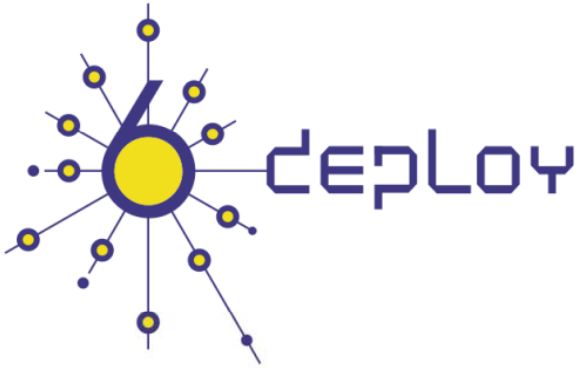
Curso IPv6

WALC 2009

Bogotá – Colombia

21 al 25 Septiembre 2009



César Olvera (cesar.olvera@consulintel.es)

Alvaro Vives (alvaro.vives@consulintel.es)

deploy

Consulintel

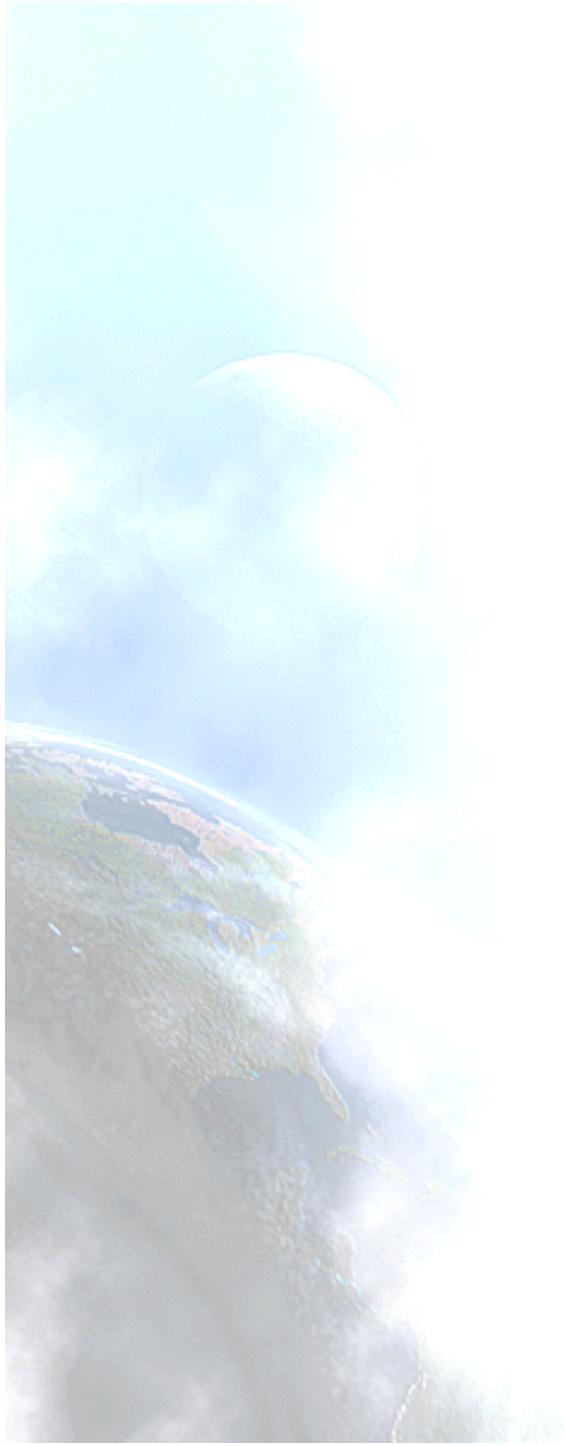
Consultores Integrales en Telecomunicaciones

Contenido del curso (1)

