Estandarización IPv6

RFC8200 (STD86)

Webinar LACNIC

Abril 2018

Jordi Palet (jordi.palet@theipv6company.com)

Agenda

1. Introducción a IPv6
2. Terminología
3. Formato de Cabecera
4. Cabeceras de Extensión
5. Tamaño de Paquetes
6. Etiquetas de Flujo
7. Clases de Tráfico
8. Protocolos de Capas Superiores
9. Otros Aspectos

¿Porque un STD?

- La gran mayoría de los protocolos en uso NO son STD
- El proceso se inicia con un ID, que puede pasar a ser un RFC de diversos tipos, uno de ellos “Standards Track”
- El RFC2026 definía 3 niveles de madurez “Standards Track”, que con el RFC6410, se reducen a 2
  - “Proposed Standard” e “Internet Standard”
- El paso de uno a otro es un esfuerzo administrativo:
  - Al menos 2 implementaciones independientes interoperables con exitosas experiencias de despliegue y operación
  - Sin erratas que puedan producir fallos de interoperabilidad entre nuevas y viejas implementaciones
  - Sin características no utilizadas que incrementen de forma muy significativa la complejidad de la implementación
  - Si hubiera patentes, demostración de al menos dos implementaciones independientes con uso exitoso del proceso de licencia

1. Introducción a IPv6

¿Porque un Nuevo Protocolo de Internet?

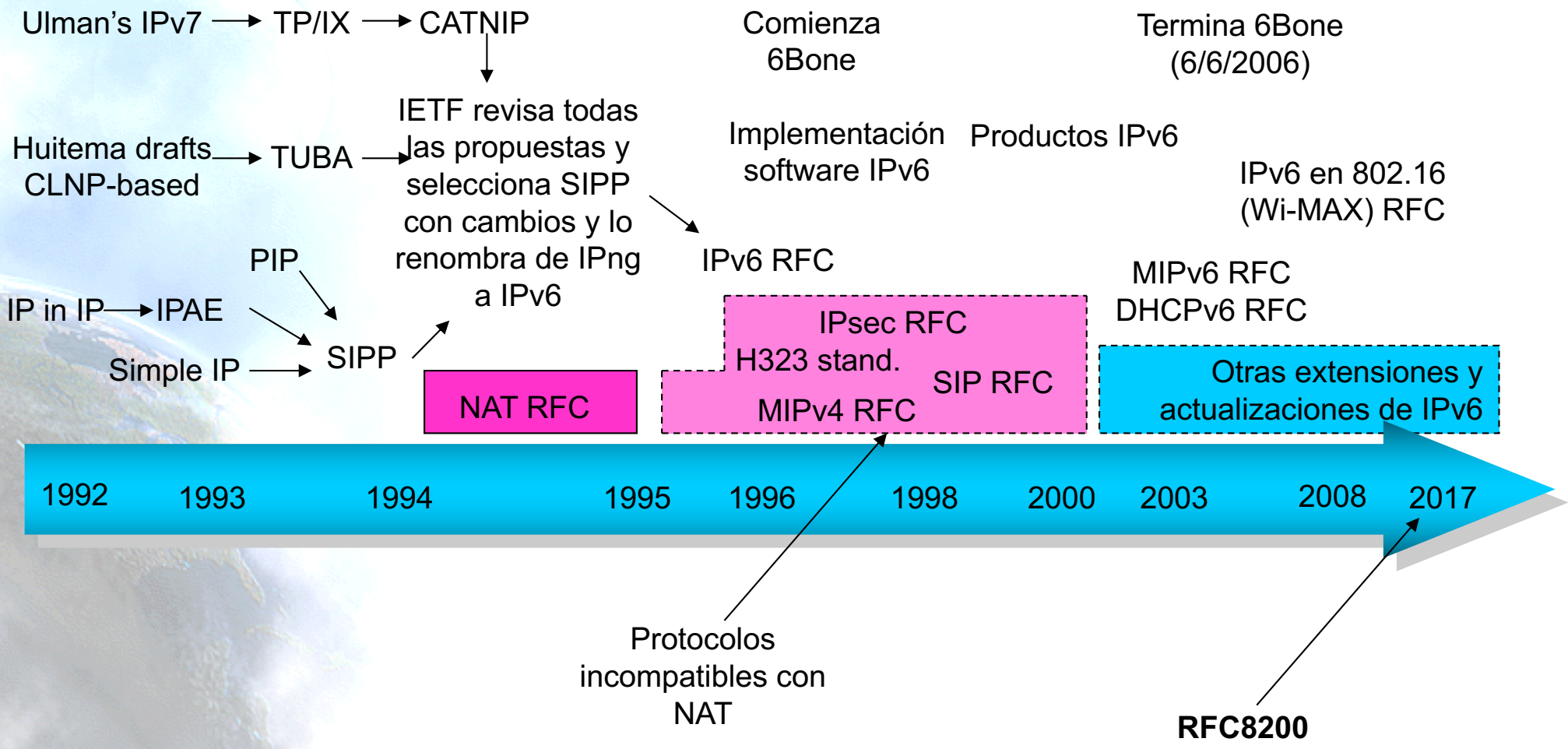
Un único motivo lo impulsó: Más direcciones!

