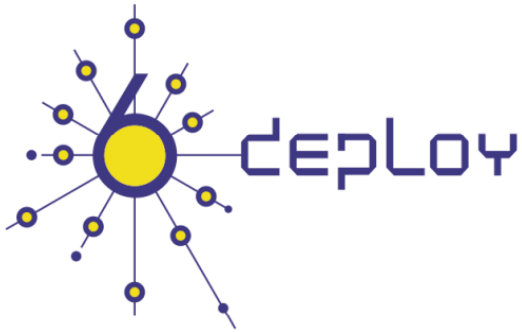
Curso IPv6

Reunión de Primavera 2010

CUDI

Morelia – México

19 al 21 Abril 2010



César Olvera (cesar.olvera@consulintel.es)
Alvaro Vives (alvaro.vives@consulintel.es)
Jordi Palet (jordi.palet@consulintel.es)

deploy

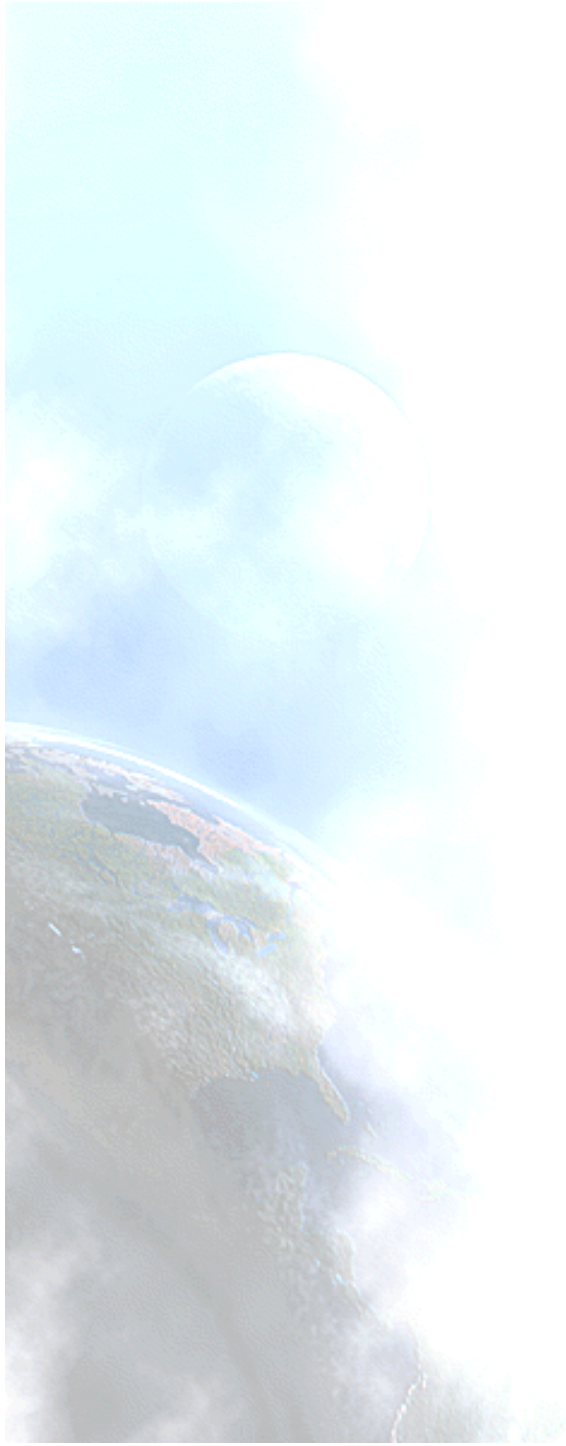
ConsulinTel
Consultores Integrales en Telecomunicaciones

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

Contenido del curso (2)

- **Bloque 2. Otros Aspectos Avanzados**
  8. Calidad de Servicio (QoS)
  9. Multicast
  10. DNS IPv6
  11. Movilidad IPv6



Bloque 1

Tutorial IPv6

1. Introducción a IPv6

1.1 Historia de IPv6

1.2 Ventajas de IPv6

1.1 Historia de 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, ethernet, etc.

Requisitos de IPng

- Noviembre, 1991
  - IETF creó un grupo de trabajo para analizar el problema del crecimiento de Internet y considerar posibles soluciones
- Julio, 1992
  - IETF determinó que era imprescindible comenzar con el diseño de un protocolo de nueva generación para Internet (next-generation Internet Protocol, IPng)
- IPng tenía que solucionar dos problemas:
  - Soportar un gran espacio de direccionamiento
  - Soportar esquemas de direccionamiento basados en jerarquías de agregación
- Aunque también aparecieron nuevos requisitos para mejorar las deficiencias de IPv4:
  - Seguridad (tanto autenticación como encriptación)
  - Auto configuración de red (Plug-and-play)
  - Mejora del soporte de calidad de servicio (QoS)
  - Soporte de movilidad

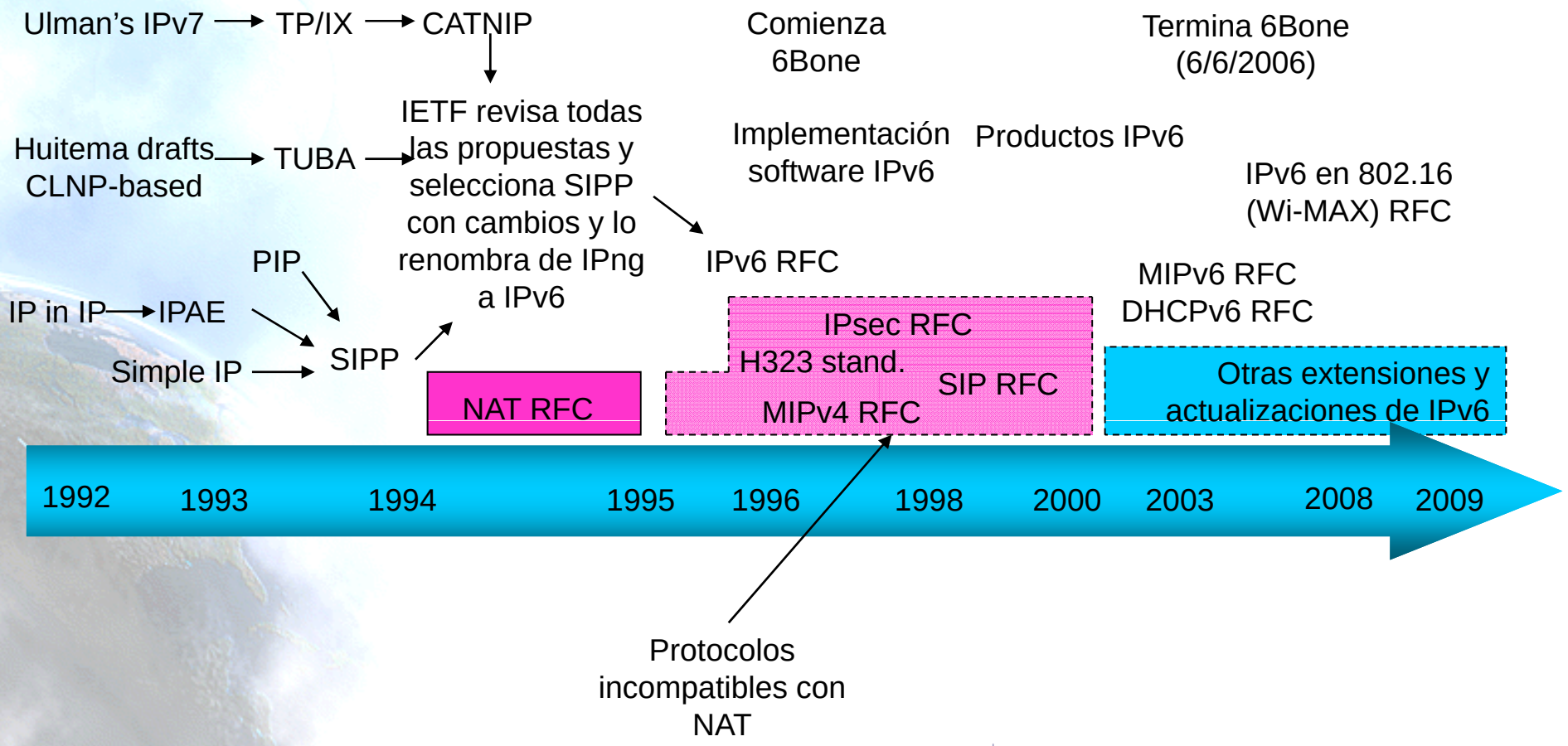
Candidatos para IPng

- La creación y selección de los protocolos nuevos se hace bajo el “paraguas” de IETF
- Entre 1992 y 1994 había siete candidaturas de las que en la primavera de 1994 quedaron solo tres :
  - CATNIP (Common Architecture for the Internet)
    - Diseñado como un “protocolo convergente”, entre IP, IPX de Novell y el protocolo de la capa de red de la suite de OSI
  - SIPP (Simple Internet Protocol Plus)
    - Una evolución del IP actual (IPv4) e inter-operable con él
  - TUBA (TCP and UDP with Bigger Addresses)
    - Una propuesta para adoptar la capa de red de OSI (CLNP) como la nueva capa de red para Internet
- En Julio de1994, IETF seleccionó SIPP como protocolo que debería convertirse en IPng
  - La documentación de SIPP constituyó la base para la definición de IPng
  - El grupo de trabajo SIPP desapareció para integrarse en el grupo IPng
- Aspectos clave de SIPP:
  - Aspectos de transición de IPv4 a IPng
    - Gran período de coexistencia entre ambos protocolos IPv4 e IPng
    - Algunos nodos nunca se actualizarán a IPng
    - Los nodos nuevos IPng pueden usar redes sólo-IPv4 para transportar paquetes IPng (túneles)
    - No se requería un día-D para desplegar IPng
- Más adelante el grupo de trabajo de IETF IPng se renombró oficialmente como IPv6

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 actual

Evolución de IPng



Agotamiento Direcciones IPv4 (1)

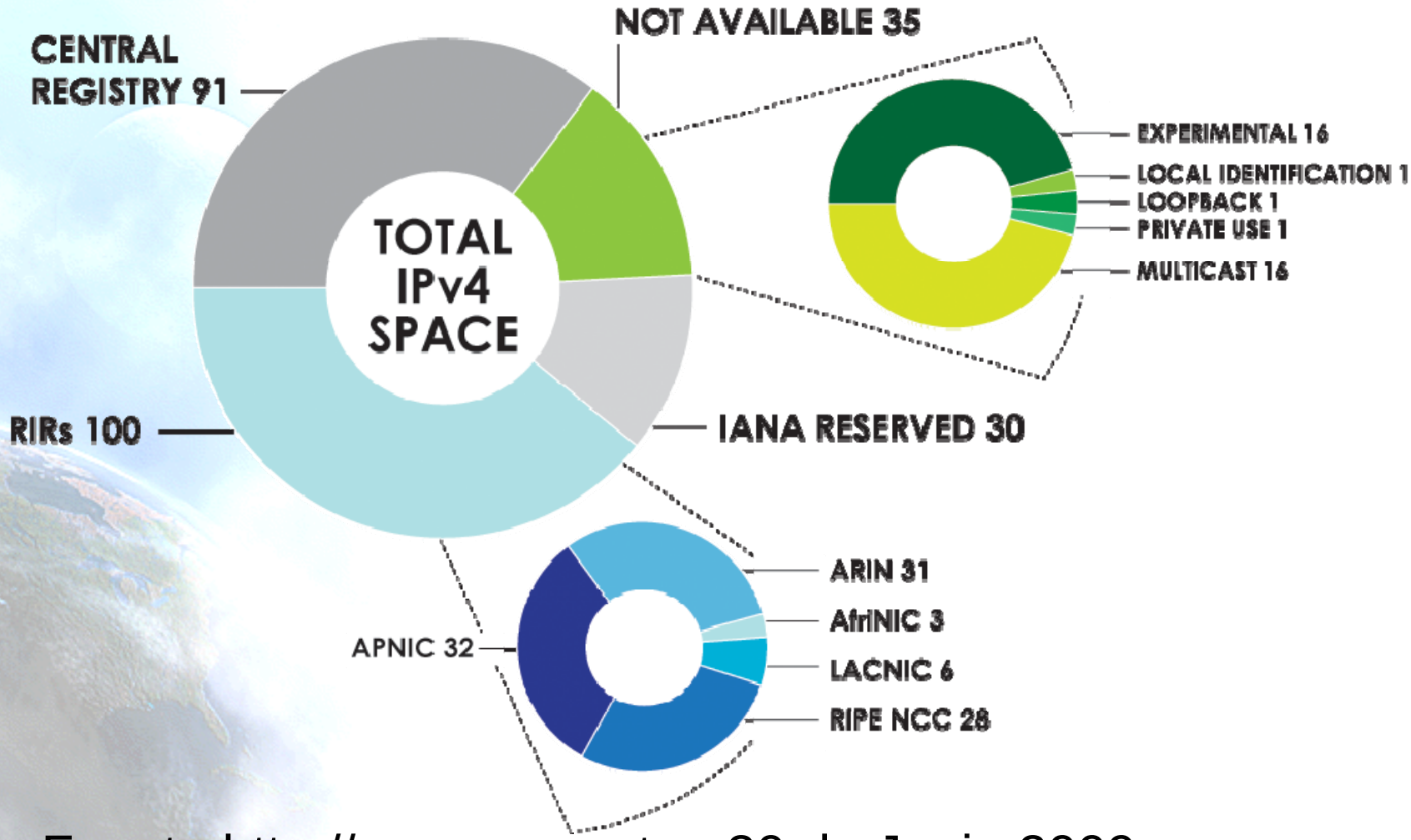
- Opinión extendida: quedan pocos años de direcciones IPv4 públicas -> Debate: Cuando se agotarán?
- Tres estrategias a seguir:
  - Aumentar el uso de NAT -> **introduce problemas técnicos y costes**
  - Tratar de obtener direcciones IPv4 libres o liberadas
  - Implementar IPv6 -> **válida a largo plazo**
- Existen múltiples comunicados de los actores de Internet recomendando la implementación de IPv6 debido al agotamiento de direcciones IPv4:
- The IPv6 Portal: Policy Recommendations: http://www.ipv6tf.org/index.php?page=meet/policy_recommendations

Agotamiento Direcciones IPv4 (2)

Año	Mes	/8s Disponibles (IANA)	Consumo Anual
2006	Septiembre	59	12
	Diciembre	55	
2007	Septiembre	44	13
	Diciembre	42	
2008	Junio	39	8
	Diciembre	34	
2009	Junio	30	4

- 30 /8s significa el 11,7 % de direcciones disponibles

Agotamiento Direcciones IPv4 (3)



Fuente http://www.nro.net a 30 de Junio 2009

Desventajas de NAT

- La traducción se hace compleja a veces (FTP, etc.)
- No es escalable
- Puede dar problemas al unificar varias redes
- Rompe el paradigma end-to-end de Internet
- No funciona con gran número de “servidores”, P2P
- Inhiben el desarrollo de nuevos servicios y aplicaciones
- Problemas con IPsec
- Aumenta el coste de desarrollo de aplicaciones
- Comprometen las prestaciones, robustez, seguridad y manejabilidad de Internet

¿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; obsoletos)
8	PIP	(obsoleto)
9	TUBA	(obsoleto)
10-15		no asignados

1.2 Ventajas de IPv6

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
- Oportunidad para incluir nuevas características, ejemplo “binding updates”