- **Bloque 1. Tutorial IPv6**
  1. Introducción a IPv6
  2. Formatos de cabeceras y tamaño de paquetes
  3. Direccionamiento IPv6
  4. ICMPv6, Neighbor Discovery y DHCPv6
  5. Seguridad IPv6
  6. Encaminamiento con IPv6
  7. Mecanismos de Transición
  8. Movilidad IPv6

Contenido del curso (2)

- **Bloque 2. Otros Aspectos Avanzados**
  9. Calidad de Servicio (QoS)
  10. Multicast
  11. Multi-homing
  12. Porting de aplicaciones
  13. Gestión SNMP sobre IPv6
  14. IPv6 sobre MPLS
  15. DNS IPv6



Bloque 1

Tutorial IPv6

2. Formatos de cabeceras y tamaño de paquetes

2.1 Terminología
2.2 Formato cabecera IPv6
2.3 Consideraciones sobre tamaño de paquete
2.4 Consideraciones sobre protocolos de capa superior
2.5 Jumbogramas

2.1 Terminología

IPv6 (RFC2460)

- 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

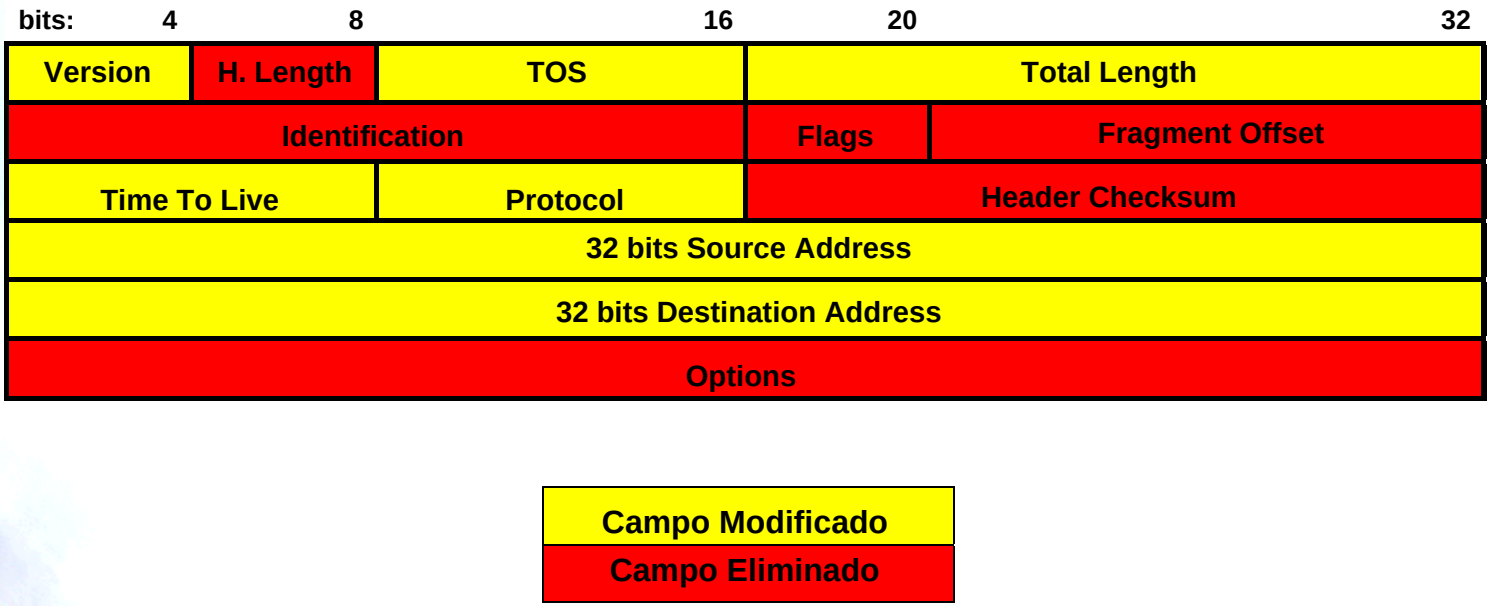
Terminología

- **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

2.2 Formato cabecera IPv6

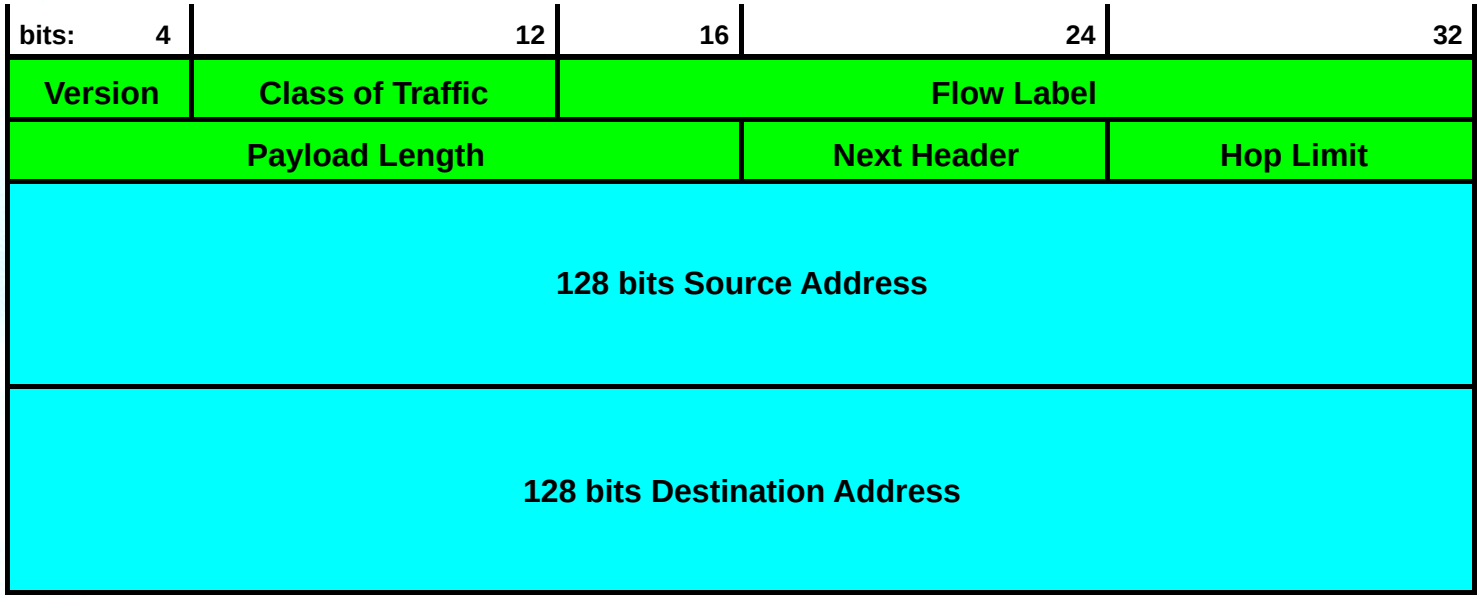
Formato de la Cabecera IPv4

- 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)