- Para miles de millones de nuevos dispositivos, como teléfonos celulares, PDAs, dispositivos de consumo, coches, etc.
- Para miles de millones de nuevos usuarios, como China, India, etc.
- Para tecnologías de acceso “always-on”, como xDSL, cable, PLC, fibra, ethernet, etc.

Hechos Históricos

- **1983** : Red investigación con ~100 computadoras
- **1991 Nov.**: IETF crea un working group para evaluar y buscar soluciones al agotamiento de direcciones
- **1992**: Actividad Comercial, crecimiento exponencial
- **1992 Julio** : IETF determina que era esencial comenzar a crear el next-generation Internet Protocol (IPng)
- **1993** : Agotamiento de direcciones clase B. Previsión de colapso de la red para 1994!
- **1993 Sept.**: RFC 1519, “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy”
- **1994 Mayo**: RFC 1631, “The IP Network Address Translator (NAT)”
- **1995 Dic.**: Primer RFC de IPv6: “Internet Protocol, Version 6 (IPv6) Specification”, RFC 1883
- **1996 Feb.**: RFC 1918, “Address Allocation for Private Internets”
- **1998 Dic.**: RFC 2460 Obsoleted RFC1883. Especificación IPv6.
- **2017 Julio.:** STD86. RFC8200. Estándar actual.

Evolución de IPng



Ventajas Adicionales con Direcciones Mayores

- Facilidad para la auto-configuración
- Facilidad para la gestión/delegación de las direcciones
- Espacio para más niveles de jerarquía y para la agregación de rutas
- Habilidad para las comunicaciones extremo-a-extremo con IPsec (porque no necesitamos NATs)

Ventajas Adicionales con el Nuevo Despliegue

- Oportunidad para eliminar parte de la complejidad, ejemplo en la cabecera IP
- Oportunidad para actualizar la funcionalidad, ejemplos como multicast, QoS, movilidad

IPv6 (RFC8200)

- Especificación básica del Protocolo de Internet versión 6
- Cambios de IPv4 a IPv6:
  - Capacidades expandidas de direccionamiento
  - Simplificación del formato de la cabecera
  - Soporte mejorado de extensiones y opciones
  - Capacidad de etiquetado de flujos
  - Capacidades de autenticación y encriptación
- Documentos adicionales:
  - RFC4291 (IPv6 Addressing Architecture)
  - RFC4443/STD89 (ICMPv6)

Resumen de las Principales Ventajas de IPv6

- Capacidades expandidas de direccionamiento
- Autoconfiguración y reconfiguración “sin servidor” (“plug-n-play”)
- Mecanismos de movilidad más eficientes y robustos
- Incorporación de encriptación y autenticación en la capa IP
- Formato de la cabecera simplificado e identificación de flujos
- Soporte mejorado de opciones/extensiones

¿Porqué 128 Bits para el Tamaño de las Direcciones?

- Había quienes deseaban direcciones de 64-bits, de longitud fija
  - – suficientes para 10^{12} sitios, 10^{15} nodos, con una eficacia del .0001 (3 órdenes de magnitud más que los requisitos de IPng)
  - – minimiza el crecimiento del tamaño de la cabecera por cada paquete
  - – eficaz para el procesado por software
- Había quienes deseaban hasta 160 bits y longitud variable
  - – compatible con los planes de direccionamiento OSI NSAP
  - – suficientemente grandes para la autoconfiguración utilizando direcciones IEEE 802
  - – se podía empezar con direcciones mas pequeñas que 64 bits y crecer posteriormente
- La decisión final fue un tamaño de 128-bits y longitud fija
  - – ¡nada menos que **340,282,366,920,938,463,463,374,607,431,768,211,456!**

¿Que pasó con IPv5?