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

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

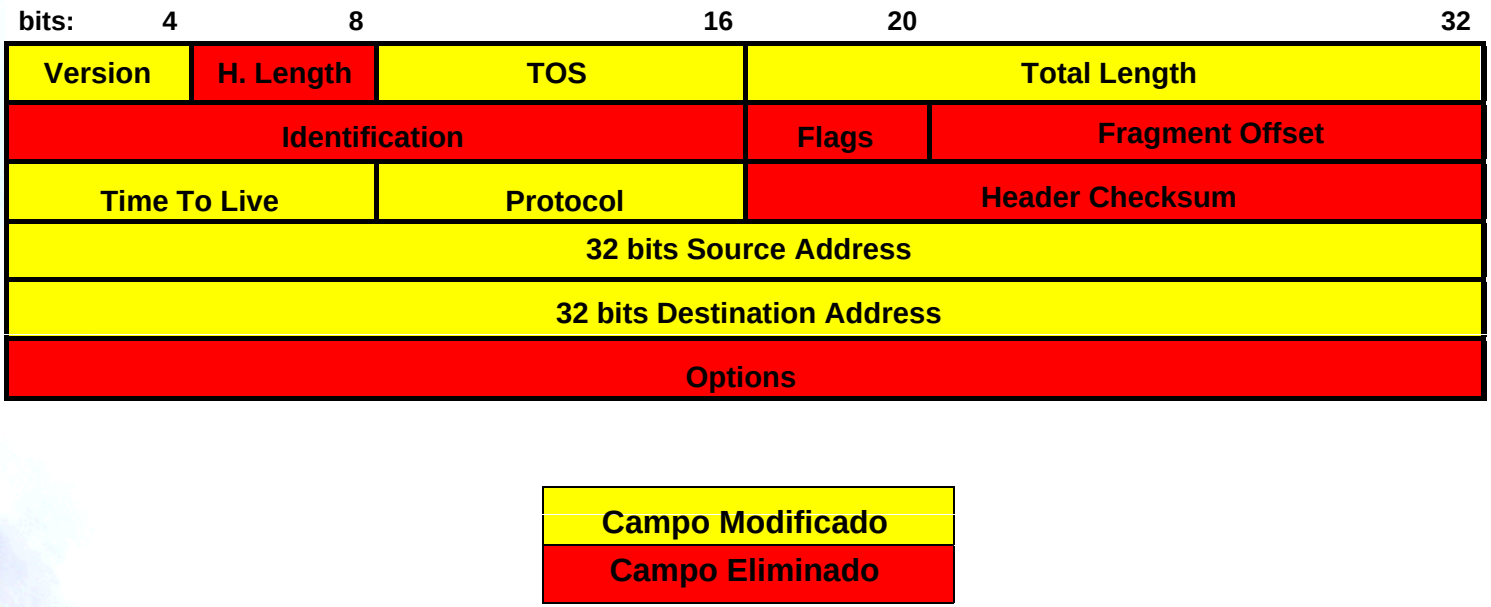
Terminología

- **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

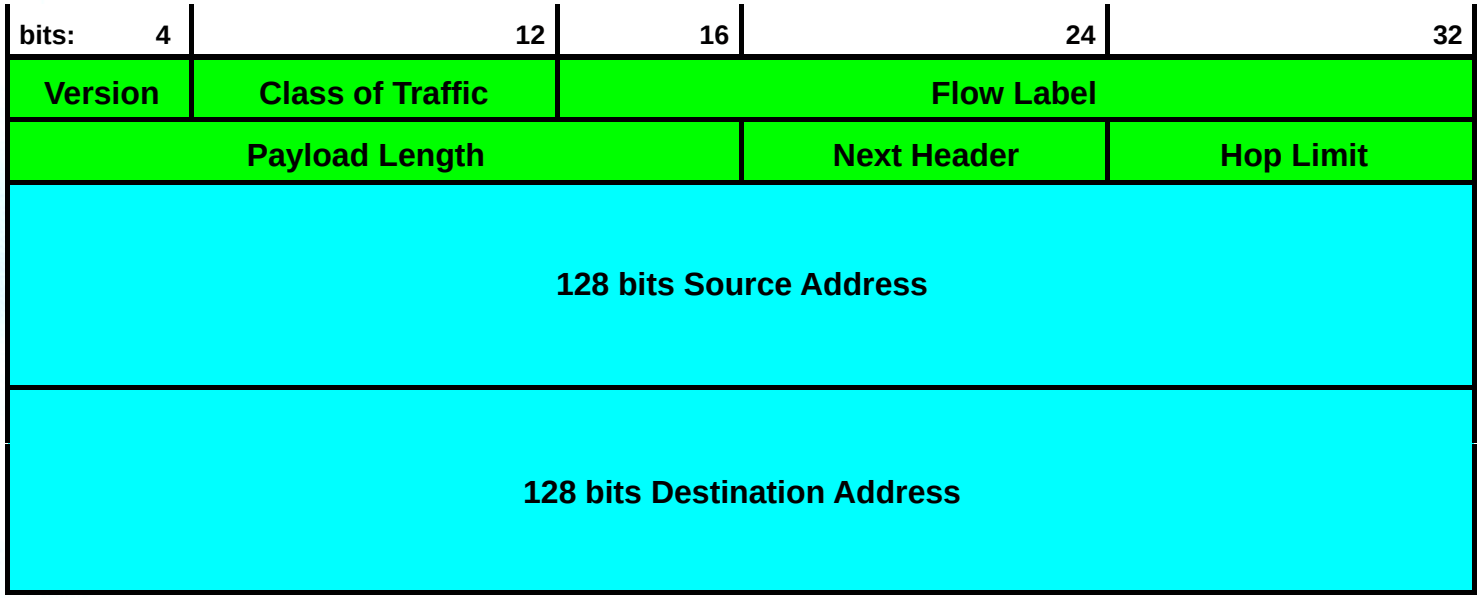
Formato de la Cabecera IPv4

- 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)



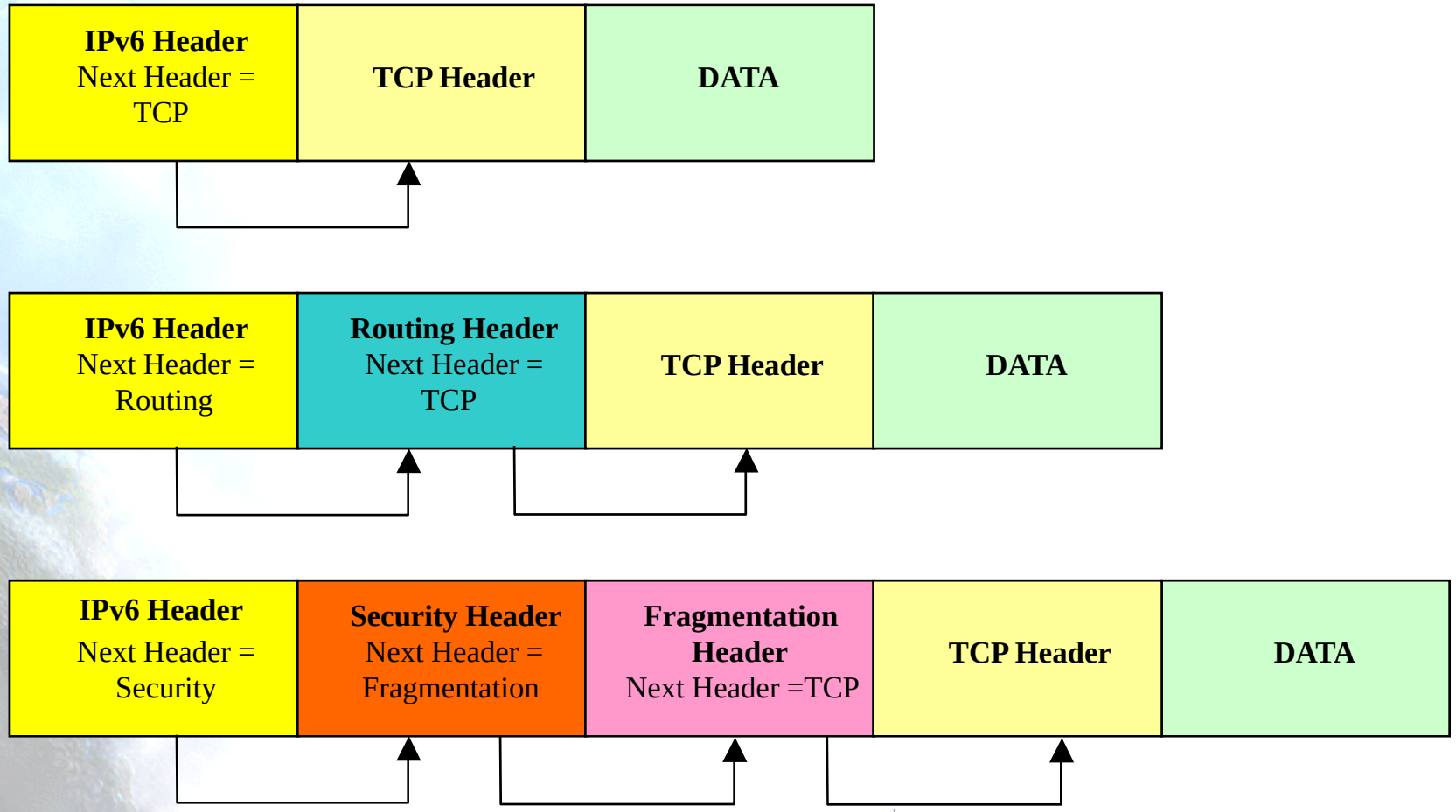
  - Evitamos la redundancia del checksum
  - Fragmentación extremo-a-extremo

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

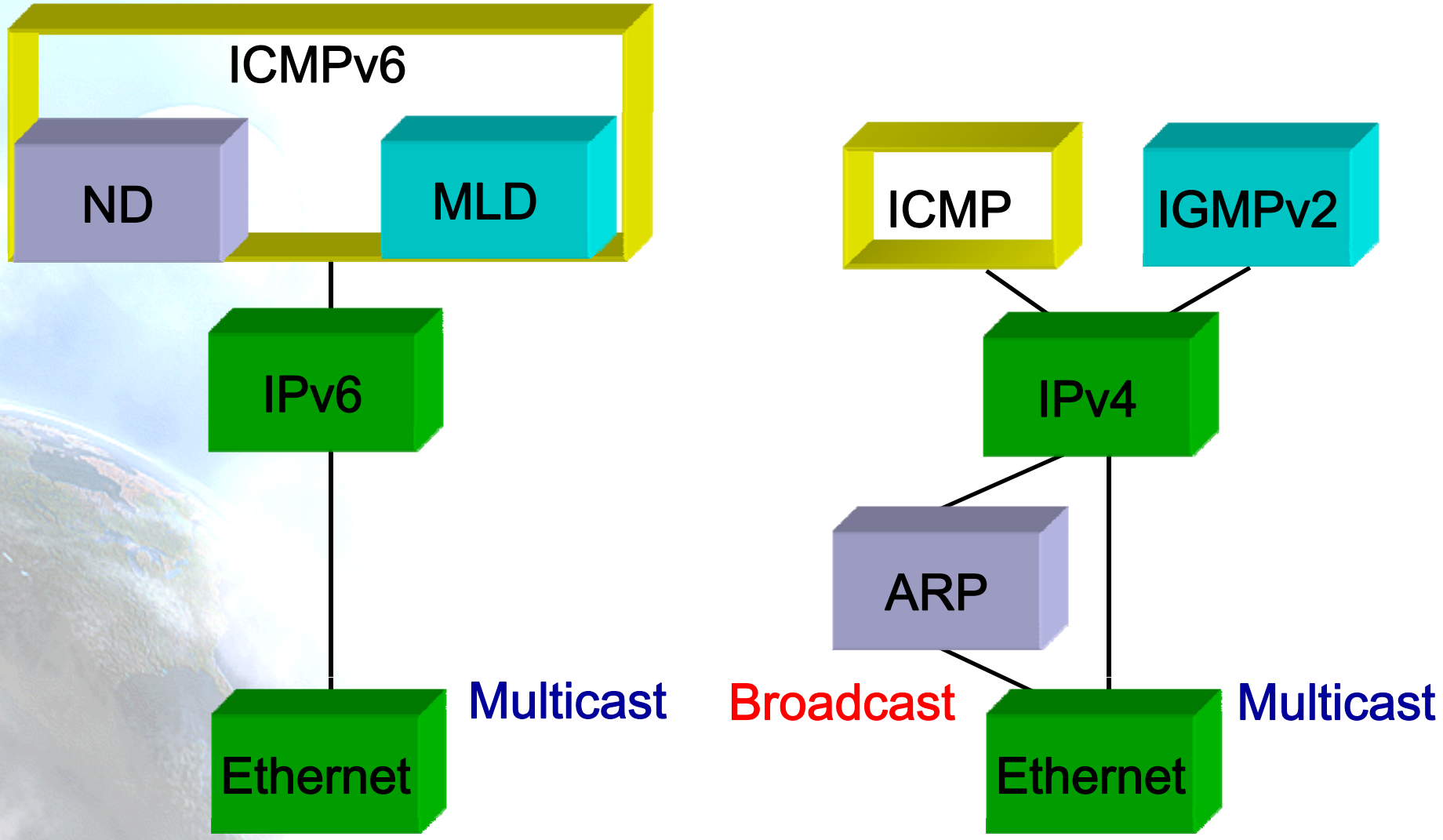
- Campo “Next Header”



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:

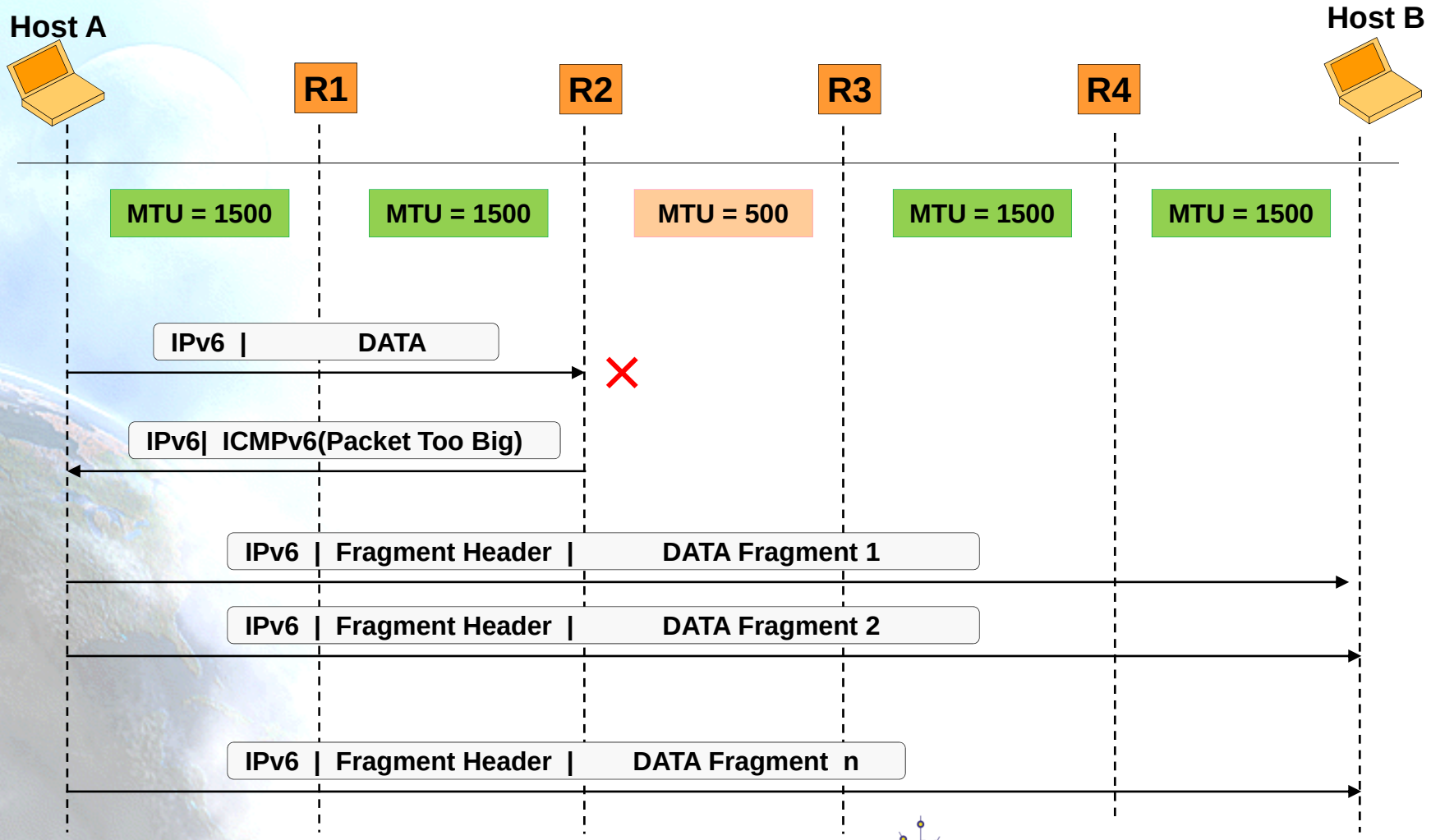
Unfragmentable Part	Fragment Header	1st Fragment

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

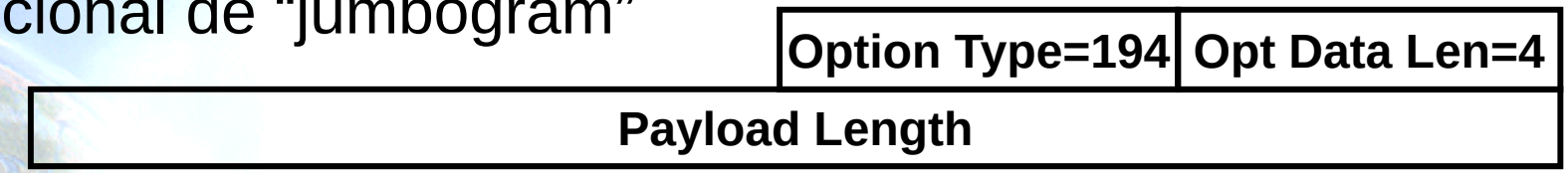
Next Header	Reserved	Fragment Offset	0 0 M
Original Packet Identifier			

- 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.