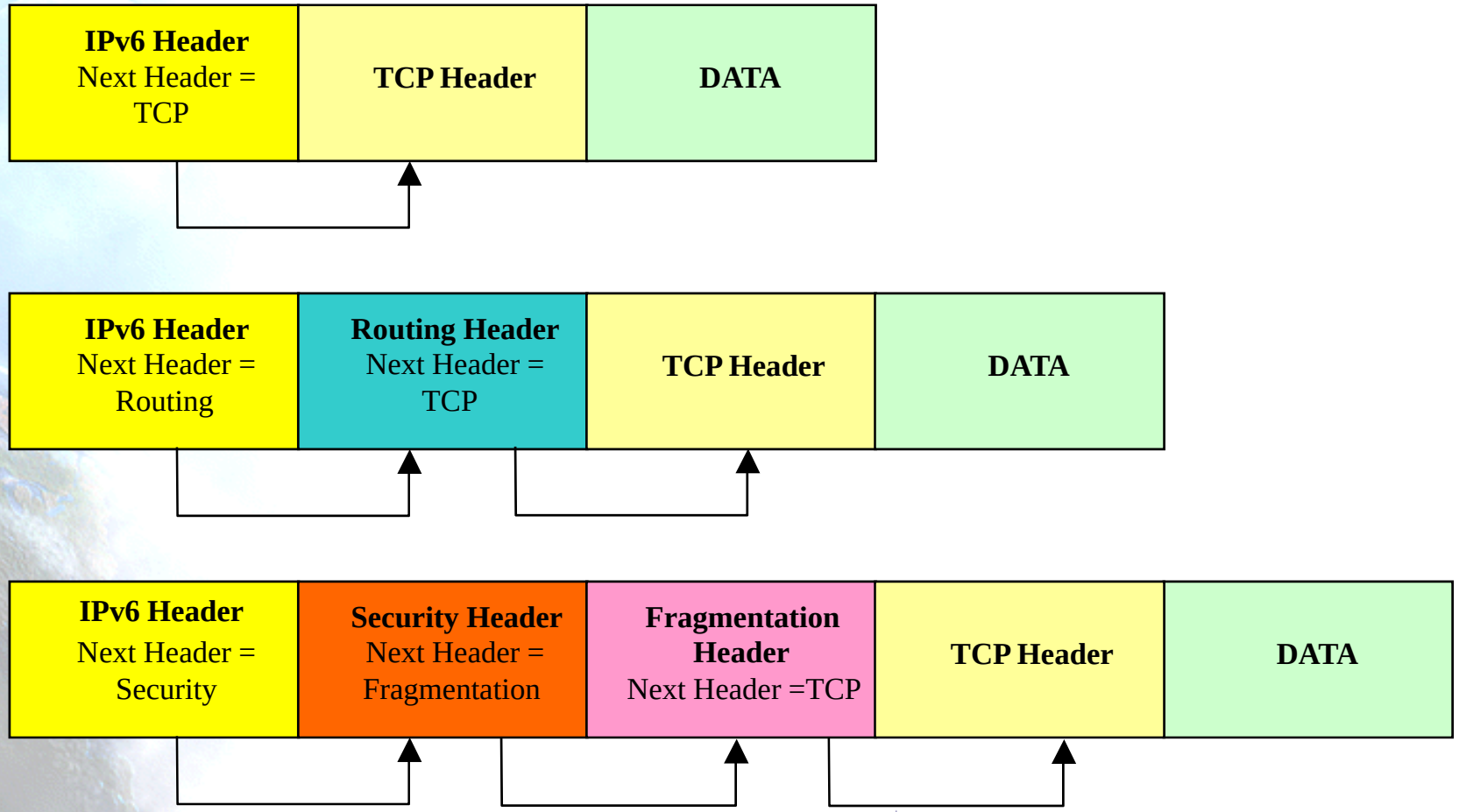
  - Evitamos la redundancia del checksum
  - Fragmentación extremo-a-extremo

