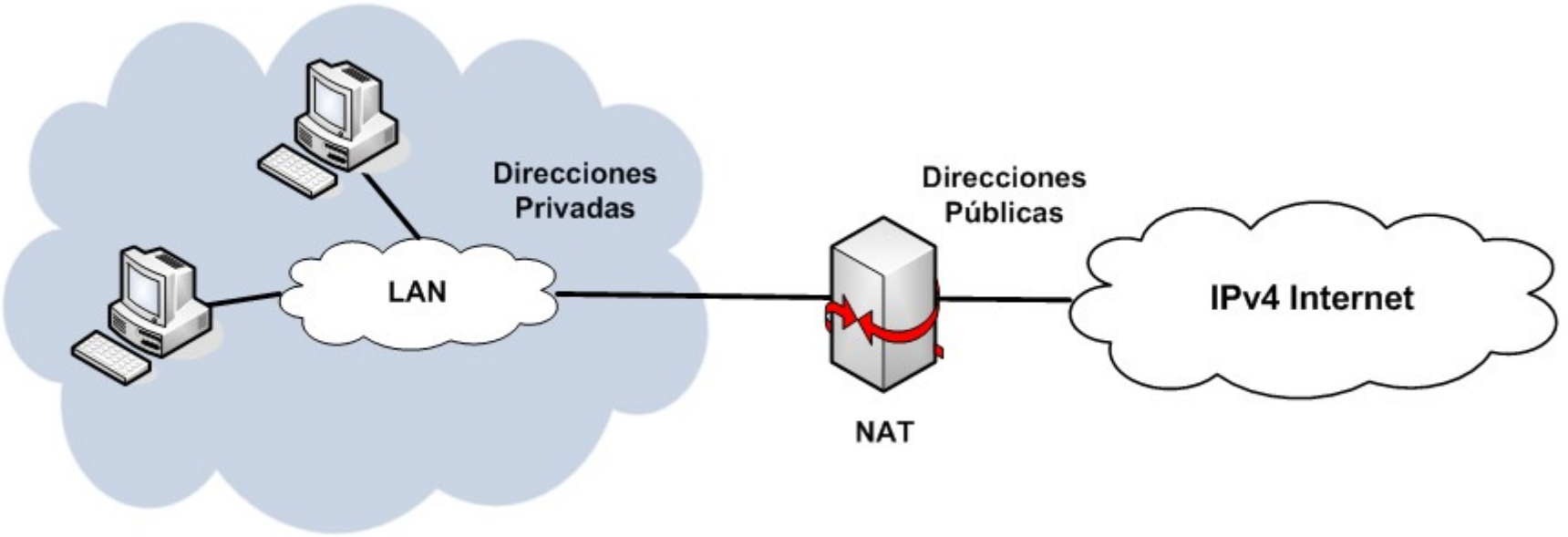
- Apareció a principios de los '80
- Brinda un servicio de transmisión de paquetes “no confiable”
- Provee en “bloque fundamental” para crear servicios más complejos.
- Originalmente respetaba estos principios:
  - Red tonta, hosts inteligentes
  - Direccionamiento extremo a extremo
  - Conectividad extremo a extremo

“Evolución” de la Internet IPv4

- La red dejó de ser tonta
  - Distintos dispositivos inspeccionan el contenido de paqutes
  - Algunos de ellos: NIDS, firewalls, proxies transparentes, etc.
- Se perdió la conectividad extremo a extremo:
  - No necesariamente dos sistemas pueden comunicarse entre si
  - “Culpables”: firewalls, NAT's, IPS's, etc.
- Se están agotando las direcciones IPv4
  - Las direcciones IPv4 de 32 bit resultaron escasas para permitir el crecimiento de Internet
  - Se introduce el NAT (Network Address Translator) como “stop-gap”
  - Se propone el diseño de un nuevo protocolo como solución a mediano/largo plazo

NAT (Network Address Translation)

- NAT permite reducir el “consumo” de direcciones IPv4
- Varios sistemas comparten una misma dirección para conectarse a la red pública.