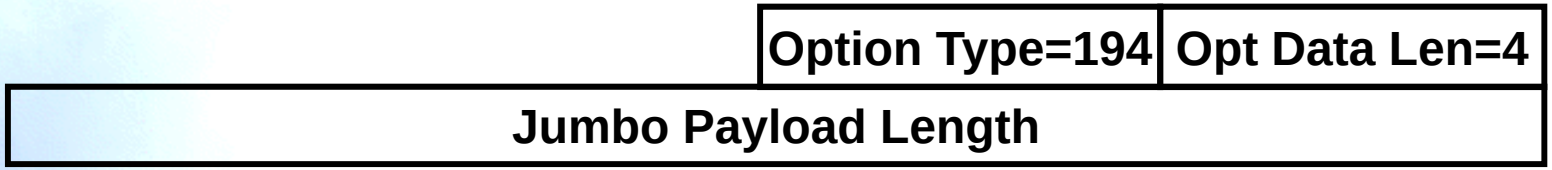
2.5 Jumbogramas

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

3. Direccionamiento IPv6

3.1 Tipos de Direcciones
3.2 Prefijo y representación
3.3 Direcciones IPv6 Unique Local
3.4 Identificadores de interfaz
3.5 Direcciones Multicast
3.6 Otras consideraciones

3.1 Tipos de Direcciones

Tipos de Direcciones (RFC4291)

- Unicast (uno-a-uno)
  - globales
  - enlace-local
  - local-de-sitio (desaprobada)
  - Unique Local (ULA)
  - Compatible-IPv4 (desaprobada)
  - Mapeada-IPv4
- Multicast (uno-a-muchas)
- Anycast (uno-a-la-mas-cercana)
- Reservado

Algunas Direcciones Unicast Especiales

- Del **RFC5156:**
- **Dirección no especificada**, utilizada temporalmente cuando no se ha asignado una dirección: **0:0:0:0:0:0:0:0 (::/128)**

- Dirección de **loopback**, para el “auto-envío” de paquetes: **0:0:0:0:0:0:0:1 (::1/128)**

- Del **RFC3849:**
- **Prefijo de documentación: 2001:0db8::/32**

3.2 Prefijo y representación

Representación Textual de las Direcciones (1)

Formato “preferido”: 2001:DB8:FF:0:8:811:200C:417A

Formato comprimido: 2001:DB8::43

IPv4-compatible: ::13.1.68.3 (desaprobada en RFC4291)

IPv4-mapped: ::FFFF:13.1.68.3

Literal: [2001:DB8:FF::8:200C]
http://[2001:DB8::43]/index.html

Se usan los principios de CIDR: Prefijo / Long. Prefijo

2001:DB8:3003::/48

2001:DB8:3003:2:a00:20ff:fe18:964c/64

Representación Textual de las Direcciones (2)

Normas:

1. 8 Grupos de 16 bits separados por “:”
2. Notación hexadecimal de cada nibble (4 bits)
3. Se pueden eliminar los ceros a la izquierda dentro de cada grupo
4. Se pueden sustituir uno o más grupos “todo ceros” por “::”. Esto se puede hacer **solo una vez**

Ejemplos:

1. (Profesor) 2001:0db8:3003:0001:0000:0000:6543:0ffe

   Queda: 2001:db8:3003:1::6543:ffe
2. (Alumnos) 2001:0db8:0000:0000:0300:0000:0000:0abc

Prefijos de los Tipos de Direcciones

Tipo de Dirección	Prefijo Binario	Notación IPv6
Unspecified	00…0 (128 bits)	::/128
Loopback	00…1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	00…0:1111…1111:IPv4	::FFFF:IPv4/128
IPv4-compatible (desaprobada)	00…0 (96 bits)	::IPv4/128
Site-Local Unicast (desaprobada)	1111 1110 11	FEC0::/10

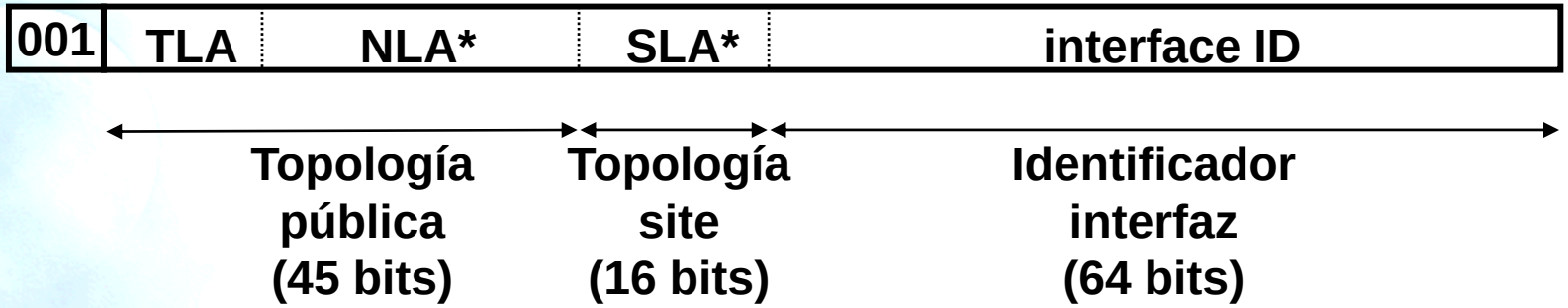
- Direcciones **Anycast** se asignan de los prefijos Unicast

Prefijos Globales Unicast

Tipo de Dirección	Prefijo Binario
IPv4-compatible	0000...0 (96 zero bits) (desaprobada)
IPv4-mapped	00…0FFFF (80 zero+ 16 one bits)
Global unicast	001
ULA	1111 110x (1= Asignado localmente) (0=Asignado centralmente)

- El prefijo **2000::/3** se esta usando para las asignaciones de direcciones Globales Unicast, todos los demás prefijos están reservados (aprox. 7/8 del total).

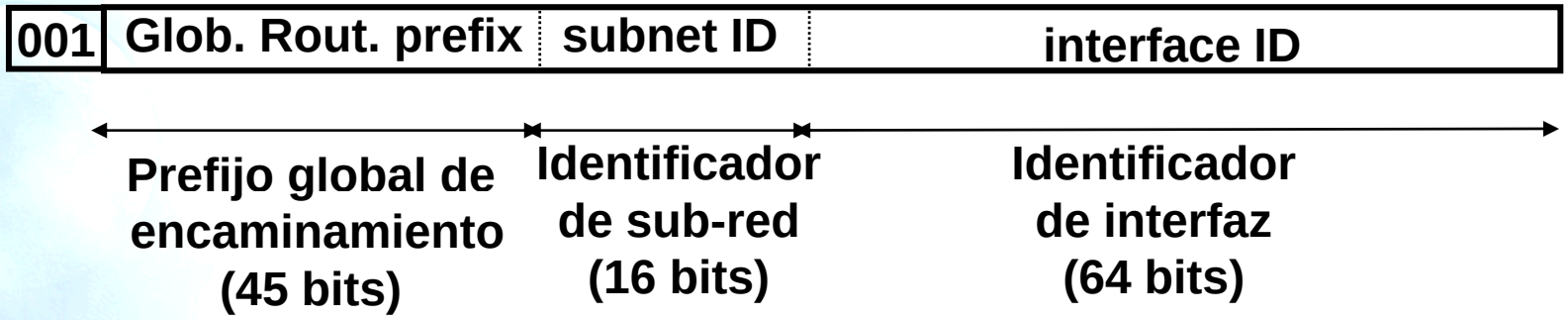
Aggregatable Global Unicast Addresses (RFC2374) (obsoleto)



- TLA = Top-Level Aggregator
  NLA* = Next-Level Aggregator(s)
  SLA* = Site-Level Aggregator(s)
- Se pueden asingar TLAs a ISP o IX

- Obsoleto por RFC3587: IPv6 Global Unicast Address Format

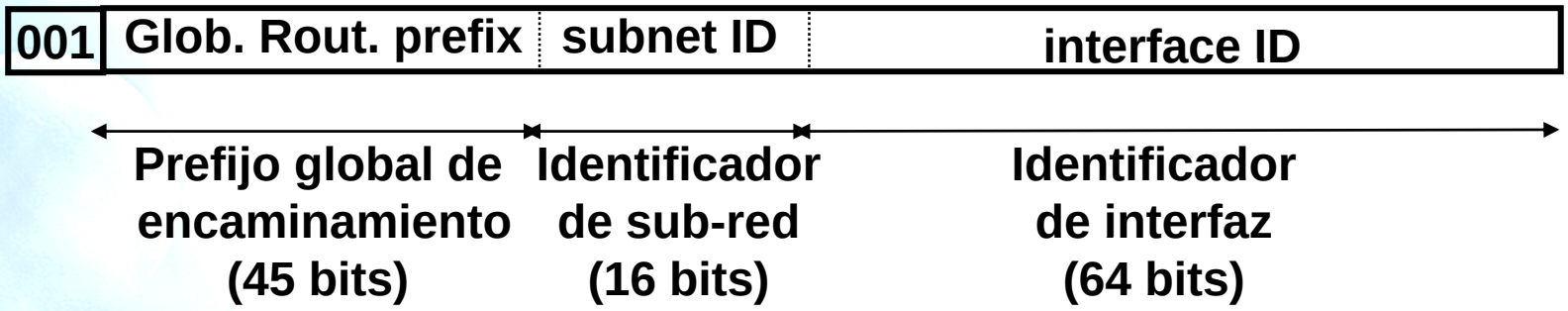
Dirección Global Unicast (RFC3587)



- El prefijo de encaminamiento global es un valor asignado a un zona (site), es decir, a un conjunto de sub-redes/links. Se ha diseñado para ser estructurado jerárquicamente por los RIRs e ISPs
- El ID de sub-red es un identificador de una subred dentro de un site. Se ha diseñado para ser estructurado jerárquicamente por el administrador del site
- El identificador de interfaz se construye normalmente según el formato EUI-64

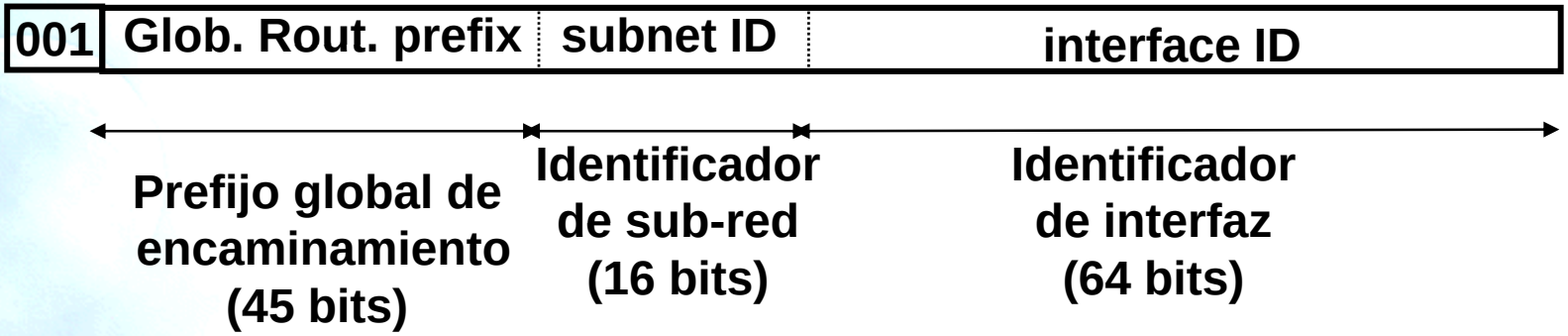
Dirección Global Unicast para 6Bone

(obsoleto desde 06-06-2006) (RFC3701)



- 6Bone: red IPv6 con fines únicamente experimentales
- 1FFE (hex) asignado a 6Bone
  - direcciones 6Bone empiezan con 3FFE:
  - (binario 001 + 1 1111 1111 1110)
- Los siguientes12 bits representan un “pseudo-TLA” (pTLA)
  - cada pseudo-ISP de 6Bone toma un prefijo /24, /28, /32
- No se usa para servicios de producción IPv6

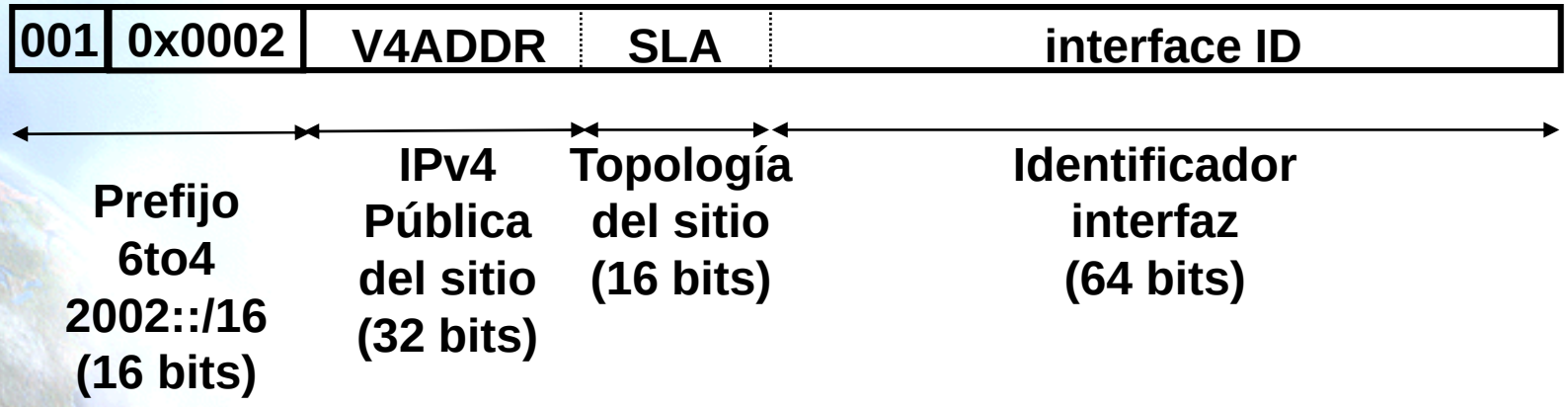
Dirección Global Unicast para Servicios de Producción