0–3		no asignados
4	IPv4	(versión más extendida hoy de IP)
5	ST	(Stream Protocol, no un nuevo IP)
6	IPv6	(inicialmente denominados SIP, SIPP)
7	CATNIP	(inicialmente IPv7, TP/IX; caducados)
8	PIP	(caducado)
9	TUBA	(caducado)
10-15		no asignados

2. Terminología

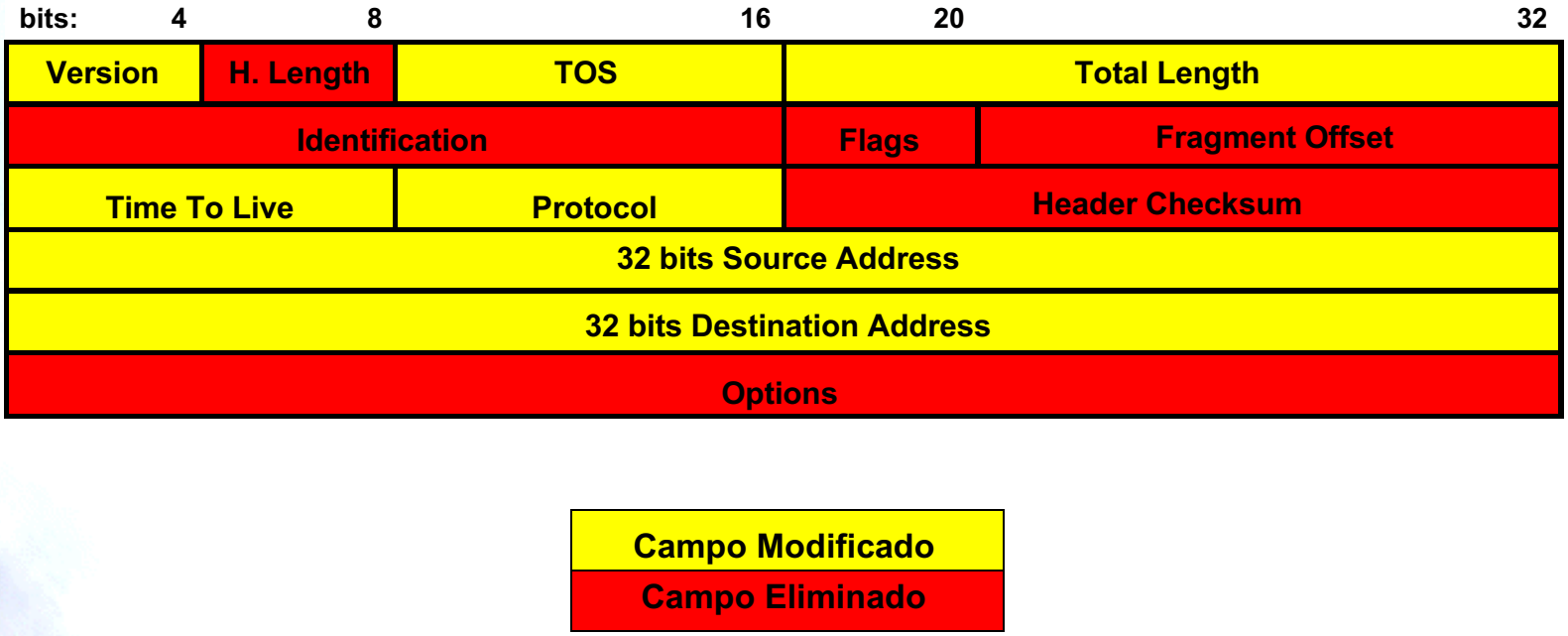
Terminología

- **Node:** Dispositivo que implementa IPv6
- **Router:** Nodo que reenvía paquetes IPv6
- **Host:** Cualquier otro nodo que no es un router
- **Upper Layer:** Protocolo que está inmediatamente por encima de IPv6
- **Link:** Medio o entidad de comunicación sobre la que los nodos pueden comunicarse a través de la capa de link
- **Neighbors:** Nodos conectados al mismo link
- **Interface:** Conexión del nodo al enlace (link)
- **Address:** Identificación IPv6 de un interfaz o conjunto de interfaces de un nodo
- **Packet:** Una cabecera IPv6 junto a los datos que incorpora
- **Link MTU:** Unidad de Transmisión Máxima
- **Path MTU:** MTU mínima en el camino que recorren los paquetes IPv6 entre dos nodos finales