NAT (Network Address Translation) (II)

- NAT requiere la “inspección” y modificación de paquetes
  - Dificulta el despliegue de nuevos protocolos
  - Introduce “puntos únicos de fallo”
- Sin embargo, se le han encontrado algunas propiedades “deseables”:
  - Oculta la topología de la red interna
  - Oculta la identidad de los hosts internos
  - Funciona como un simple firewall que “solo permite conexiones salientes”
- “Alarga” la vida de IPv4, pero **no indefinidamente**

El “futuro” de IPv4

- La única forma de extender la vida de IPv4, de manera **limitada**, es con múltiples capas de NAT
- Esto resultaría en un incremento de la fragilidad de la red
- Significaría el despliegue de una **capa de NAT controlada por el proveedor de servicio** (y no por el usuario)
- Esto limitaría la usabilidad de la red
- **Necesitamos de un nuevo protocolo de Internet**

Internet Protocol version 6 (IPv6)
Motivación

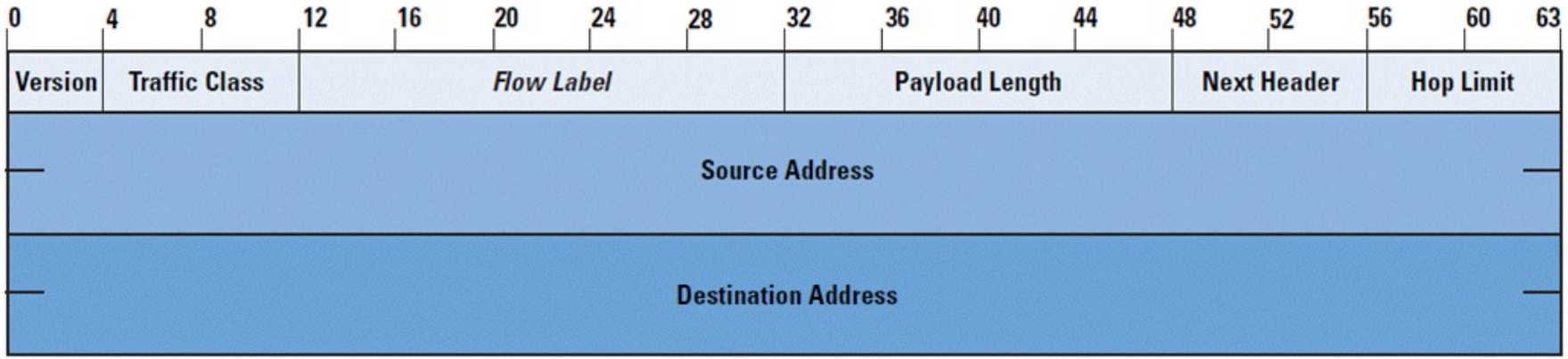
Objetivos de diseño de IPv6

- Proveer suficientes direcciones como para permitir el crecimiento de Internet
- Eliminar algunos mecanismos que tenían impacto de performance negativo en routers:
  - Chequeo del checksum en routers
  - Fragmentación en routers
- Proveer el mismo tipo de servicio que su antecesor IPv4

Encabezado IPv6

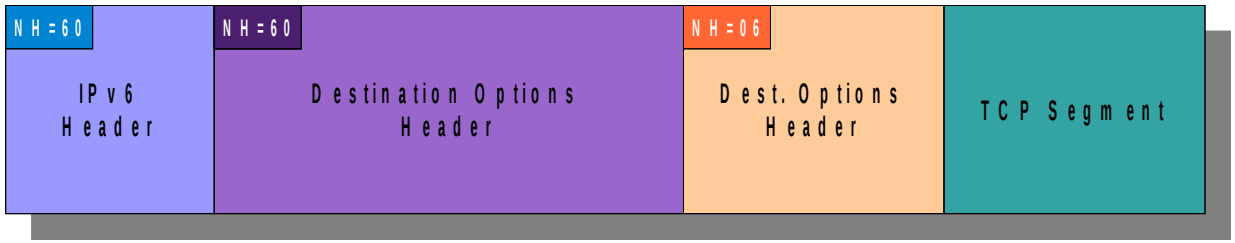
Formato del encabezado IPv6

- Todos los campos “no elementales” fueron removidos del encabezado mandatorio



Encabezados de extensión

- Todas las opciones se incluyen en “encabezados de extensión”
- Los mismos se colocan entre el encabezado IPv6, y el protocolo de capa superior