- Los ISPs normalmente toman prefijos /32
  - Las direcciones IPv6 de producción empiezan por **2001, 2003, 2400, 2800, etc.**
- Hasta /48 se estructura jerárquicamente por el ISP según el uso interno
- Desde /48 hasta /128 se delega a los usuarios
  - Recomendaciones para la delegación de direcciones (RFC3177)
    - /48 caso general, excepto para abonados grandes
    - /64 si se sabe que una y solo una única red es necesaria
    - /128 si es absolutamente seguro que se va a conectar uno y solo un dispositivo

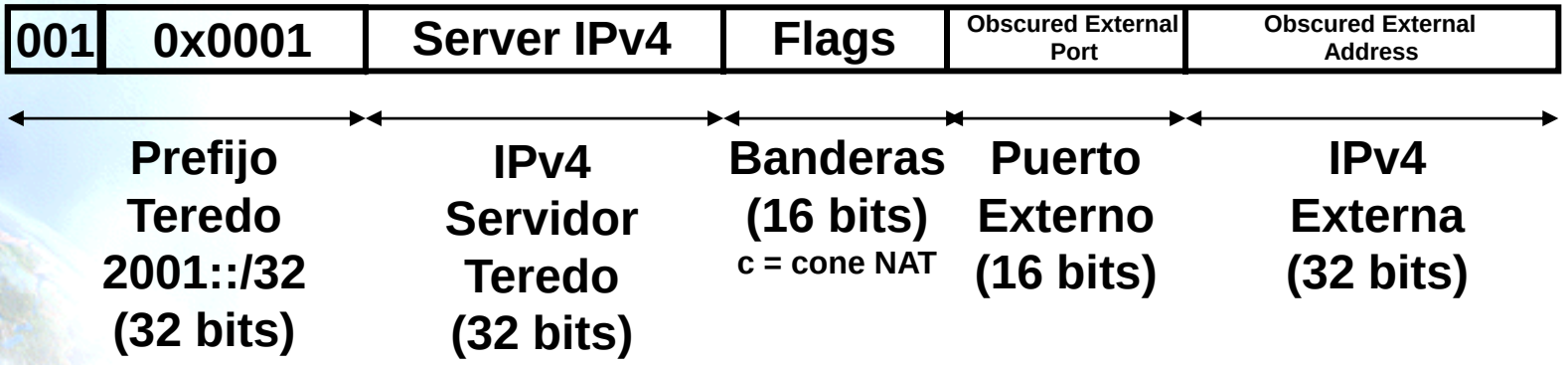
Direcciones 6to4 (RFC3056)

- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- Prefijo asignado **2002::/16**
- Para asignar a los sitios **2002:V4ADDR::/48**



Direcciones Teredo (RFC4380)

- RFC4380: Tunneling IPv6 over UDP through NATs
- Prefijo asignado **2001::/32**
  - **3FFE:831F::/32** Obsoleto



- Puerto 5000 = 0x1388, 0x1388 XOR 0xFFFF = 0xEC77 RFC4380: Tunneling IPv6 over UDP through NATs
- Dirección 131.107.0.1 = 0x836B0001, 0x836B0001 XOR 0xFFFFFFFF = 0x7C94FFFE = 7C94:FFFE

Direcciones Link-Local y Site-Local

Las direcciones **link-local** se usan durante la autoconfiguración de los dispositivos y cuando no existen encaminadores (**FE80::/10**)

1111111010	0	interface ID

Las direcciones **site-local** se usan para tener independencia del ISP y facilitar su cambio. Pueden usarse junto a direcciones globales o en exclusiva si no hay conectividad global (**FEC0::/10**) **(desaprobada en RFC3879)**

1111111011	0	SLA*	interface ID

Dirección Anycast

- Es un identificador de un conjunto de interfaces (normalmente en diferentes nodos).
- Un paquete enviado a una dirección anycast se entregará a una de las interfaces identificadas por esa dirección (la más cercana desde el punto de vista de los protocolos de encaminamiento)

- Se obtienen del espacio de direcciones unicast (de cualquier ámbito) y son **sintacticamente indistiguinguibles de las direcciones unicast.**

- Las direcciones anycast reservadas se definen en el RFC2526

3.3 Direcciones IPv6 Unique Local

Unique Local IPv6 Unicast Addresses - IPv6 ULA (RFC4193)

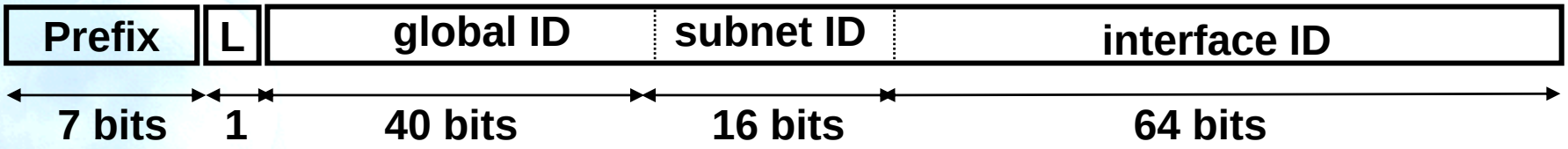
- Prefijo global con alta probabilidad de ser único
- Para comunicaciones locales, normalmente dentro de un “site”
- No son prefijos que vayan a ser encaminados en la Internet Global
- Son prefijos encaminables dentro de un área más limitada, como un determinado “site”
- Incluso podrían ser encaminados entre un conjunto limitado de “sites”
- Direcciones locales localmente asignadas
  - vs direcciones locales centralmente asignadas

Características IPv6 ULA

- Prefijos “bien-conocidos” que facilitan su filtrado en las fronteras de los “sites”
- Son independientes del ISP y se pueden usar para comunicaciones dentro de un “site” que tiene conectividad a Internet intermitente o incluso no tiene
- Si el prefijo se extiende accidentalmente fuera del “site”, vía routing o DNS, no hay ningún conflicto con otras direcciones
- En la práctica, las aplicaciones pues tratar estas direcciones como direcciones de ámbito global

Formato IPv6 ULA

- Formato:



- FC00::/7 Prefijo indicativo de direcciones unicast IPv6 locales
- L = 1 se asigna localmente
- L = 0 Según el RFC4193 puede ser definido en el futuro. En la práctica se usa para especificar asignaciones centrales
- ULA se crea usando una asignación pseudo-aleatorio para el ID global
  - Esto asegura que no hay ninguna relación entre las asignaciones y deja claro que estos prefijos no son para ser encaminados globalmente

ULA Asignadas Centralmente

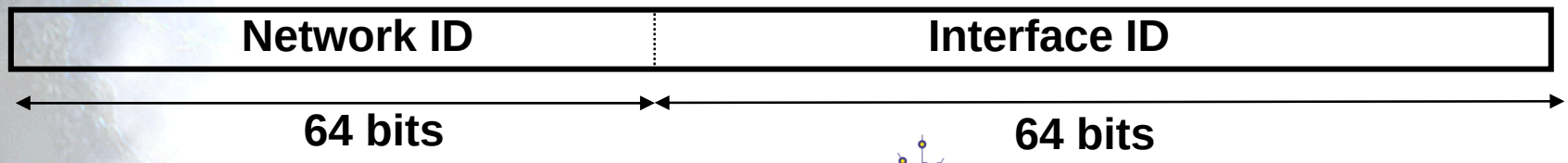
- La principal diferencia entre ambas asignaciones:
  - Las asignadas centralmente son direcciones únicas y la asignación se registra en una base de datos pública (para resolver disputas)
- Recomendación: “sites” que planeen hacer uso de ULA, usen prefijos asignados centralmente para evitar posibilidad de conflicto (no existe obligación, es una recomendación)
- El procedimiento de asignación para crear global-IDs en la asignación centralizada es configurando L=0, mientras que la asignación local es con L=1, según se define en RFC4193
- Más información sobre políticas en RIRs para asignaciones centralizadas
  - http://www.arin.net/meetings/minutes/ARIN_XVIII/ppm2_transcript.html#anchor_3
  - http://www.arin.net/meetings/minutes/ARIN_XIX/ppm1_notes.html

3.4 Identificadores de interfaz

Identificadores de Interfaz

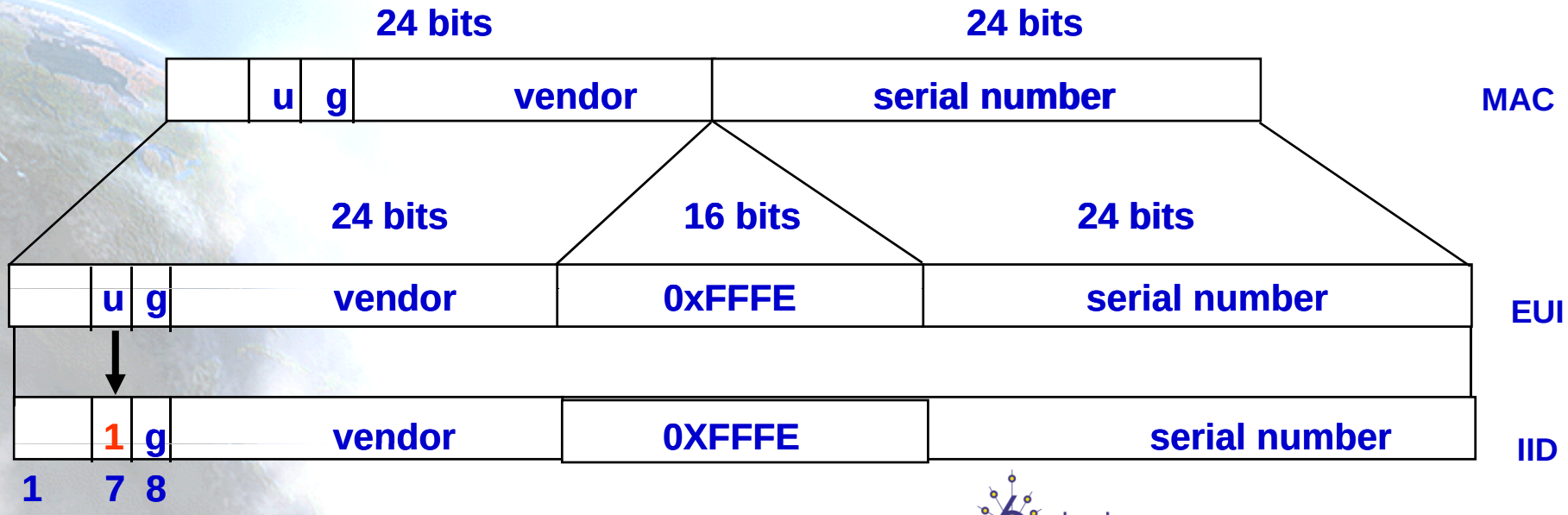
Los 64-bits de menor peso de las direcciones Unicast pueden ser asignados mediante diversos métodos:

- auto-configuradas a partir de una dirección MAC de 64-bit (FireWire)
- auto-configuradas a partir de una dirección MAC de 48-bit (ejemplo, Ethernet), y expandida aun EUI-64 de 64-bits
- asignadas mediante DHCP
- configuradas manualmente
- auto-generadas pseudo-aleatoriamente (protección de la privacidad)
- posibilidad de otros métodos en el futuro



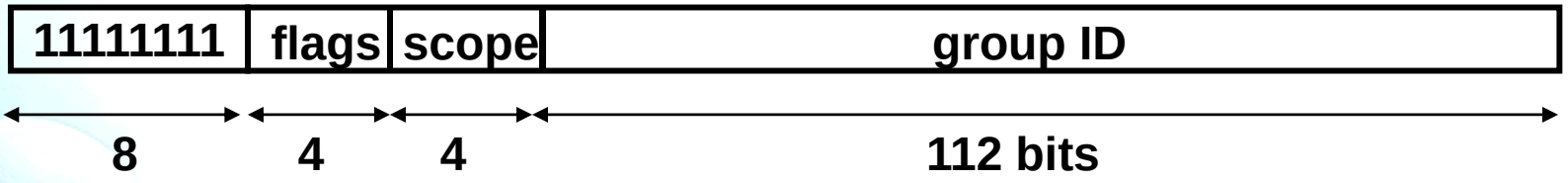
EUI-64

- IEEE define un mecanismo para crear una EUI-64 desde una dirección IEEE 802 MAC (Ethernet, FDDI)
- El IID se obtiene modificando el EUI-64 en el bit u (Universal). Se pone 1 para indicar alcance universal y 0 para indicar alcance local



3.5 Direcciones Multicast

Direcciones Multicast



- Flags: **0RPT**: El flag de más peso está reservado y debe inicializarse a 0
  - T: Asignación Transitoria, o no
  - P: Asignación basada, o no, en un prefijo de red
  - R: Dirección de un Rendezvous Point incrustada, o no
- Scope:
  1 - Interface-Local
  2 - link-local
  4 - admin-local
  5 - site-local
  8 - organization-local
  E - global

(3,F reservados)(6,7,9,A,B,C,D sin asignar)

3.6 Otras consideraciones

Direcciones Obligatorias Nodo IPv6

- Direcciones obligatorias en un Host IPv6:

1. Dirección Link-Local para cada interfaz.
2. Cualquier otra dirección Unicast y Anycast adicional que se haya configurado en las interfaces del nodo (manual o automáticamente).
3. Dirección de loopback.
4. Direcciones multicast de todos-los-nodos (All-Nodes)(FF01::1, FF02::1).
5. Dirección multicast Solicited-Node para cada una de las direcciones unicast y anycast.
6. Direcciones Multicast de todos los grupos a los que el nodo pertenezca.

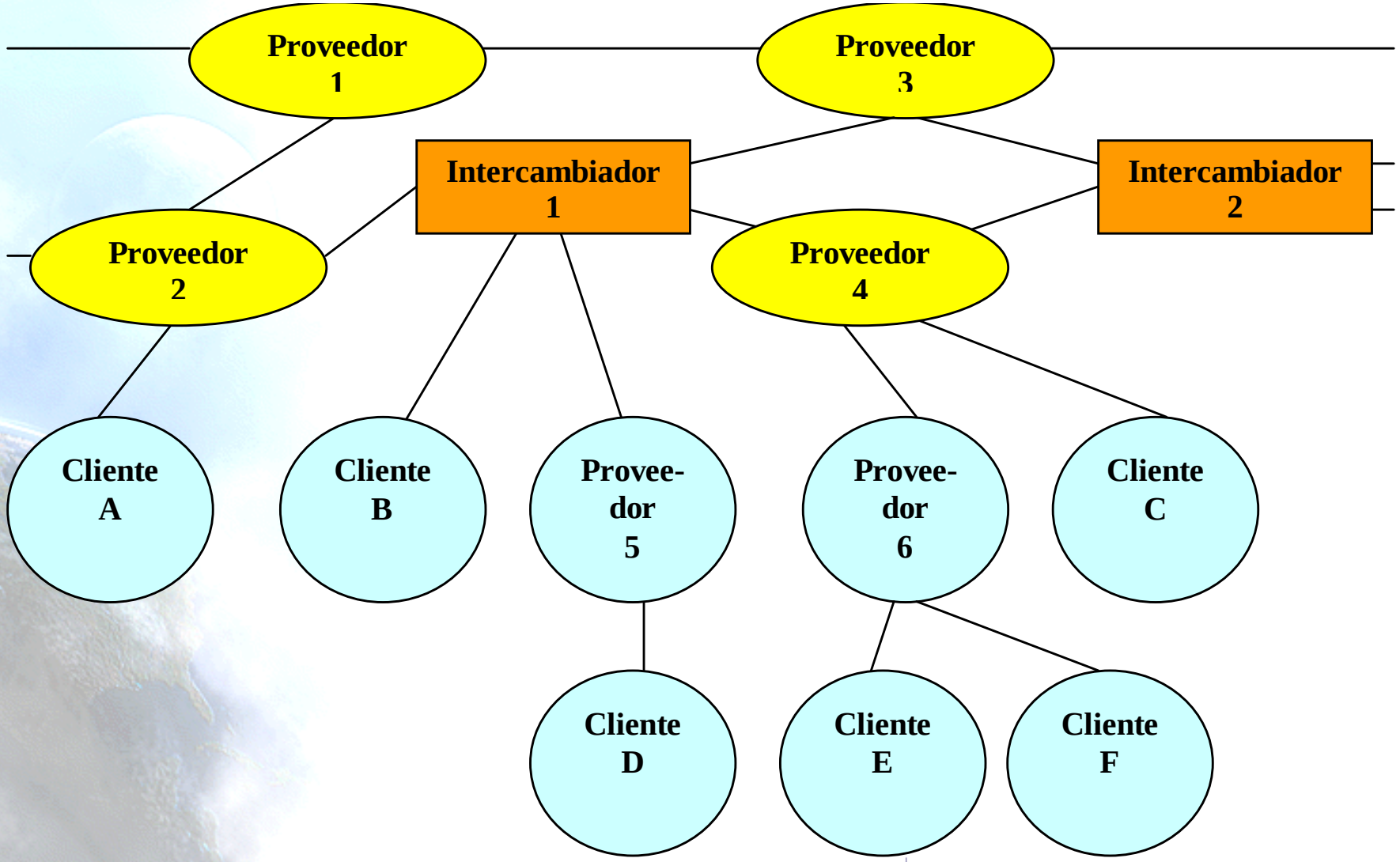
- Direcciones obligatorias en un Router IPv6: Host +:

1. Direcciones Anycast Subnet-Router para todas las interfaces para las que este configurado que se comporte como un router.
2. Todas las demás direcciones Anycast que se hayan configurado en el router.
3. Direcciones multicast All-Routers (FF01::2, FF02::2, FF05::2).