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**

Cabeceras de Extensión

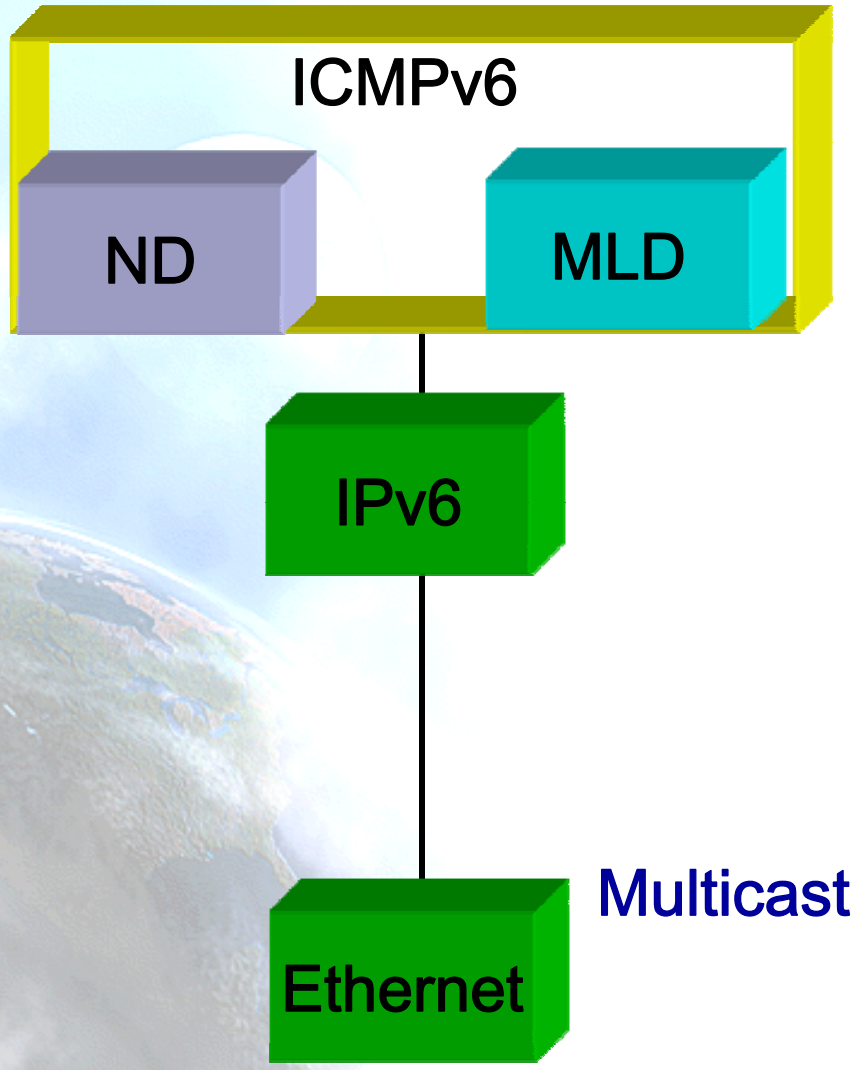
- Campo “Next Header”