Breve comparación entre IPv6/IPv4

Breve comparación entre IPv6/IPv4

- Muy similares en *funcionalidad*, pero no así en *mecanismos*

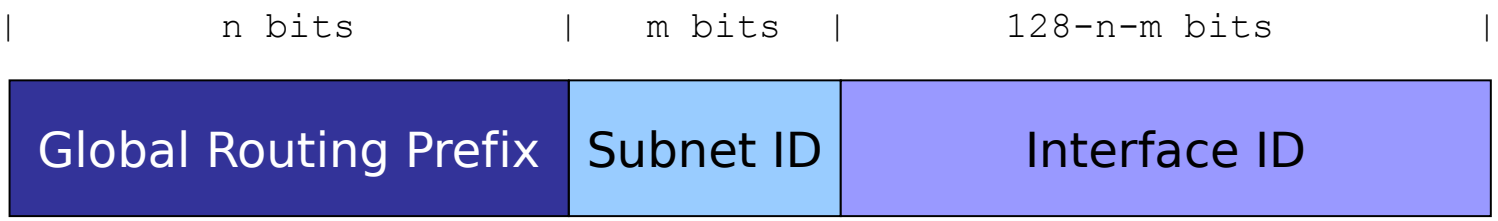
	IPv4	IPv6
Direccionamiento	**32 bits**	**128 bits**
Resolución de direcciones	**ARP**	**ICMPv6 NS/NA (+ MLD)**
Auto-configuración	**DHCP & ICMP RS/RA**	**ICMPv6 RS/RA & DHCPv6 (optional) (+ MLD)**
Aislamiento de fallos	**ICMPv4**	**ICMPv6**
Soporte de IPsec	**Opcional**	**Opcional**
Fragmentación	**Tanto en hosts como en routers**	**Sólo en hosts**

Direccionamiento IPv6
Breve Introducción

Breve reseña de direccionamiento IPv6

- El mayor espacio de direcciones es el “motivador” de IPv6
- Se utilizan direcciones de 128 bits
- Semántica muy similar a IPv4:
  - Se agregan direcciones en “prefijos” para el ruteo
  - Existen distintos tipos de direcciones
  - Existen distintos alcances para las direcciones
- Cada interfaz utiliza multiples direcciones, de multiples tipos y alcances:
  - Una dirección link-local unicast
  - Una o mas direcciones global unicast
  - etc.

Formato de Direcciones Globales IPv6



- Diferentes políticas de selección de IID:
  - Embeber la MAC address (SLAAC tradicional)
  - Embeber la dirección IPv4 (por ej., 2001:db8::192.168.1.1)
  - Low-byte (por ej., 2001:db8::1, 2001:db8::2, etc.)
  - Wordy (por ej., 2001:db8::dead:beef)
  - Indicado por una tecnología de transición

Resolución de direcciones

Breve reseña

- Resolución de direcciones: IPv6 → capa de enlace
- Realizada en IPv6 por “Neighbor Discovery”:
  - Basado en mesajes ICMPv6 (Neighbor Solicitation y Neighbor Advertisement)
  - Análogo a ARP Request y ARP Reply
  - Implementado sobre IPv6, y **no** sobre la capa de enlace
- Básicamente,
  - Un host envía un **Neighbor Solicitation** a una dirección multicast (“Quien tiene la dirección 2001::db8::1?”)
  - El host en cuestión responde reponde con un **Neighbor Advertisement** (“2001::db8::1 tiene la MAC address 00:11:22:33:44:55”).

Auto-configuración

Breve reseña

- Dos mecanismos de autoconfiguración en IPv6:
  - Stateless Address Auto-Configuration (SLAAC)
    - Basado en ICMPv6
  - DHCPv6
    - Basado en UDP
- SLAAC es mandatorio, mientras que DHCPv6 es opcional
- Funcionamiento básico de SLAAC:
  - Los hosts solicitan información mediante ICMPv6 **Router Solicitations**
  - Los routers responden con **Router Advertisements**:
    - Prefijos a utilizar
    - Rutas a utilizar
    - Parametros de red
    - etc.

Conectividad Extremo a Extremo

Breve reseña

- La red Internet se basó en el principio de “extremo a extremo”
  - Red tonta, extremos (hosts) inteligentes
  - La comuncación es posible entre cualquier par de nodos
  - La red no examina el contenido de los paquetes IP
- Se suele argumentar que este principio permite la innovación
- Los NATs lo han eliminado de Internet
- Se espera que con IPv6 no existan NATs, y se retorne al principio “extremo a extremo”

IPv6 y el principio “extremo a extremo”

Mito: “*IPv6 devolverá a Internet el principio 'extremo a extremo*'”