Agregación de Direcciones

- El formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia, intercambiadores, proveedores de niveles inferiores, y Clientes
- A diferencia de lo que ocurre actualmente, los intercambiadores también pueden proporcionar direcciones públicas IPv6
  - Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad, a través del intercambiador, o de uno o varios proveedores de larga distancia
- De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia
  - Fácil cambiar de proveedor sin necesidad de renumerar su organización. Este es uno de los objetivos de IPv6

Esquema de Agregación



Plan de Direccionamiento (1)

- El plan de direccionamiento o numeración tiene como objetivo la asignación de direcciones del espacio de direccionamiento IPv6 asignado por un RIR
  - Dicha asignación es para las diferentes redes y subredes existentes en una red operativa así como las planeadas a futuro
- Para ello se pueden considerar los siguientes criterios (**RFC3177 y tendencias reales**)
  - Todas las redes internas que vayan a desplegar IPv6 tendrán un prefijo /64
    - Necesario para la construcción automática de direcciones IPv6 de tipo Unicast y/o Anycast
  - Los usuarios finales, clientes residenciales (acceso xDSL, FTTx, etc.), como corporativos (empresas, ISPs, Universidad, etc.) podrán recibir prefijos de longitud /48
    - Posibilita crear hasta 2^{16} (65.536) subredes IPv6 de prefijo /64

Plan de Direccionamiento (2)

- La asignación de 65.536 posibles subredes IPv6 de prefijo /64 puede parecer “a priori” excesiva, sin embargo existen varias razones para ello

1. El despliegue futuro de redes NGN facilitará la implementación de servicios nuevos como VoIP, IPTV, etc., cuya distribución puede requerir el uso de redes /64 específicas para cada usuario final
2. Es previsible la llegada en los próximos años de nuevas aplicaciones y/o servicios, aun inimaginables, basadas en domótica, inteligencia ambiental, etc. que requieran un espacio de direccionamiento propio y separado del resto de tráfico, en la red del usuario final
   - Por ejemplo, podría ser necesario tener redes IPv6 /64 exclusivas para conectar electrodomésticos de la cocina, otra red diferente para sensores de presencia ubicados en las habitaciones del usuario, otra red para dispositivos de seguridad como detectores de humo, gas, etc.

Plan de Direccionamiento (3)

- Para numerar enlaces y asignar prefijos de los usuarios existen dos aproximaciones:
  - Usar un pool de direcciones específico para numerar los enlaces nativos IPv6 punto-a-punto o túneles de IPv6 sobre IPv4 entre el CPE del usuario y el router/BRAS del proveedor. Y usar otro pool de direcciones para asignaciones de /48 a los usuarios finales.
    - Este es el método más tradicional.
  - La otra aproximación, que busca facilitar la numeración y asignación, es la de utilizar el primer /64 del prefijo /48 reservado a cada usuario final (GPRS/3G, doméstico, empresa, ISP, etc.) cuando sea necesario numerar el enlace punto-a-punto entre el CPE y el router/BRAS del proveedor (draft-palet-v6ops-point2point). De esta forma se simplifica el coste de operación y se facilita una estructura plana en el espacio de direccionamiento

Plan de Direccionamiento (4)

- Para la elaboración del plan de direccionamiento se deben tener en cuenta las diversas subredes existentes susceptibles de desplegar IPv6 en algún momento, éstas pueden incluir
  - Subredes susceptibles de ser nativas IPv6 desde el primer momento del despliegue de IPv6
  - Subredes susceptibles de ser nativas IPv6 a medio o largo plazo, no necesariamente desde el comienzo del despliegue de IPv6
  - Servicios de transición a IPv6

- El objetivo es tratar de garantizar que no se requerirá modificar la estructura del plan de direccionamiento en el futuro, cuando el despliegue de IPv6 en la red se haga de forma masiva
- Existen dos aproximaciones para la distribución de direcciones: por servicios o geográfica. No son excluyentes.

Plan de Direccionamiento (5)

- Las subredes consideradas en el plan de direccionamiento IPv6 podrían incluir
  - Internet/Encaminamiento Interdominio BGP.
  - Red troncal/Encaminamiento Intradominio OSPF.
  - Red de gestión/supervisión.
  - Servicios básicos de red: DNS, NTP, etc.
  - Web Caches.
  - Intranet Corporativa.
  - Acceso interno (VPNs, etc.).
  - WiFi externa.
  - Enlaces GPRS.
  - Red movilidad.
  - Data Center.
  - Transición IPv6 (túneles, etc.).
  - Clientes finales/ISPs.
  - Usuarios domésticos con acceso RAS.
  - Usuarios domésticos con acceso ADSL-FTTH.
  - Usuarios telefonía GPRS/3G.

Plan de Direccionamiento (6)

- A continuación se presenta un ejemplo de plan de direccionamiento inicial basado en un prefijo /32
- Con este prefijo /32 y los criterios anteriormente descritos se tiene capacidad de proporcionar prefijos /48 a más de 50 000 usuarios de manera simultánea

- Partiendo del prefijo 32 se forman varios grupos diferentes de los 64 posibles prefijos /38 para las diferentes subredes consideradas, atendiendo a los siguientes criterios
  - Grupos de redes que sean independientes de otras
  - Grupos de redes que tengan similitudes en cuanto a su topología
  - Grupos de prefijos /38 libres para proporcionar flexibilidad al plan y posibilitar crecimientos inmediatos

Plan de Direccionamiento (7)

- Un ejemplo típico podría incluir 6 grupos de prefijos /38
  1. Red troncales y redes internas
     - Encaminamiento
     - Servicios básico
     - Redes internas
     - WiFi
     - Enlaces
     - Movilidad
     - Data Center
  2. Túneles
  3. Clientes corporativos e ISPs
  4. Usuarios residenciales (ADSL-FTTH)
  5. GPRS/3G
  6. Prefijos Libres

Plan de Direccionamiento (8)

#	Prefijo	Categoría	Número de prefijos	Longitud prefijos
0	2001:DB8:0000::/38	Encaminamiento, Servicios básico, Redes internas, WiFi, Enlaces, Movilidad, Data Center		
1	2001:DB8:0400::/38	Libre	1	/38
2	2001:DB8:0800::/38	Túneles		
	2001:DB8:0C00::/38 2001:DB8:1000::/38	Libres	2	/38
5	2001:DB8:1400::/38	Clientes corporativos e ISPs	1.024	/48
6	2001:DB8:1800::/38	Clientes corporativos e ISPs	1.024	/48
7	2001:DB8:1C00::/38	Clientes corporativos e ISPs	1.024	/48
	2001:DB8:2000::/38 ... 2001:DB8:3C00::/38	Libres	8	/38
16	2001:DB8:4000::/38	Usuarios ADSL-FTTH	1.024	/48
	Hasta	Usuarios ADSL-FTTH	1.024	/48
35	2001:DB8:8C00::/38	Usuarios ADSL-FTTH	1.024	/48
	2001:DB8:9000::/38 2001:DB8:9400::/38 2001:DB8:9800::/38	Libres	3	/38
39	2001:DB8:9C00::/38	GPRS/3G	67.108.864	/64
	2001:DB8:A000::/38 2001:DB8:A400::/38	Libres	2	/38
42	2001:DB8:A800::/38	GPRS/3G	1.024	/48
	Hasta	GPRS/3G	1.024	/48
61	2001:DB8:F400::/38	GPRS/3G	1.024	/48
	2001:DB8:F800::/38 2001:DB8:FC00::/38	Libres	2	/38
		Total prefijos /38 Libres	18	

4. ICMPv6, Neighbor Discovery y DHCPv6

4.1 ICMPv6
4.2 Neighbor Discovery
4.3 Autoconfiguración
4.4 DHCPv6
4.5 Secure Neighbor Discovery
4.6 Router Renumbering

4.1 ICMPv6

ICMPv6 (RFC4443)

- IPv6 emplea el Internet Control Message Protocol (ICMP) como se define en IPv4 (RFC792)
- Aunque se introducen algunos cambios para IPv6: ICMPv6.
- Valor Next Header = 58.
- Se emplea ICMPv6 en los nodos IPv6 para reportar errores encontrados durante el procesamiento de los paquetes y para realizar otras funciones de la capa de Red, tales como diagnósticos (ICMPv6 "ping").
- ICMPv6 es una parte integral de IPv6 y DEBE ser completamente implementado por cada nodo IPv6.

Mensajes ICMPv6

- Agrupados en dos clases:
  - Mensajes de error
  - Mensajes informativos

bits 8	16	32
Type	Code	Checksum
Message Body		

- Los mensajes de error tienen un cero en el bit de mayor orden del valor del campo Type. Por tanto el valor del campo Type es de 0 a 127.
- Los mensajes informativos tienen valores para el campo Type de 128 a 255.

Determinación de la Dirección Origen del Mensaje

- Un nodo que envía un mensaje ICMPv6 tiene que determinar las direcciones IPv6 origen y destino de la cabecera IPv6 antes de calcular el checksum.
- Si el nodo tiene más de una dirección unicast la dirección origen del mensaje la elige de la siguiente forma:

a) Si el mensaje es como respuesta a un mensaje enviado a una de las direcciones unicast del nodo, entonces Dirección Fuente Respuesta = Misma Dirección

b) Si el mensaje es como respuesta a un mensaje enviado a una dirección multicast o grupo anycast del cual el nodo es miembro, en ese caso Dirección Fuente Respuesta = dirección unicast perteneciente a la interfaz que recibió el paquete multicast o anycast.

c) Si el mensaje es como respuesta a un mensaje enviado a una dirección que no pertenece al nodo, entonces Dirección Fuente = Dirección unicast perteneciente al nodo que sirva de más ayuda en el diagnóstico del error.

d) En cualquier otro caso se debe examinar la tabla de encaminamiento del nodo para determinar que interfaz se va a usar para transmitir el mensaje a su destino, Dirección Fuente = Dirección unicast perteneciente a esa interfaz.

Mensaje ICMP de Error

Type = 0-127	Code	Checksum
Parameter		
El mayor contenido posible del paquete invocado sin que el paquete ICMPv6 resultante exceda de 1280 bytes (mínima Path MTU IPv6)		

Tipos de mensajes de error ICMPv6

- Destino Inalcanzable (tipo = 1, parámetro = 0)
  - No hay ruta al destino (código = 0)
  - Comunicación con el destino prohibida administrativamente (código = 1)
  - Más allá del ámbito de la dirección origen (código = 2)
  - Dirección Inalcanzable (código = 3)
  - Puerto Inalcanzable (código = 4)
  - Dirección origen falló política ingress/egress (código = 5)
  - Ruta a destino rechazada (código = 6)
- Paquete demasiado grande (tipo = 2, código = 0, parámetro = next hop MTU)
- Tiempo Excedido (tipo = 3, parámetro = 0)
  - Límite de saltos excedidos en tránsito (código = 0)
  - Tiempo de reensamblado de fragmentos excedido (código = 1)
- Problemas de parámetros (tipo = 4, parámetro = offset to error)
  - Campo de cabecera erróneo (código = 0)
  - Tipo no reconocido de “Next Header” (código = 1)
  - Opción IPv6 no reconocida (código = 2)

Mensajes ICMP Informativos

- Echo Request (tipo =128, código = 0)
- Echo Reply (tipo = 129, código = 0)

Type = 128-255	Code	Checksum
Maximum Response Delay		Reserved
Multicast Address		

- Mensajes MLD (Multicast Listener Discovery):
  - Query, report, done (como IGMP para IPv4):

4.2 Neighbor Discovery

ND (RFC4861)

- Define el protocolo Neighbor Discovery (ND) (Descubrimiento de Vecinos) en IPv6.
- Los nodos usan ND para determinar la dirección de la capa de enlace de los nodos que se sabe que están en el mismo segmento de red y para purgar rápidamente los valores almacenados inválidos.
- Los hosts también usan ND para encontrar encaminadores vecinos que retransmitirán los paquetes que se les envíen.
- Los nodos usan el protocolo para tener conocimiento de los vecinos que son alcanzables y los que no y para detectar cambios de sus direcciones en la capa de enlace.
- ND habilita el mecanismo de autoconfiguración en IPv6.

Interacción Entre Nodos

- Define el mecanismo para solventar:
  - Descubrimiento de encaminadores
  - Descubrimiento de prefijos de red
  - Descubrimiento de parámetros
  - Autoconfiguración de direcciones
  - Resolución de direcciones
  - Determinación del “Next-Hop”
  - Detección de Vecinos Inalcanzables (NUD).
  - Detección de Direcciones Duplicadas (DAD).
  - Redirección del “First-Hop”.

Nuevos Tipos de Paquetes ICMP

- ND define 5 tipos de paquetes:
  - "Router Solicitation" (RS)
  - "Router Advertisement" (RA)
  - "Neighbor Solicitation" (NS)
  - "Neighbor Advertisement" (NA)
  - "Redirect"

Router Advertisements

- En una red (link) con capacidad broadcast, cada encaminador envía periódicamente paquetes multicast RA.
- Un host recibe los RAs de todos los encaminadores, construyendo una lista de encaminadores por defecto.
- El algoritmo de Neighbor Unreachability Detection (NUD) detecta si existen problemas en alcanzar los encaminadores.
- Los RAs contienen una lista de prefijos usados por los hosts para determinar si una dirección destino de un paquete pertenece a dicho link y para la autoconfiguración de direcciones.
- Los RAs y los 'Flags' asociados a cada prefijo permiten a los encaminadores indicar a los hosts como realizar la autoconfiguración (stateless o DHCPv6).

Comparación con IPv4

- IPv6 ND equivaldría a ARP, ICMP Router Discovery e ICMP Redirect en IPv4, con algunas cosas más (NUD).
- ND supone mejoras en muchos aspectos sobre los protocolos usados en IPv4, entre otras:
  - RAs llevan la dirección de la capa de enlace del encaminador, no es necesario resolverla.
  - RAs llevan los prefijos de un enlace, no es necesario un mecanismo para conocer la máscara de red.
  - RAs permiten la Autoconfiguración de direcciones.
  - REDIRECTS llevan la dirección de la capa de enlace del nuevo 'first hop', no es necesario resolverla.
  - El uso de direcciones de enlace local para identificar a los encaminadores, hace que los hosts 'resistan' una renumeración de la red.
  - Usando un 'Hop Limit' de 255 ND es inmune a mensajes ND de fuera del enlace. En IPv4 podían enviar de fuera Redirects y RAs.