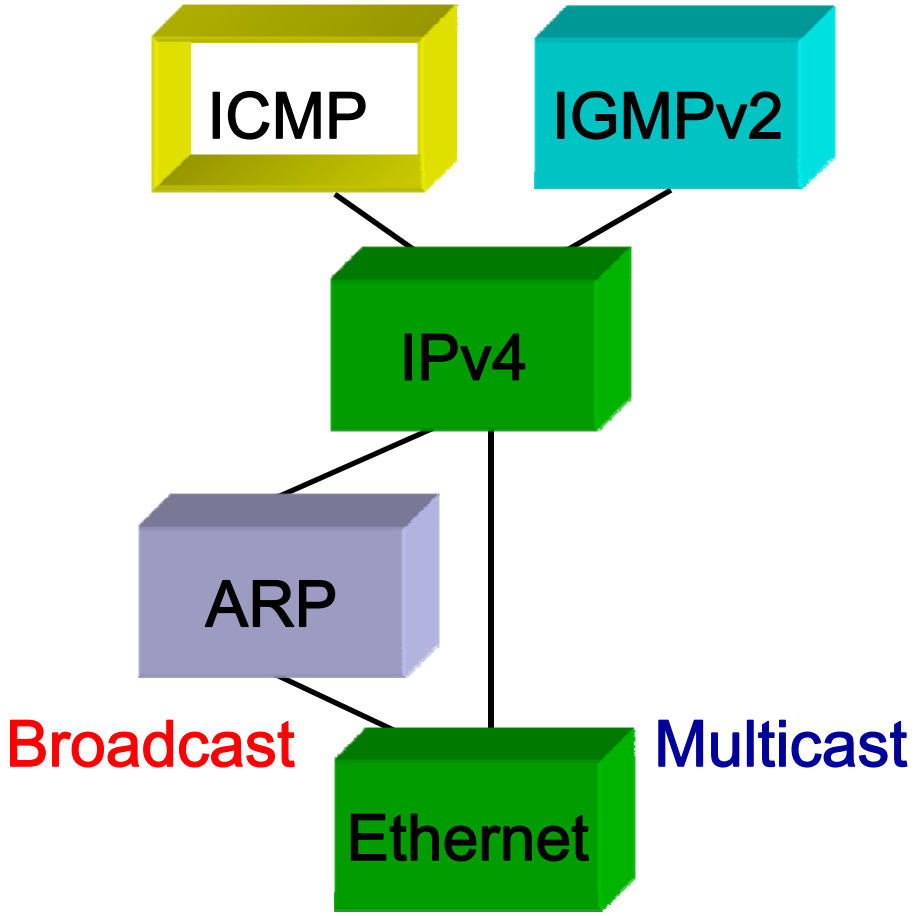


Ventajas de las Cabeceras de Extensión

- 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)

Plano de Control IPv4 vs. IPv6





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:

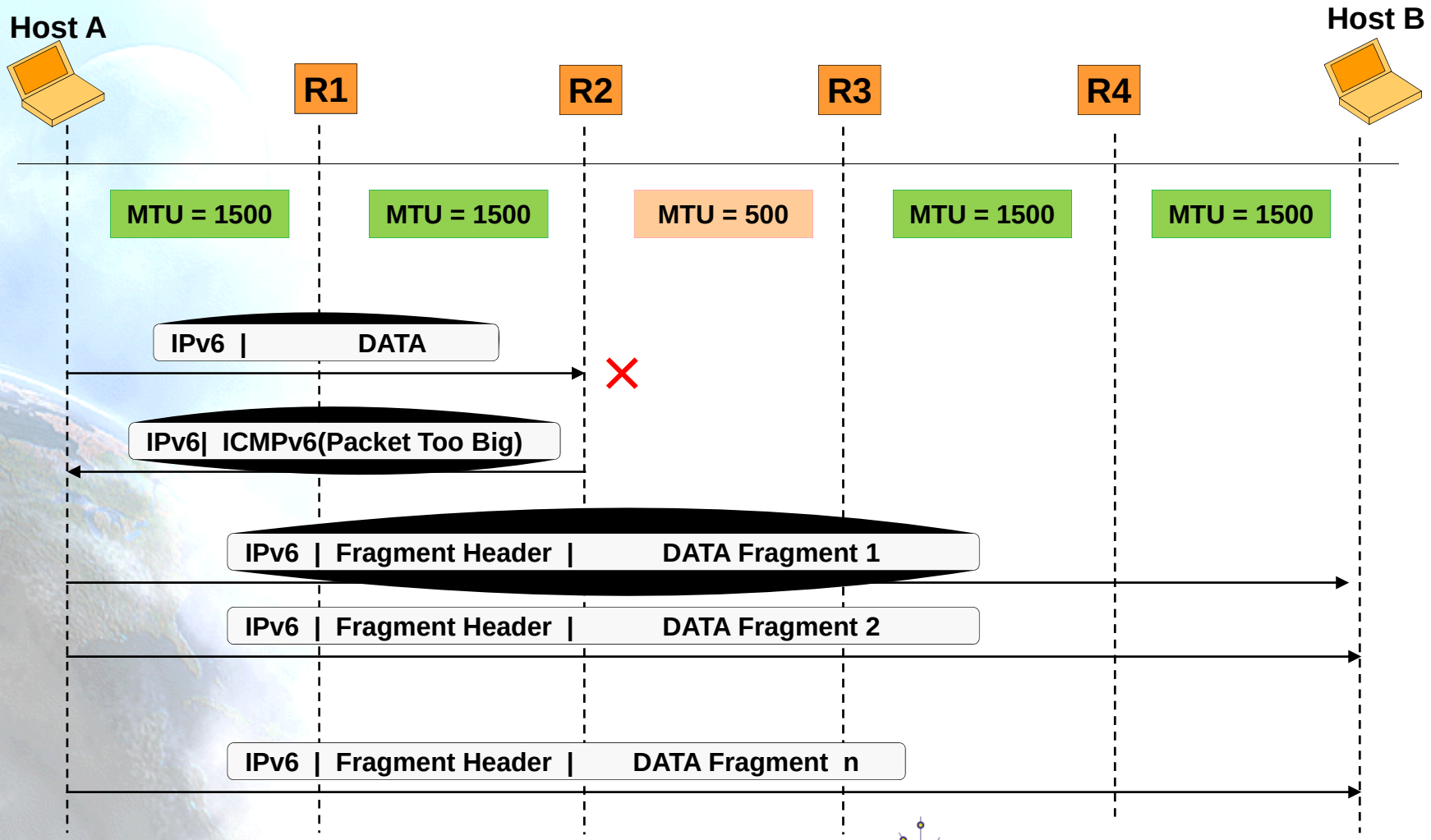
Unfragmentable Part	Fragment Header	1st Fragment