3. Formato de cabecera

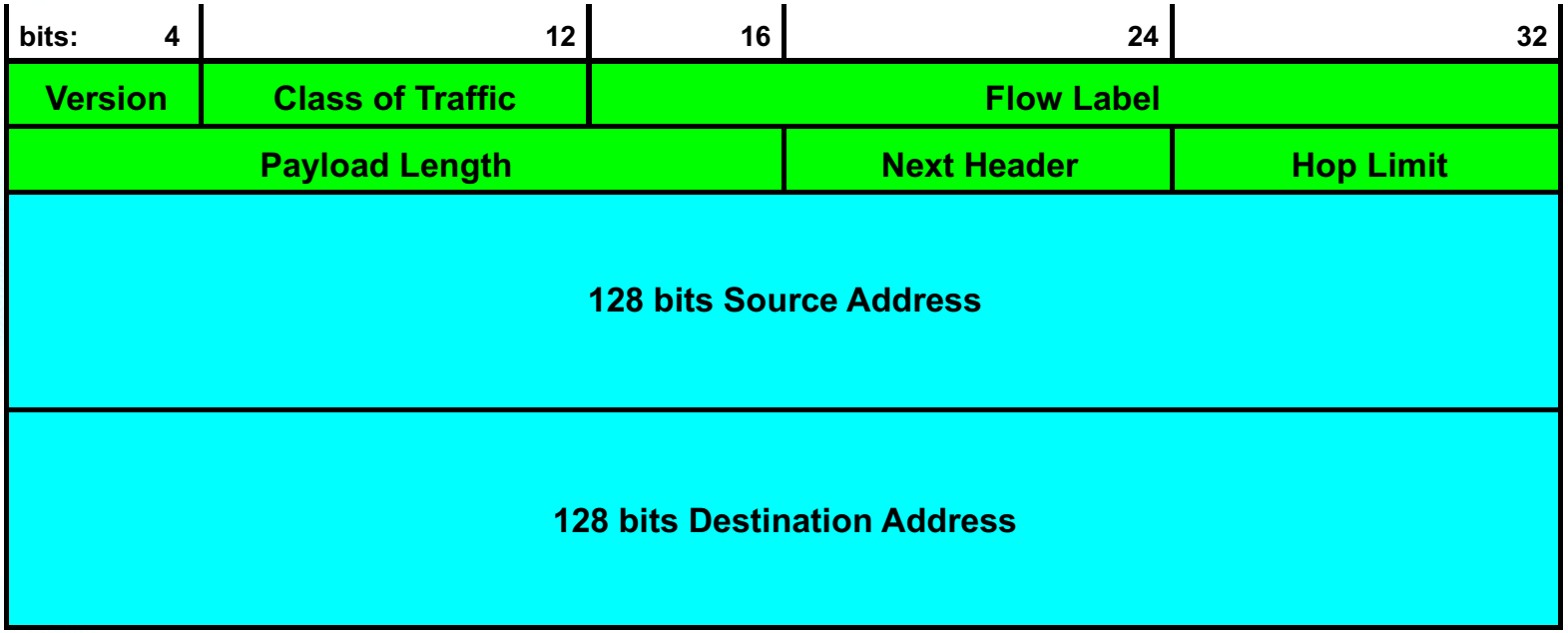
Formato de la Cabecera IPv4

- 20 Bytes + Opciones (40 Bytes máximo)
  - Tamaño variable: 20 Bytes a 60 Bytes



Formato de la Cabecera IPv6

- Reducción de 12 a 8 campos (40 bytes)