- Se asume que el gran espacio de direcciones devolverá este principio
- Sin embargo,
  - Las direcciones globales no garantizan conectividad extremo a extremo
  - La mayoría de las redes no tiene interés en “innovar”
  - Los usuarios esperan en IPv6 los mismos servicios que en IPv4
  - Este principio aumenta la exposición de los sistemas
- En resumen,
  - La conectividad extremo a extremo no necesariamiente es deseable
  - La subred típica IPv6 solo permitirá “trafico saliente” (mediante firewalls)

Soporte de IPsec

Breve reseña y consideraciones

- En su origen, IPsec fue mandatorio para IPv6, y opcionla para IPv4
- En la práctica, esto fue/es irrelevante:
  - Es mandatorio el soporte, pero no así su uso
  - Las implementaciones no respetan el estándar
  - Existen en IPv6 los mismos obstaculos para IPsec que en IPv4
- Incluso la IETF reconoció esta situación
  - Actualmente, IPsec es **opcional** para ambos protocolos
- Conclusión:
  - El despliegue de IPv6 no implica un mayor uso de IPsec

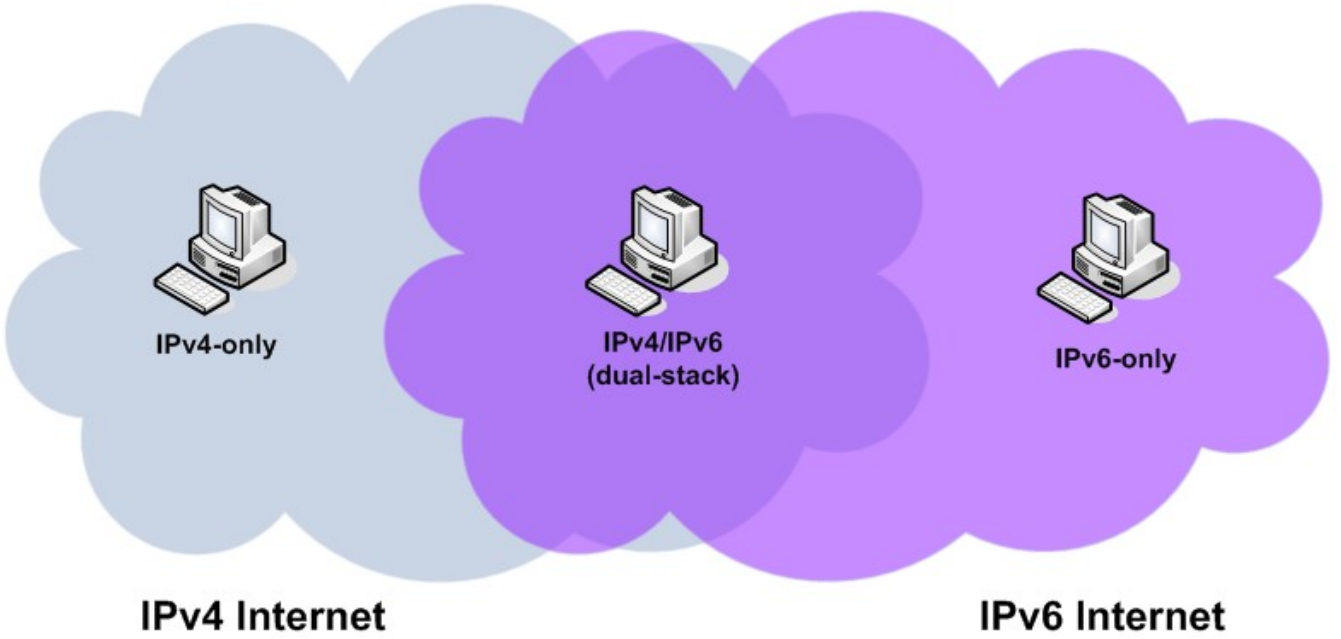
Mecanismos de transición y co-existencia

Breve reseña

- IPv6 **no** es compatible hacia atrás
- Plan original de transición: doble pila (dual stack)
  - Desplegar IPv6 en paralelo con IPv4 **antes** de **necesitar** IPv6
- La estrategia actual es transición/co-existencia basada en:
  - Doble pila
  - Túneles
    - Automáticos
    - Configurados
  - Traducción
    - CGN
    - NAT64
- La mayoria de los sistemas soportan algunos de estos mecanismos