Unfragmentable Part	Fragment Header	2nd Fragment

• • •

Unfragmentable Part	Fragment Header	Last Fragment

Fragmentación en Origen



2.3 Consideraciones sobre tamaño de paquete

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 (RFC1981)

- 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

Cabecera de Fragmentación

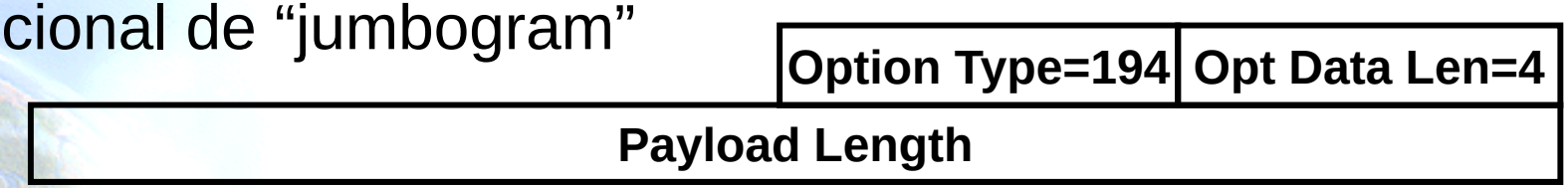
Next Header	Reserved	Fragment Offset	0 0 M
Original Packet Identifier			

- Aunque no es recomendable, se puede usar la cabecera Fragment Header para ayudar a los protocolos superiores a realizar el descubrimiento del path MTU

- La fragmentación y reensamblado de los paquetes IPv6 es una función que se realiza en los extremos finales. Los encaminadores no fragmentan los paquetes si estos resultan ser demasiado grandes para el link por el que se van a encaminar sino que envían un paquete ICMPv6 de tipo “packet too big”

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)

2.4 Consideraciones sobre protocolos de capa superior

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.