Formato Router Advertisement

Bits 8	16			32
Type = 134	**Code = 0**			**Checksum**
Cur Hop Limit	**M**	**O**	**Reserved = 0**	**Router Lifetime**
Reachable Time				
Retrans Timer				
Options …				

- Cur Hop Limit: valor predeterminado que debería ponerse en el campo Hop Count de la cabecera IPv6 de los paquetes que van a ser enviados
- M: 1-bit "Managed address configuration" flag
- O: 1-bit "Other configuration" flag
- Router Lifetime: entero sin signo de16-bits
- Reachable Time: entero sin signo de 32-bits
- Retrans Timer: entero sin signo de 32-bits
- Possible Options: Source LinkLayer Address, MTU, Prefix Information, Flags Expansion (RFC5175)

Formato Router Solicitation

- Cuando arrancan los hosts envían RSs para indicar a los encaminadores que generen un RA inmediatamente.
- Se envía a la dirección multicast que engloba a todos los encaminadores del segmento de red.

Bits 8	16	32
Type = 133	**Code = 0**	**Checksum**
Reserved = 0		
Options …		

- Opciones Posibles: Source Link-Layer Address.

Formato Neighbor Solicitation

- Los nodos envían NSs para obtener la dirección MAC del nodo con el que se pretende comunicar, a la vez que se proporciona la propia dirección MAC del nodo solicitante.
- Los paquetes NSs son multicast cuando el nodo precisa resolver una dirección y unicast cuando el nodo pretende averiguar si un vecino es alcanzable.

Bits 8	16	32
Type = 135	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Options …		

- Target Address: La dirección IPv6 objetivo de la solicitud. No debe ser una dirección multicast.
- Opciones Posibles : Source Link-Layer Address.

Formato Neighbor Advertisement

- Un nodo envía NAs como respuesta a un NS y envía NAs no solicitados para propagar nueva información rápidamente.

Bits 8	16	32
Type = 136	**Code = 0**	**Checksum**
R | **S** | **O**	**Reserved = 0**	
Target Address		
Options …		

- Flags:
  - **R**: **Router Flag**=1 indica que el que envía en un encaminador.
  - **S**: **Solicited Flag**=1 indica que se envía como respuesta a un NS.
  - **O**: **Override Flag**=1 indica que deben actualizarse las caches.
- Para NA solicitados, igual al campo “Target Address” del NS. Para un NA no solicitado, la dirección cuya MAC ha cambiado. No puede ser una dirección multicast.
- Posibles Opciones: Target Link-Layer Address (MAC del Tx).

Formato Redirect

- Los encaminadores envían paquetes Redirect para informar a un host que existe otro encaminador mejor en el camino hacia el destino final.
- Los hosts pueden ser redireccionados a otro encaminador mejor pero también pueden ser informados mediante un paquete Redirect que el destino es un vecino.

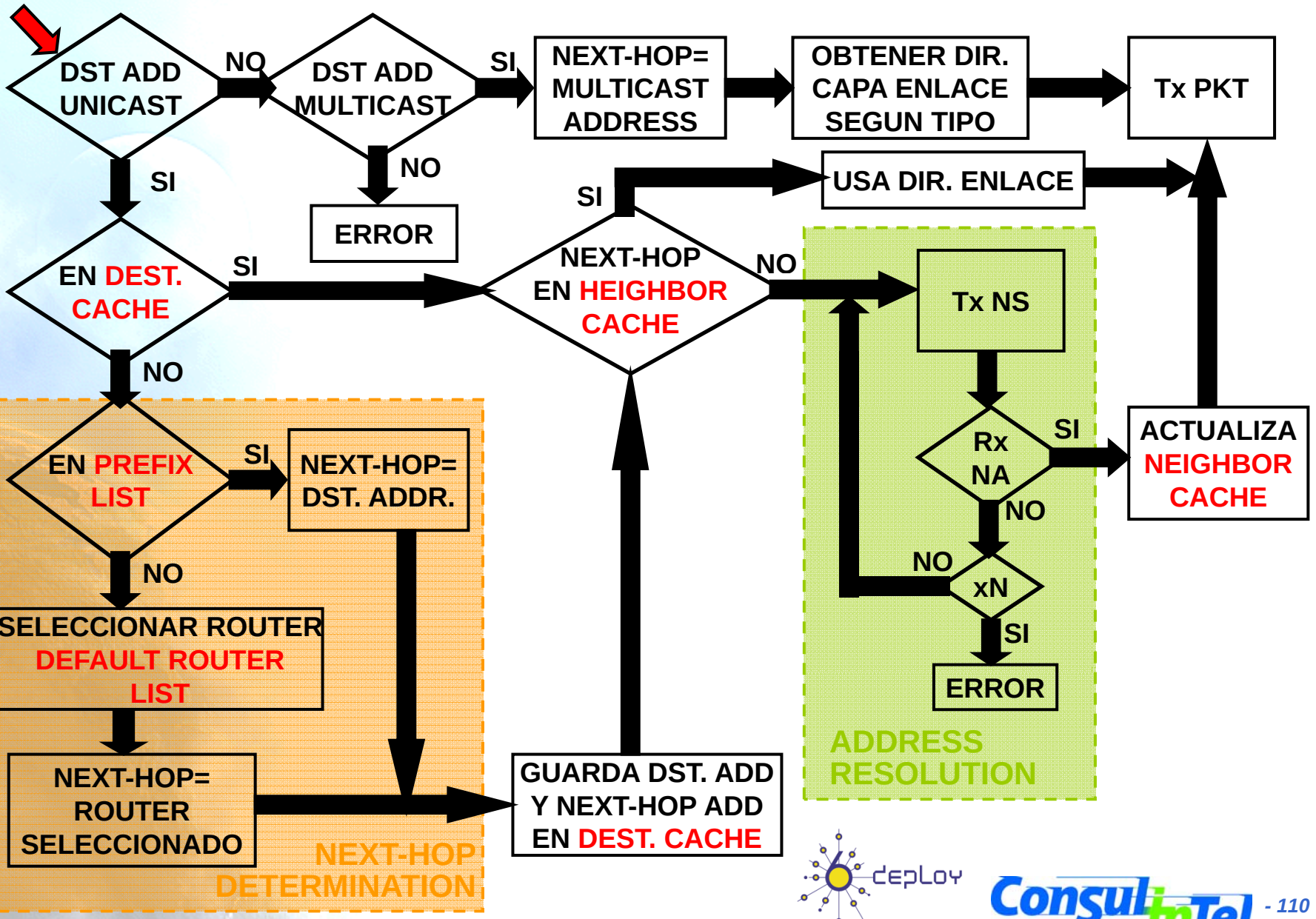
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- Target Address: La dirección IPv6 del ‘first hop’ que es mejor usar para llegar al ‘Destination Address’ del paquete ICMPv6
- Destination Address: La dirección IPv6 de destino que es redireccionada al ‘target address’ del paquete ICMPv6

Ejemplo Funcionamiento (1)

- **Neighbor Cache**: Vecinos a los que se les ha enviado tráfico recientemente. Se indexa por la ‘on-link unicast IP address’. Cada entrada contiene: dir. capa enlace, si es router/host, información de NUD (reachability state, etc.).
- **Destination Cache**: Mapea IP destino con ‘next hop’. Direcciones a las que se ha enviado recientemente.
- **Prefix List**: Contiene los prefijos del enlace. Se basa en los RAs, de donde se saca también el tiempo de validez.
- **Default Router List**: Lista de routers a donde los paquetes ‘off-link’ deben ser enviados. Cada entrada apunta a una entrada en la Neighbor Cache y tiene un tiempo de validez obtenido del RA (router lifetime).

Ejemplo Funcionamiento (2): Envío



Preferencias Encaminador por Defecto y Rutas Más Específicas (RFC4191)

Bits 8	16			32
Type = 134	**Code = 0**			**Checksum**
Cur Hop Limit	**M**	**O**	**H| PRF| Rsvd**	**Router Lifetime**
Reachable Time				
Retrans Timer				
Options …				

- RFC4191 describe una extensión opcional para los RAs para que los encaminadores comuniquen a los hosts preferencias para los encaminadores por defecto y rutas más específicas.
- PRF (Default Router Preference) = 01 Alta
  = 00 Meda (Por defecto)
  = 11 Baja
  = 10 Reservada (NO SE DEBE usar)
- También se define la **Route Information Option**, también con PRF (Route Preference) de 2-bits (entero con signo) (mismos valores).

4.3 Autoconfiguración

Autoconfiguración

- El estándar especifica los pasos que un host debe seguir para decidir cómo auto-configurar sus interfaces de red en IPv6
- El proceso de auto-configuración incluye la creación de una dirección IPv6 de ámbito local (link-local) y la verificación de que no está duplicada en el mismo segmento de red, determinando qué información debería ser auto-configurada y en el caso de direcciones, si estas deberían obtenerse mediante “stateful”, “stateless” o ambos
- IPv6 define tanto un mecanismo de auto-configuración de direcciones de tipo “stateful” como “stateless”
- La auto-configuración “stateless” (SAAC) no precisa de configuración manual en el host, mínima (si acaso alguna) configuración de encaminadores y ningún servidor adicional

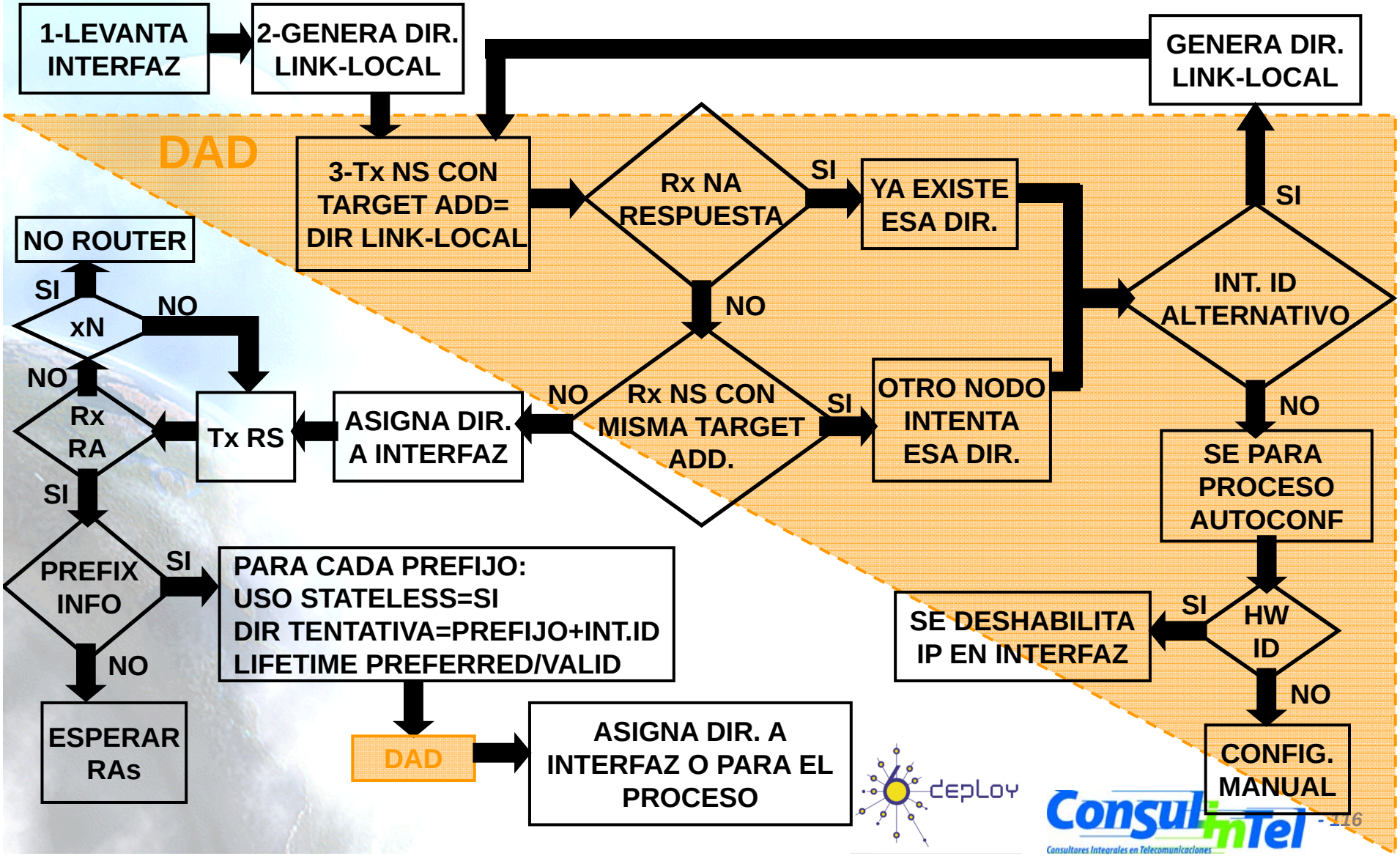
Autoconfiguración Stateless o Serverless (RFC4862)

- El mecanismo “stateless” permite a un host generar su propia dirección usando una combinación de información localmente disponible y de información proporcionada por los encaminadores
- Los **encaminadores anuncian los prefijos de red** que identifican la sub-red asociada a un determinado segmento de red
- Los **hosts generan un identificador de interfaz** que lo identifica de manera única en la subred. Dicho identificador se genera localmente, por ejemplo a partir de la dirección MAC
- Una dirección IPv6 se forma mediante la combinación de ambas informaciones
- En la ausencia de encaminadores, un host puede generar solo las direcciones IPv6 de ámbito local (link-local)
- Las direcciones link-local son suficiente para permitir la comunicación IPv6 entre nodos que están conectados en el mismo segmento de red

Ventajas/Beneficios de la Autoconfiguración Stateless

- La configuración manual de cada máquina antes de conectarla a la red no es necesaria
- Los sitios pequeños compuesto de pocas máquinas conectadas al mismo segmento no necesitarían de un servidor DHCPv6 ni de un encaminador para comunicarse, usarían direcciones link-local
- Un sitio grande con varias subredes no necesitaría de un servidor DHCPv6 para la configuración de direcciones
- Facilita el cambio de prefijo de una sitio mediante el uso de varias direcciones por interfaz y tiempo de vida

Funcionamiento de la Autoconfiguración Stateless



Formato Prefix Information Option

Bits 8	16	24	32		
Type = 3	**Length = 4**	**Prefix Length**	**L**	**A**	**Reserved1 = 0**
Valid Lifetime					
Preferred Lifetime					
Reserved2 = 0					
Prefix					

- **L**(1bit): **on-link flag**=1 indica que el prefijo se puede usar para la determinación ‘en-enlace’.
- **A**(1bit): **autonomous address-configuration flag**=1 indica que este prefijo puede usarse para SAAC.
- **Valid Lifetime**: Tiempo en segs. que el prefijo es valido para determinación ‘en-enlace’. También usado en SAAC.
- **Preferred Lifetime**: Tiempo en segundos que la dirección generada con SAAC permanece como ‘preferred’.
- **Prefix** (128 bits): Dirección IP o prefijo de una dirección.