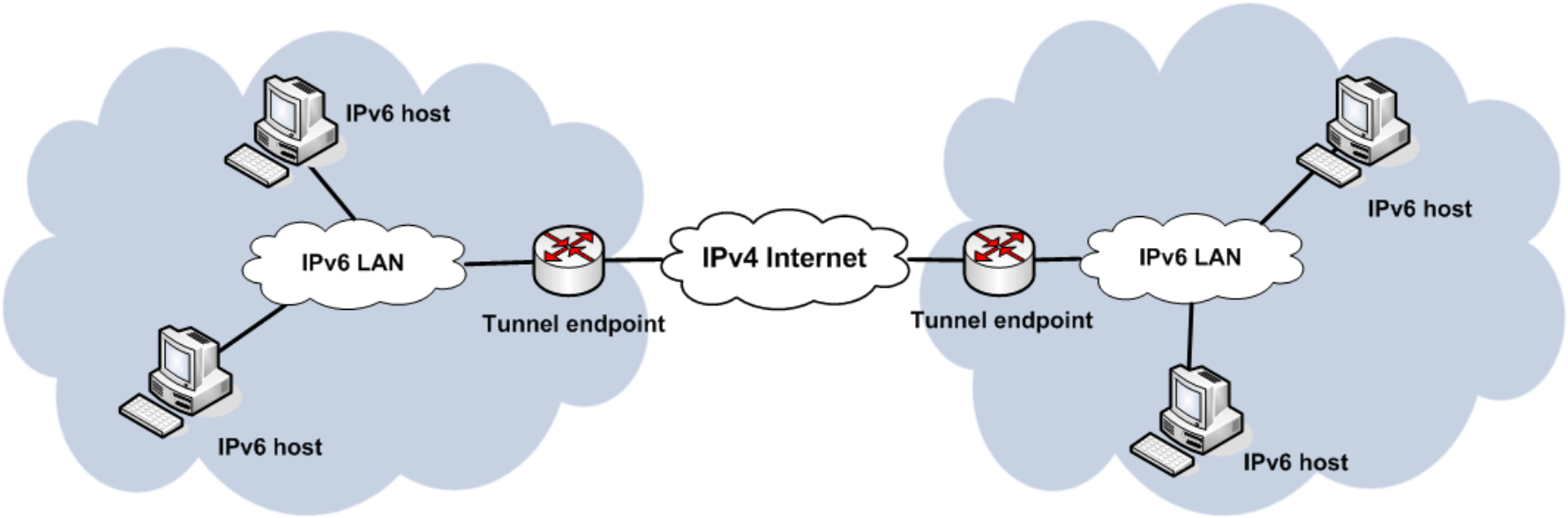
Dual-stack

- Consiste en que cada sistema soporte ambos protocolos
- Se usa el protocolo indicado de acuerdo a que protocolo(s) soportan los sistemas que desean comunicarse