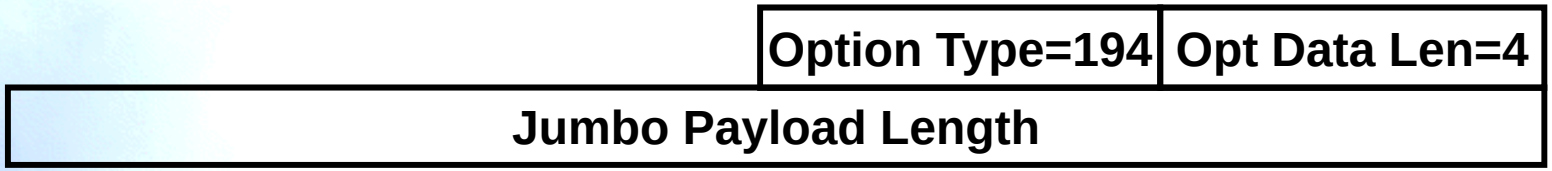
2.5 Jumbogramas

Jumbogramas IPv6 (RFC2675)

- “Jumbograma" es un paquete IPv6 que contiene una parte para datos (payload) mayor que 65.535 octetos
- Jumbograma
  - Sólo es relevante en nodos IPv6 que pueden estar conectados en enlaces con una MTU mayor de 65.575 octetos (65.535 + 40 de la cabecera IPv6)
  - No necesita ser implementados por los nodos IPv6 que no soportan enlaces con MTU tan grades
- RFC2675 describe la opción “IPv6 Jumbo Payload”
  - También proporciona la forma de especificar longitudes de datos tan grandes
  - Y describe los cambios necesarios en TCP y UPD para que puedan hacer uso de los Jumbogramas

Opción “IPv6 Jumbo Payload”

- La opción “Jumbo Payload” se transporta en la opción “IPv6 Hop-by-Hop”, justo a continuación de la cabecera IPv6
- Formato:



- Campo “Jumbo Payload Length”
  - Entero sin signo de 32-bit
  - Longitud del paquete IPv6 en octetos, excluyendo la cabecera IPv6 pero incluyendo la cabecera “Hoy-by-Hop” y otras posibles cabeceras de extensión existentes
  - Debe ser mayor que 65.535

Jumbogramas UDP

- El campo de 16 bits de la cabecera UDP limita la longitud total de un paquete UDP (cabecera UDP más datos) por debajo de 65.535 octetos

- RFC2675 define la modificación de UDP para sobrepasar ese límite:
  - Los paquetes UDP mayores de 65.535 octetos se pueden enviar poniendo el valor cero en el campo “UDP length”, dejando al receptor la responsabilidad de averiguar la longitud real del paquete UDP basándose en la longitud del paquete IPv6
  - Hay que notar que antes de esta modificación, el cero no era un valor permitido para el campo “UDP length” porque dicho campo incluye la cabecera UDP, de manera que el valor mínimo era de 8

Jumbogramas TCP

- En la cabecera TCP no hay un campo para la longitud del paquete, de manera que no hay nada que limite la longitud de un paquete TCP individual. Sin embargo:
  - El valor MSS que se negocia en el comienzo de una conexión limita el tamaño del paquete más grande que se puede transmitir
  - El “Urgent Pointer” no puede referenciar datos > 65.535 octetos
- Soluciones
  - Al determinar qué valor MSS value se puede enviar
    - Si MTU del interfaz directamente conectado menos 60 > = 65.535, entonces se configura MSS a 65.535
    - Cuando se recibe un valor MSS de 65.535, se trata como si fuerea infinito
    - El MSS real se determina restando 60 del valor aprendido al ejectur “Path MTU Discovery” sobre el camino que se debe recorrer hacia el otro extremo de la conexión TCP
  - El problema del “Urgent Pointer” se resuelve añadiendo una opción “TCP Urgent Pointer”. Sin embargo, dado que es improbable que las aplicaciones que usan Jumbogramas también usen “Urgent Pointers”, un cambio menos agresivo, parecido a la propuesta para MSS sería suficiente

Gracias !!

Contacto:

- Cesar Olvera (Consulintel): cesar.olvera@consulintel.es
- Alvaro Vives (Consulintel): alvaro.vives@consulintel.es

6DEPLOY Project: http://www.6deploy.org

The IPv6 Portal: http://www.ipv6tf.org