Autoconfiguración Stateful o DHCPv6 (RFC3315)

- Los hosts obtienen las direcciones de la interfaz de red y/o información de configuración desde un servidor
- Los servidores mantienen una base de datos que actualizan con las direcciones que han sido asignadas y con información de a qué hosts se han asignado
- La auto-configuración “stateless” y la “stateful” se complementan una a la otra
- Ambos tipos de auto-configuración se pueden usar de forma simultánea
- El administrador de red especifica qué tipo de auto-configuración se usa, por medio de la configuración de los campos adecuados de los mensajes RAs

Tiempo de Validez de las Direcciones

- Las direcciones IPv6 se asignan a un interfaz por un tiempo determinado (posiblemente infinito) que indica el periodo de validez de la asignación
- Cuando el tiempo de asignación expira, la asignación ya no es válida y la dirección puede ser reasignada a otra interfaz de red en cualquier otra red dentro de Internet
- Con el fin de gestionar de una manera adecuada la expiración de las direcciones, una dirección pasa por dos fase distintas mientras está asignada a una interfaz.
  - Inicialmente una dirección es la preferida (preferred), lo cual significa que su uso en una comunicación arbitraria no está restringida
  - Más tarde, una dirección se convierte en “deprecada” anticipándose al hecho de que su asignación al interfaz de red será inválido en breve

Detección de Direcciones Duplicadas

- Para asegurarse de que todas las direcciones configuradas son únicas en un determinado segmento de red los nodos ejecutan el algoritmo DAD (Duplicate Address Detection) antes de que la asignación de las direcciones a una interfaz de red sea definitiva
- El algoritmo DAD se realiza para todas las direcciones, independientemente de si se obtienen mediante auto-configuración “stateless” o “stateful”
- El procedimiento para detectar las direcciones duplicadas emplea mensajes NS y NA
- Ya que la auto-configuración de los hosts usa la información anunciada por los encaminadores, estos necesitan ser configurados por algún otro medio. Sin embargo, los encaminadores deben generar las direcciones de ámbito local (link-local) usando el mismo mecanismo
- De este modo los encaminadores también deben pasar adecuadamente el algoritmo de DAD en todas las direcciones antes de asignarlas a sus respectivas interfaces

Configuración DNS usando Autoconfiguración Stateless (1)

- Tradicionalmente la configuración del servidor DNS en los nodos IPv6 se ha hecho por medio de:
  - Configuración manual
  - DHCPv6 o DHCPv4 (en el caso de nodos de Doble Pila)
- Sin embargo esto plantea algunos inconvenientes en ciertos entornos:
  - Necesidad de ejecutar dos protocolos en IPv6 (Auto-configuración Stateless –RA-, DHCPv6)
  - Retardo en la obtención de la dirección del servidor DNS cuando se emplea DHCP
  - Inviabilidad de la configuración manual y/o retardo por DHCP en entornos inalámbricos en los que el nodo cambia de red de manera contínua
- Se puede emplear la configuración DNS basada en RA de forma alternativa para proporcionar la dirección de uno o varios servidores DNS
  - Se emplea una opción específica en el paquete RA
    - Recursive DNS Server (RDNSS)
  - Se puede emplear de forma conjunta con DHCPv6

Configuración DNS usando Autoconfiguración Stateless (2)

- El funcionamiento es el mismo que el que usan los nodos para aprender los encaminadores o el prefijo IPv6 /64 en una red, especificado en RFC4862: IPv6 Stateless Address Autoconfiguration
- Por medio de la opción RDNSS, los nodos aprenden con un solo intercambio de paquetes:
  - Configuración relativa a la red (prefijo /64)
  - Servidores DNS más próximos
- Si además de proporcionar la dirección de los servidores DNS por medio de la opción RDNSS se va a emplear DHCPv6, entonces hay que activar el Flag “O” del paquete RA
- La configuración de la opción RDNSS en los encaminadores se realiza:
  - de forma manual
  - de forma automática mediante DHCPv6 (cliente)

4.4 DHCPv6

DHCPv6 (RFC3315 - RFC4361)

- DHCP para IPv6 (DHCPv6) es un protocolo UDP cliente/servidor diseñado para reducir el coste de la gestión de nodos IPv6 en entornos donde los administradores de red precisan de más control sobre la asignación de direcciones IPv6 y la configuración de los parámetros de red que el ofrecido por la auto-configuración de tipo “stateless”
- DHCPv6 reduce el coste de la asignación de direcciones centralizando la gestión de los recursos de red en vez de distribuir dicha información en ficheros de configuración local entre cada nodo de la red
- DHCPv6 se ha diseñado para ser extendida fácilmente para transportar parámetros nuevos de configuración añadiendo nuevas opciones DHCP definidas para dichas necesidades

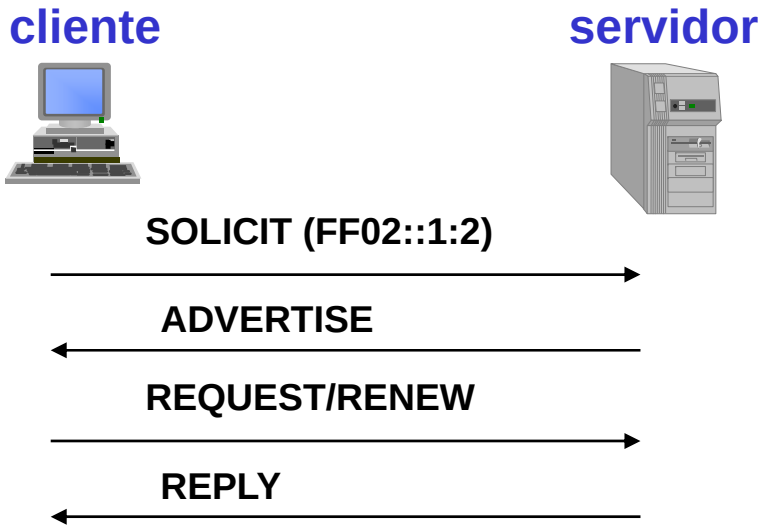
Objetivos de DHCPv6

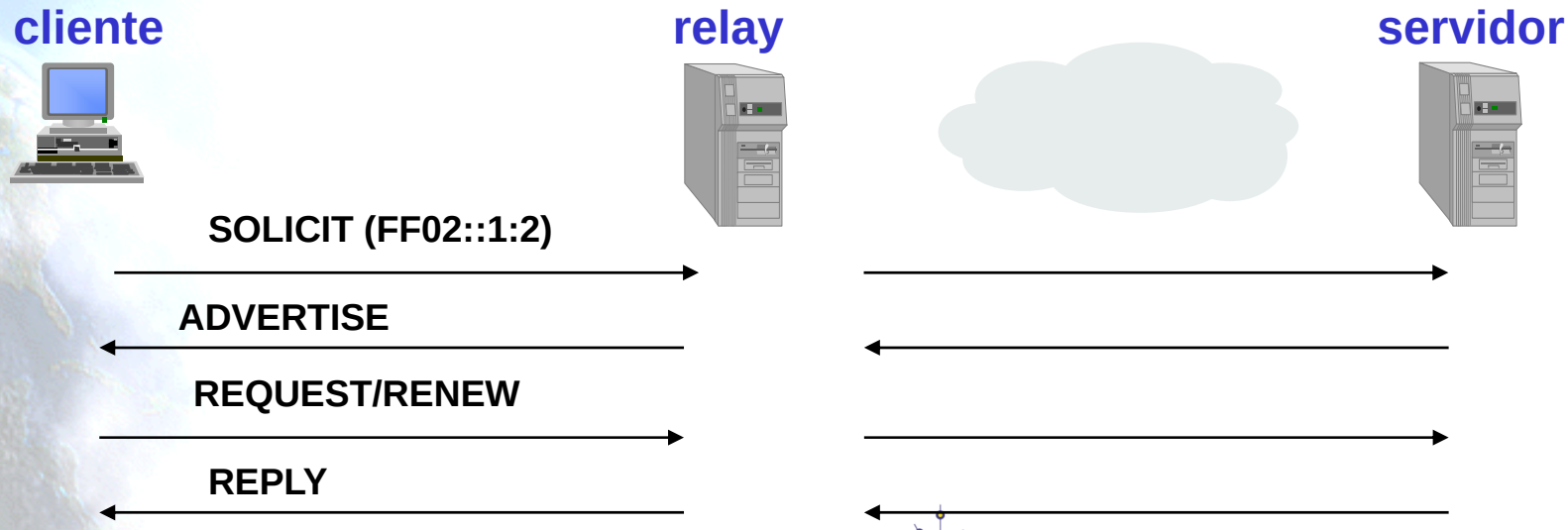
- Es un mecanismo, no una política de asignación
- Es compatible con la auto-configuración IPv6 “stateless”
- No requiere configuración manual de parámetros de red en los clientes DHCP
- No requiere un servidor en cada segmento de red
- Coexiste con nodos configurados estáticamente, nodos no participantes y con otras implementaciones de protocolos de red existentes
- Los clientes DHCP pueden operar en un segmento de red sin que estén presentes encaminadores IPv6
- DHCP proporciona la capacidad de renumeración de las redes
- Un cliente DHCP puede hacer peticiones diferentes y múltiples
- DHCP contiene temporizadores y mecanismos de retransmisión para funcionar de forma eficiente en entornos con alta latencia y bajo ancho de banda

Detalles de DHCPv6

- Los puertos UDP son
  - Clientes escuchan en el 546
  - Servidores y relays escuchan en el 547
- Direcciones para servidores DHCPv6 y relays
  - FF02::1:2 (link local scope)
  - FF05::1:3 (site scope only for servers)
- Mensajes DHCP
  - SOLICIT
  - ADVERTISE
  - REQUES
  - CONFIRM
  - RENEW
  - REBIND
  - REPLY
  - RELEASE
  - DECLINE
  - RECONFIGURE
  - INFORMATION-REQUEST
  - RELAY-FORW
  - RELAY-REPL
- Cada mensaje puede transportar una o más opciones DHCP
  - Domain-list
  - DNS-server
  - IA-NA, etc.
- Identificador Único DHCP (DHCP Unique Identifier, DUID)
  - Los servidores usan DUIDs para identificar a los clientes para la selección de unos determinados parámetros de configuración
  - Los clientes usan los DUIDs para identificar un servidor en aquellos mensajes en los que el servidor necesita ser identificado

Ejemplo Básico de DHCPv6





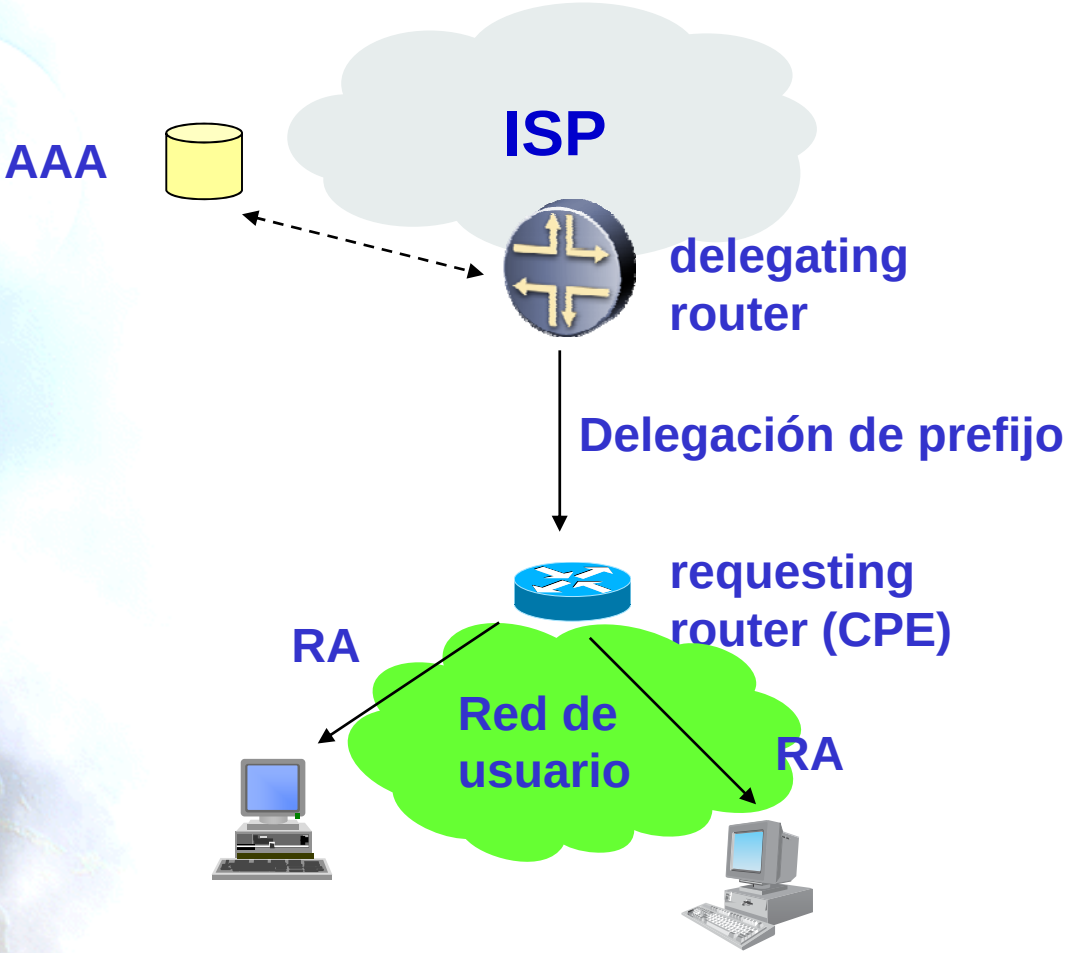
DHCPv6-PD (RFC3633)

- Proporciona a los encaminadores autorizados que lo necesiten un mecanismo automatizado para la delegación de prefijos IPv6
- Los encaminadores que delegan no necesitan tener conocimiento acerca de la topología de red a la que están conectados los encaminadores solicitantes
- Los encaminadores que delegan no necesitan ninguna información aparte de la identidad del encaminador que solicita la delegación de un prefijo
  - un ISP que asigna un prefijo a un CPE que actúa como encaminador

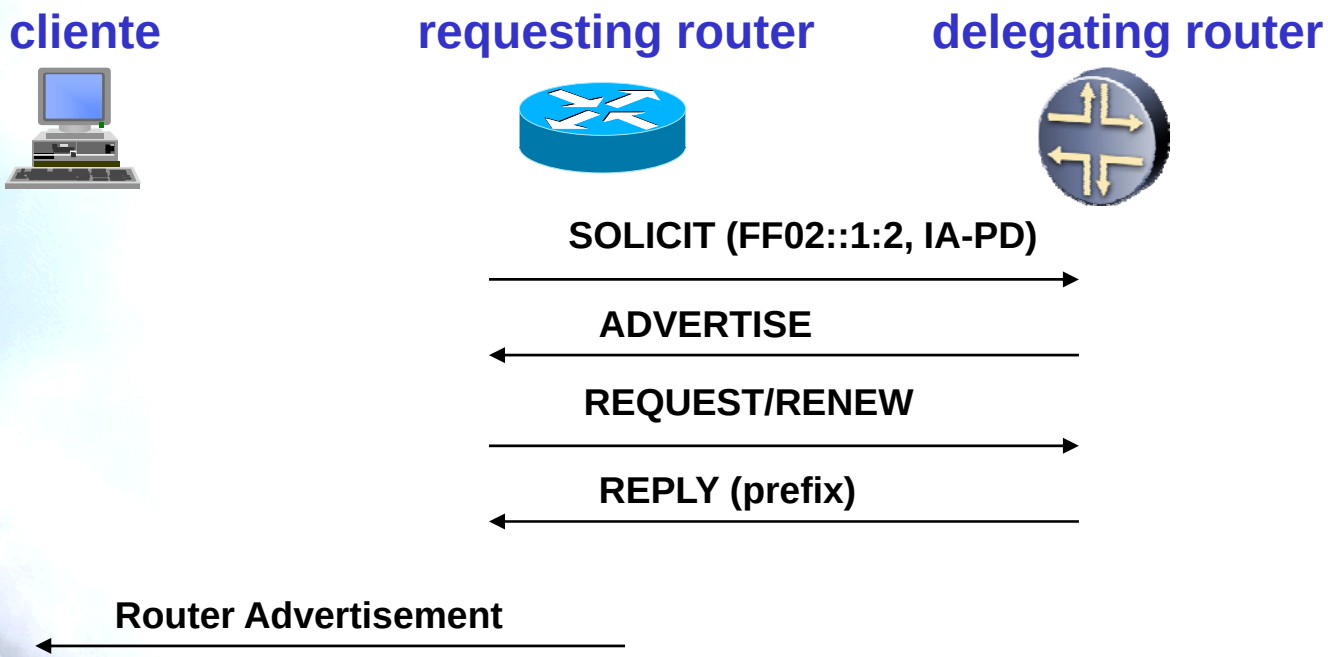
Detalles de DHCPv6-PD

- El encaminador que solicita la delegación (Requesting Router, RR) necesita autenticación
- El perfil de un RR se puede almacenar en un servidor AAA
- El prefijo delegado se puede extraer de:
  - Perfil del cliente almacenado en el servidor AAA
  - Lista de prefijos (prefix pool)
- Los prefijos delegados tienen cierto período de validez, al igual que las direcciones IPv6 en DHCPv6
- Lo que DHCPv6-PD no hace es proporcionar un método para propagar el prefijo delegado a través de la red del usuario
  - Todos los prefijos ::/64 que se pueden extraer de un prefijo delegado se asignan en el RR de acuerdo a las políticas que tengan configuradas
- Se pueden usar los DHCPv6 relays en DHPv6-PD de igual forma que en DHCPv6