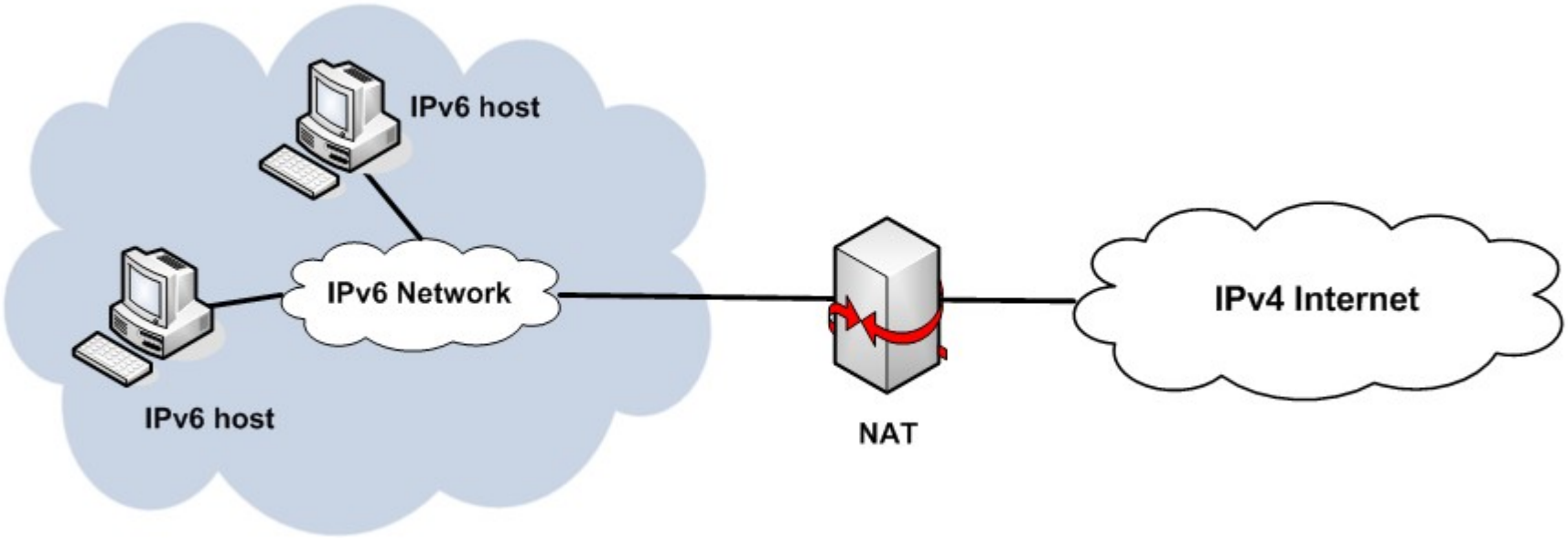
Túneles

- Permiten interconectar “islas” de un protocolo a través de otro



Network Address Translation (NAT)

- Permiten:
  - Interconectar hosts IPv4-only con hosts IPv6-only (por ej., NAT64)
  - Compartir direcciones entre varios sistemas (por ej., el NAT tradicional de IPv4)



Terminando el “rompecabezas”

- Para un determinado nombre, el DNS puede contener
  - Registros A (direcciones IPv4)
  - Registros AAAA (direcciones IPv6)
- El sistema pedirá registros A y/o AAAA de según una variedad de criterios
- De acuerdo a los registros disponibles, y protocolos soportados, podrá utilizarse IPv4 y/o IPv6
- La decisión no siempre es simple:
  - Puede haber varias direcciones, de varios protocolos distintos
  - Elegir la dirección e destino inadecuada puede ocasionar problemas

Desafíos para el despliegue de IPv6

Dónde estamos con IPv6?

- Todavía no ha sido amplia/globalmente desplegado
- Soportado por la mayoría de sistemas de propósito general
- Los ISPs y otras organizaciones lo han empezado a tomar más en serio a partir de:
  - Agotamiento del pool central de direcciones IPv4 de IANA
  - Actividades de concientización como el “World IPv6 Day” y el “World IPv6 Launch Day”
  - Inminente agotamiento del pool de direcciones de los RIR
- Parece que IPv6 finalmente va a despegar

Desafíos técnicos

- Se cuenta con mucha menos experiencia que con IPv4
- Se cuenta con pocos recursos humanos bien capacitados
- Las implementaciones de IPv6 son menos maduras que las de IPv4
- Exite menor soporte para IPv6 en equipamiento de red y seguridad que para IPv4
- La coomplejidad de la red Internet será mayor
  - Contaremos on dos protocolos de Internet (IPv4 e IPv6)
  - Se incrementará el uso de túneles, NATs, etc.

Desafíos económicos

- La utilidad de IPv6 aumenta al aumentar la cantidad de sistemas que lo iplementan
- Quién se sube primero al tren?
  - Proveedores de contenido: “Para qué desplegar IPv6 si no hay usuarios que lo utilicen?”
  - Roveedores de servicio: “Para que proveer IPv6 a los usuarios si no existe contenido sobre IPv6?”
- Este circulo vicioso fue parcialmente abordado por:
  - World IPv6 Day y World IPv6 Launch Day
- El Retorno de Inversión es, básicamente, “continuidad de negocio”
  - Se volverá evidente solo cuando “sea demasiado tarde”

Próximos pasos

Actividades propuestas

- Generar un plan de despliegue de IPv6
- Relevar equipos y aplicaciones
- Considerar el soporte de IPv6 en los procesos de adquisición de equipos y aplicaciones
- Capacitar a todo el personal técnico sobre IPv6
- Realizar pruebas piloto, previo al despliegue en producción
- Analizar las implicancias de seguridad de IPv6

Algunas conclusiones

Algunas conclusiones

- Nos estamos quedando sin direcciones IPv4
- La red internet precisa del trabajo conjunto de todos los actores involucrados
- De nosotros depende la Internet con que contaremos en el futuro

Preguntas?

Gracias!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

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

www.si6networks.com