  - Evitamos la redundancia del checksum
  - Fragmentación extremo-a-extremo

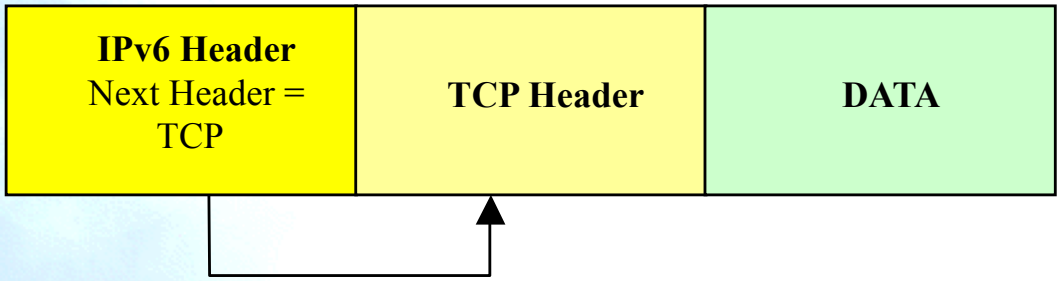
Resumen de los cambios de la Cabecera

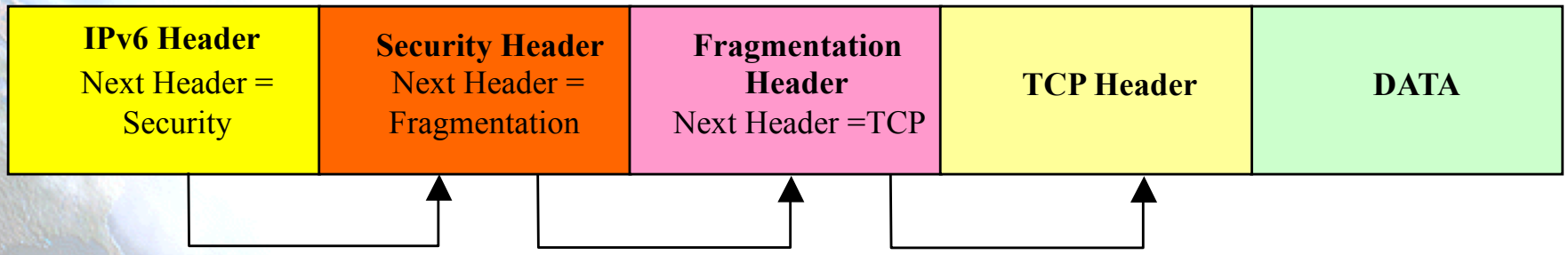
- 40 bytes
- Direcciones incrementadas de 32 a 128 bits
- Campos de fragmentación y opciones retirados de la cabecera básica
- Retirado el checksum de la cabecera
- Longitud de la cabecera es sólo la de los datos (dado que la cabecera tiene una longitud fija)
- Nuevo campo de Etiqueta de Flujo
- TOS -> Traffic Class
- Protocol -> Next Header (cabeceras de extensión)
- Time To Live -> Hop Limit
- Alineación ajustada a 64 bits
- **Las cabeceras NO SON COMPATIBLES**

4. Cabeceras de Extensión

Cabeceras de Extensión

- Campo “Next Header”





Ventajas de las Cabeceras de Extensión

- Procesadas sólo por los nodos destino
  - Excepción: Hop-by-Hop Options Header
- Sin limitaciones de “40 bytes” en opciones (IPv4)
- Cabeceras de extensión definidas hasta el momento (usar en este orden):
  - Hop-by-Hop Options (0)
  - Destination Options (60) / Routing (43)
  - Fragment (44)
  - Authentication (RFC4302, next header = 51)
  - Encapsulating Security Payload (RFC4303, next header = 50)
  - Destination Options (60)
  - Mobility Header (135)
  - No Next Header (59)
    - TCP (6), UDP (17), ICMPv6 (58)

Definir Cabeceras de Extensión

- Como se ha visto las cabeceras de extensión son un mecanismo potente que permite añadir funcionalidades
- Para “regular” la creación de nuevas cabeceras de extensión se establecen algunas reglas y un formato [RFC6564]:
  - Se debe preferir el uso de *Destination Options* para mandar información, en la cabecera *Destination Options* ya existente
  - Usar *Extension Headers* solamente si con una *Destination Option* no se pueden satisfacer las necesidades
  - Se debe evitar la creación de cabeceras de extensión con comportamiento hop-by-hop y crear nuevas opciones para esa cabecera de extensión, siempre que sea posible
  - Por compatibilidad, no se deben crear nuevas cabeceras de extensión a no ser que no se pueda usar ninguna opcion nueva en las cabeceras ya existentes

Cabecera de Fragmentación

- Se emplea cuando el paquete que se desea transmitir es mayor que el Path MTU existente hacia el destino
- En IPv6 la fragmentación se realiza en el origen, nunca en los nodos intermedios
- Next Header = 44

8 bits	8 bits	13 bits unsigned	2 bits	1 bit
Next Header	**Reserved = 0**	**Fragment Offset**	**Res. = 0**	**M**
Identification				

- Paquete Original (no fragmentado):

Unfragmentable Part	**Fragmentable Part**

Proceso de Fragmentación

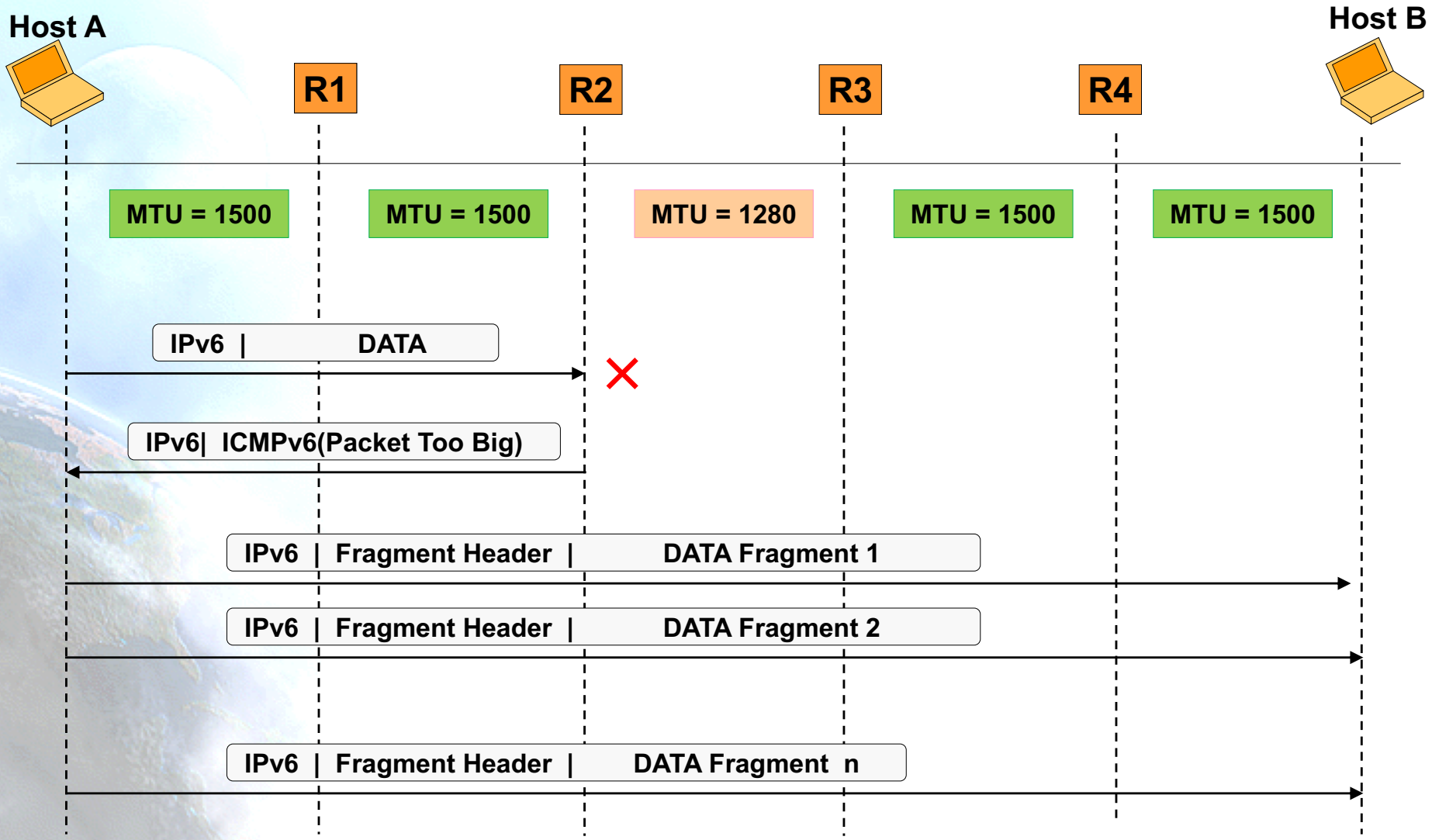
- La parte fragmentable del paquete original se divide en fragmentos de tamaño múltiplo de 8 bytes, excepto el último. Cada fragmento se envía en paquetes separados

Unfragmentable Part	1st Fragment	2nd Fragment	...	Last Fragment

- Paquetes fragmentados:

Unfragmentable Part	Fragment Header	1st Fragment
Unfragmentable Part	Fragment Header	2nd Fragment
• • •		
Unfragmentable Part	Fragment Header	Last Fragment

Fragmentación en Origen



5. Tamaño de Paquetes

MTU Mínimo

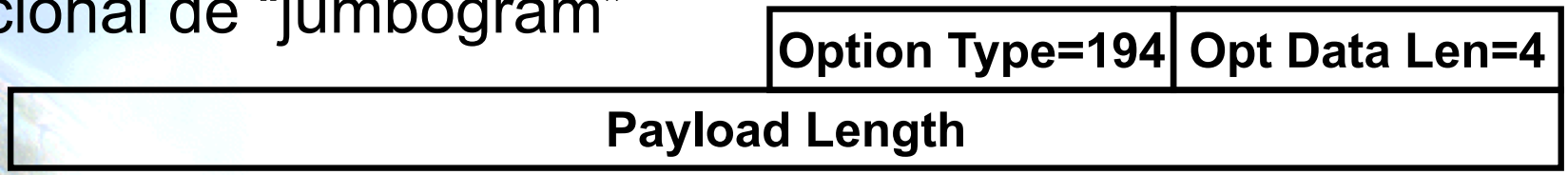
- Link MTU:
  - El máximo MTU del link, es decir, el tamaño máximo del paquete IP que puede transmitirse sobre el link.
- Path MTU:
  - El mínimo MTU de todos los links en la ruta desde el nodo origen hasta el nodo destino.
- El mínimo link MTU para IPv6 es de 1280 bytes en vez de 68 bytes como en el caso de IPv4.
- En links donde Path MTU < 1280, es necesario usar fragmentación y reensamblado en el nivel de enlace.
- En links donde se puede configurar el MTU, se recomienda usar el valor de 1500 bytes.

Descubrimiento del Path MTU (RFC8201, STD87)

- Las implementaciones deben realizar el descubrimiento del path MTU enviando paquetes mayores de 1280 bytes.
  - Para cada destino, se comienza asumiendo el MTU del primer salto
  - Si un paquete llega a un link en el que el MTU es menor que su tamaño, se envía al nodo origen un paquete ICMPv6 “packet too big”, informando del MTU de ese link. Dicho MTU se guarda para ese destino específico
  - Ocasionalmente se descartan los valores almacenados de MTU para detectar posibles aumentos del MTU para los diversos destinos
- Las implementaciones minimalistas pueden omitir todo el proceso de descubrimiento de MTU si observan que los paquetes de 1280 bytes pueden llegar al destino.
  - Útil en implementaciones residentes en ROM

Tamaño Máximo de Paquete

- En el campo de datos de la cabecera IPv6 caben hasta 65.535 bytes (no se incluyen por tanto los 40 bytes de la cabecera IPv6)
- Pero se pueden transportar mayores tamaños si el campo Payload Length es igual a cero y se añade la cabecera opcional de “jumbogram”



- El inconveniente es que no se pueden fragmentar “jumbograms” (RFC2675)

6. Etiquetas de Flujo

Flow Label

- Campo de 20 bits en cabecera IPv6
- El nodo fuente puede así etiquetar paquetes para que la red los trate como un único flujo
- Especificado su uso por el RFC6437
  - Ejemplos como balanceo de carga (ECMP, Equal Cost Multi-Path) y agregación de enlaces (LAG, Link Aggregation Group)

7. Clases de Tráfico

Traffic Class

- Campo de 8 bits en cabecera IPv6

- Mismo uso que ToS en IPv4:
  - RFC2474, DS (Differentiated Services)
  - RFC3168, ECN (Explicit Congestion Notification)

8. Protocolos de capas Superiores

Checksums en Capas Superiores

- Cualquier protocolo de transporte o en general de capa superior a la de Red que incluya la dirección de los nodos para el cálculo de su "checksum" debe ser modificado para ser usado con IPv6 puesto que las nuevas direcciones son de 128 bits en vez de 32
- "pseudo-header" TCP/UDP para IPv6:

Source Address	
Destination Address	
Upper-Layer Packet Length	
zero	Next Header

- ICMPv6 incluye la pseudo-cabecera anterior para calcular su "checksum" a diferencia de ICMPv4. La razón es para proteger ICMP de las pérdidas o corrupción de los campos de la cabecera IPv6 de los que depende, los cuales, a diferencia de IPv4 no están cubierto por un "checksum" inter-capa. El valor del campo Next Header en la pseudo-cabecera es de 58 que identifica la versión IPv6 de ICMP

Máximo Tiempo de Vida del Paquete

- Los nodos IPv6 no están obligados a configurar un tiempo de vida para los paquetes IPv6
- Por este motivo el campo “Time to Live” de IPv4 ha sido renombrado en IPv6 por “Hop Limit”
- Esto no supone un cambio real puesto que en la práctica muy pocas implementaciones de IPv4 cumplen el requisito de limitar la vida del paquete
- Cualquier protocolo de capa superior que dependa de la capa de Red (tanto IPv4 como IPv6) para limitar el tamaño de vida del paquete, debería actualizarse para proporcionar su propio mecanismo de detección de descarte de paquetes obsoletos

Máximo Tamaño de Datos de Capas Superiores

- Cuando se calcula el tamaño máximo disponible de datos para capas superiores, el protocolo de capa superior debe tener en cuenta el mayor tamaño de la cabecera IPv6 respecto de la cabecera IPv4
- Ejemplo: En IPv4, la opción MSS de TCP se calcula como el tamaño máximo de paquete menos 40 bytes (20 bytes para el tamaño mínimo de la cabecera IPv4 y 20 bytes para el tamaño mínimo de la cabecera TCP). Al usar TCP sobre IPv6, el valor de MSS se debe calcular como el máximo tamaño de paquete menos 60 bytes puesto que el tamaño mínimo de la cabecera IPv6 es de 20 bytes mayor que la de IPv4

Respuestas a Paquetes con Cabeceras de Encaminamiento

- Cuando un protocolo de capa superior envía uno o más paquetes en respuesta a paquetes recibidos que incluyen una cabecera de encaminamiento, los paquetes de respuesta no deben incluir otra cabecera de encaminamiento derivada de la inversión de la primera a no ser que la integridad y autenticidad de la dirección de origen y de la cabecera de encaminamiento se haya verificado mediante el uso de una cabecera de Autenticación.

9. Otros Aspectos

Cambios respecto de RFC2460

- Cambios editoriales y similares, incluyendo textos procedentes de otros RFCs, updates, erratas, etc.
- Clarificación respecto de las cabeceras de extensión, con la excepción de “hop-by-hop” no son procesadas, insertadas o eliminadas por ningún nodo en el camino
- Clarificaciones diversas sobre la fragmentación
- Mejorada la sección de “consideraciones de seguridad”

IPv6 es Obligatorio (RFC6540)

- IPv6 ya no es considerado opcional [RFC6540, BCP177], Abril 2012, recomendaciones:
  - Nuevas implementaciones de IP deben soportar IPv6
  - Actualizaciones de implementaciones de IP deben soportar IPv6
  - La calidad y funcionalidad del soporte de IPv6 debe ser igual o mayor que para IPv4 en las implementaciones nuevas o actualizadas
  - Las implementaciones IP nuevas o actualizadas deben soportar IPv4 e IPv6 (doble-pila), pero no deben requerir de IPv4 para una funcionalidad completa y adecuada
  - Se anima a los implementadores a actualizar las implementaciones de hardware y software con IPv6 siempre que sea técnicamente viable

Gracias !!

Contacto:

- Jordi Palet (The IPv6 Company): jordi.palet@theipv6company.com