Arquitectura de Red para DHCPv6-PD



Ejemplo Básico de DHCPv6-PD



Nuevas Características de Usuario con DHCPv6

- Configuración de actualizaciones dinámicas de servidores DNS
- Deprecación de direcciones para la renumeración dinámica
- Los “relays” se pueden configurar con direcciones de servidor o usar multicast
- Autenticación
- Los clientes pueden pedir múltiples direcciones IPv6
- Las direcciones pueden ser reclamadas usando mensajes “Reconfigure-init”
- Integración entre auto-configuración de tipo “stateful” y “stateless”
- Habilitando “relays” para localizar servidores no alcanzables

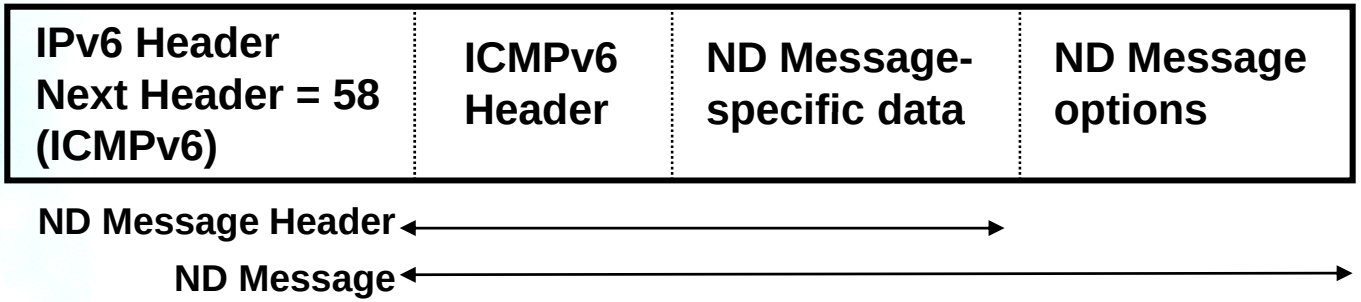
4.5 Secure Neighbor Discovery

Secure Neighbor Discovery - SEND (RFC3971)

- Los nodos IPv6 usan NDP (Neighbor Discovery Protocol) para:
  - Descubrir otros nodos en el segmento de red o enlace
  - Determinar su dirección de nivel de enlace
  - Mantener información para saber si los vecinos siguen activos
- NDP es vulnerable a varios ataques si no se asegura
- El RFC3971 especifica ciertos mecanismos de seguridad para NDP
  - Estos mecanismos no usan IPSec, a diferencia de las especificaciones originales de NDP
  - SEND se aplica en entornos donde la seguridad física del enlace no está asegurado (como por ejemplo redes inalámbricas)
- De momento solo hay implementaciones de SEND para linux y *BSD
  - P.e. http://www.docomolabs-usa.com/lab_opensource.html

Elementos de SEND

- Un mensaje NDP sigue el mismo formato que los mensajes ICMPv6
- Un mensaje NDP real incluye:
  - Cabecera del mensaje NDP
    - Cabecera ICMPv6
    - Datos específicos del mensaje ND
  - y cero o más opciones NDP, las cuales siguen el formato “Type-Length-Value”



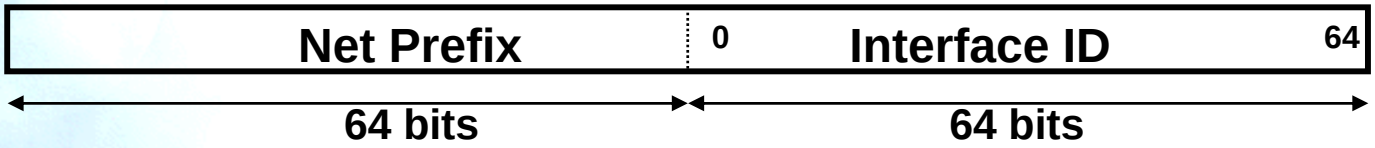
- Se definen una serie de nuevas opciones ND para asegurar NDP y proteger sus mensajes
- El RFC3971 introduce
  - Opciones de SEND para Neighbor Discovery
  - Un proceso de descubrimiento de delegación de autorización
  - Un mecanismo para probar la propiedad de una dirección
  - Y los requisitos para el uso de estos componentes en NDP

Funcionamiento de SEND y CGAs

- SEND se basa en el uso de CGAs (Cryptographically Generated Addresses)
- Una CGA es una dirección IPv6 que se ha formado con un mecanismo especial definido en RFC3972
  - El RFC3972 describe un método para ligar una clave pública a una dirección IPv6 en el contexto de SEND
  - Para ello, se genera un par de claves pública-privada en el nodo que usa SEND
  - Partiendo de un ID de interfaz, una clave pública y de ciertos parámetros auxiliares, se construye un nuevo ID de interfaz mediante una función hash criptográfica univoca
  - Las CGAs son direcciones IPv6 para las que el ID de interfaz se genera por medio de dicho método
  - La relación entre la clave pública y la dirección se puede verificar re-calculando el valor hash y comparándolo con el ID de interfaz
  - La protección así definida funciona sin necesidad de una autoridad certificadores ni una infraestructura de seguridad añadida
  - Los nodos que usen SEND DEBEN usar CGAs
- La autenticidad del nodo que use una CGA viene dada por la acción conjunta de
  - El uso de su clave publica para generar la CGA
  - La firma del mensaje con su clave privada

Formato de CGAs IPv6

- RFC3972 considera
  - Dirección IPv6: leftmost 64 bits = subnet prefix, rightmost 64 bits = ID de interfaz
  - Los bits ID de interfaz se numeran empezando desde el bit cero que está a la izquierda
  - Una CGA tiene un parámetro de seguridad (Sec) que determina su fortaleza frente a ataques de fuerza bruta
    - Sec es un parámetro entero sin singo de 3 bits codificado en los tres bits mas a la izquierda del ID de interfaz (bits 0 - 2)
    - Sec = (ID de interfaz & 0xe000000000000000) >> 61



- La CGA se asocia a una serie de parámetros que consisten en una clave pública y parámetros auxiliares
  - Se calculan dos valores hash a partir de esos parámetros: Hash1 (64 bits) y Hash2 (112 bits)
- La CGA satisface las dos condiciones siguientes:
  - El valor hash1 es igual al ID de interfaz de la dirección. Los bits 0, 1, 2, 6 y (parámetro Sec y bits “u” y “g” del formato de una dirección IPv6 estándar) se ignoran en la comparación
  - Los 16*Sec bits de la izquierda del segundo valor hash (Hash2) son cero
  - La definición anterior se puede establecer en los términos de las dos máscaras siguientes :
    Mask1 (64 bits) = 0x1cffffffffffffff
    Mask2 (112 bits) = 0x00000000000000000000000000 if Sec=0,
    0xffff0000000000000000000000 if Sec=1,
    0xffffffff00000000000000000000 if Sec=2,
    0xffffffffffff000000000000000000 if Sec=3,
    0xffffffffffffffff0000000000000000 if Sec=4,
    0xffffffffffffffffff00000000 if Sec=5,
    0xffffffffffffffffffffff0000 if Sec=6, y
    0xffffffffffffffffffffffffff if Sec=7

- Luego una CGA es un dirección IPv6 para las que se cumplen las dos ecuaciones siguientes:
  Hash1 & Mask1 == ID de interfaz & Mask1
  Hash2 & Mask2 == 0x00000000000000000000000000

Opciones de SEND para Neighbor Discovery (1)

- La opción CGA (Cryptographically Generated Addresses) para transportar la clave pública y los parámetros asociados necesarios para verificar que la CGA es correcta
  - Si el nodo usa SEND, la opción CGA es obligatoria y asegura que el remitente de un mensaje ND es el propietario de la dirección que dice tener
  - Un par de claves publica-privada deben generarse por todos los nodos antes de poder reclamar una dirección
  - El RFC3971 también permite a un nodo usar direcciones que no son CGA, sino que son aseguradas por medio de certificados, aunque los detalles en este caso quedan fuera de la especificación
- Formato:

Bits 8	Bits 16	24	32
Type = 11	**Length**	**Pad Length**	**Reserved**
CGA Parameters			
Padding			

Opciones de SEND para Neighbor Discovery (2)

- La opción de firma RSA (RSA Encryption Standard) se usa para proteger todos los mensaje relacionados con ND y RD
  - Las firmas con claves privada protegen la integridad de los mensajes y autentican la identidad del remitente
  - Esta opción permite añadir una firma RSA al mensaje NDP
  - Es sólo opcional, pero recomendable para verificar la autenticdad del remitente

- Formato:

Bits 8	Bits 16	32
Type = 12	**Length**	**Reserved**
Key Hash (128-bit)		
Digital Signature (PKCS#1 v1.5 signature)		
Padding		

Opciones de SEND para Neighbor Discovery (3)

- Las opciones “Timestamp” y “Nonce” sirven para prevenir ataques de réplica
  - La opción “Timestamp” ofrece protección frente a reenvío de paquetes aprendidos (ataque de réplica) sin necesidad de usar números de secuencia ni establecimiento de estados. Sirve de gran utilidad por ejemplo, para mensajes ND y RD enviados a direcciones multicast
  - La opción “Nonce” protege los pares de mensajes de solicitación y anuncio de vecinos
    - El “nonce” es un número aleatorio o pseudo-aleatorio impredecible y generado y usado solo una vez por un nodo. En SEND estos números se usan para asegura que un anuncio particular se refiere a la solicitud que lo ha generado

Proceso de “Authorization Delegation Discovery” (1)

- Planteamiento del problema
  - NDP permite a un nodo autoconfigurarse basándose en la información recibida de la red
  - Es muy fácil configurar un nodo como encaminador “maligno” en un enlace de red que no sea seguro y por contra muy difícil para el nodo recién conectado distinguir entre fuentes de información de red válidas o inválidas
    - El nodo necesita precisamente esa información para poder comunicar
  - Puesto que el nodo recién conectado no se puede comunicar con otros nodos fuera del link, no puede ser responsable de buscar información que le ayude a validar al encaminador que le envía información sobre la red
  - Sin embargo, si existe un “certification path” el nodo puede concluir que un determinado encaminador es una fuente autorizada o no
  - In the typical case, a router already connected beyond the link can communicate if necessary with off-link nodes and construct a certification path
- Certification path
  - SEND hace obligatorio el uso de
    - Un formato para el certificado
    - Dos nuevos mensajes ICMPv6 usados entre nodos y encaminadores
  - Ambas cosas permite que el nodo conozca el camino de certificación con la ayuda del encaminador

Proceso de “Authorization Delegation Discovery” (2)

- Modelo para la autorización
  - Para proteger el RD, SEND requiere que los encaminadores sean autorizados a actuar como tal
  - Esta información se proporciona tanto a los encaminadores como a los nodos
  - Una autoridad de confianza proporciona certificados a los encaminadores y a los nodos se les configura esa autoridad de confianza para autorizar a los encaminadores
  - Este modelo es específico de SEND y no asume que los certificados que ya estén desplegados para otros propósitos sean usados para SEND
- La autorización para los encaminadores es doble:
  - Los encaminadores son autorizados a actuar como encaminadores
    - Solo si el encaminador pertenece al conjunto de encaminadores autorizados por la autoridad de confianza
  - Opcionalmente, a los encaminadores también se les puede autorizar a anunciar un conjunto de prefijos de red
    - A un encaminador específico se le autoriza a anunciar un determinado conjunto de prefijos mientras que a otros encaminadores se les autoriza a anunciar un conjunto de prefijos diferente

Formato del Certificado (1)

- El camino de certificación de un encaminador acaba en un Certificado de Autorización de Encaminador el cual autoriza a un nodo IPv6 específico a actual como encaminador
  - Dado que los caminos de autorización no son muy comunes en la práctica en Internet, el camino DEBE estar compuesto de Certificados de Clave Pública estándar (Public Key Certificates, PKC)
  - El camino de certificación DEBE comenzar en la autoridad de confianza compartida entre el nodo y el encaminador.
  - Una autoridad de confianza puede emitir multitud de certificados
- Certificado de Autorización de Encaminador
  - Son certificados X.509v3 (RFC3280)
  - DEBEN incluir al menos una instancia de una extensión X.509 para direcciones IP (RFC3779)

Formato del Certificado (2)

- Ejemplo de camino de certificación
  - Supongamos que isp_group_example.net es la autoridad de confianza. El nodo tendrá el siguiente certificado:

```
Certificate 1:
  Issuer: isp_group_example.net
  Validity: Jan 1, 2004 through Dec 31, 2004
  Subject: isp_group_example.net
  Extensions:
    IP address delegation extension:
       Prefixes: P1, ..., Pk
    ... possibly other extensions ...
  ... other certificate parameters ...
```

  - Cuando un nodo se conecta a la red servida por router_x.isp_foo_example.net, recibe el siguiente camino de certificación:

```
Certificate 2:
  Issuer: isp_group_example.net
  Validity: Jan 1, 2004 through Dec 31, 2004
  Subject: isp_foo_example.net
  Extensions:
    IP address delegation extension:
      Prefixes: Q1, ..., Qk
    ... possibly other extensions ...
  ... other certificate parameters ...

Certificate 3:
  Issuer: isp_foo_example.net
  Validity: Jan 1, 2004 through Dec 31, 2004
  Subject: router_x.isp_foo_example.net
  Extensions:
    IP address delegation extension:
      Prefixes R1, ..., Rk
    ... possibly other extensions ...

  ... other certificate parameters ...
```

4.6 Router Renumbering

Router Renumbering (RFC2894)

- ND y la auto-configuración de direcciones IPv6 hacen la asignación inicial de los prefijos y de las direcciones de red a los diversos hosts
- Gracias a estos dos mecanismos, el procedimiento de reconfiguración de hosts es extremadamente sencillo cuando los prefijos de una red cambian
- El mecanismo de renumeración de encaminadores (Router Renumbering, "RR“) permite configurar y reconfigurar los prefijos de direcciones en los encaminadores tan fácilmente como funciona la combinación de ND y la auto-configuración de direcciones en los hosts
- Proporciona un medio para que el administrador de la red haga actualizaciones en los prefijos usados y que se anuncian por medio de los encaminadores IPv6 a toda una red

Funcionamiento

- Los paquetes “Router Renumbering Command” contiene una secuencia de operaciones de control de prefijos (Prefix Control Operations, PCO)
- Cada PCO especifica una operación, un prefijo-plantilla y cero o más prefijos de uso
- Un encaminador procesa cada PCO, comprobando cada una de sus interfaces para una dirección o prefijo que concuerda con el prefijo-plantilla
- Se aplica a cada interfaz en la que el prefijo-plantilla concuerda
- La operación puede ser: ADD, CHANGE, o SET-GLOBAL para respectivamente instar al encaminador a añadir un prefijo de uso, para configurar prefijos, quitar un prefijo y reemplazarlo con el prefijo de uso, o reemplazar todos los prefijos de ámbito global con los prefijos de uso

5. Seguridad IPv6

5.1 Introducción
5.2 IPsec: La teoría
5.3 Extensiones de Privacidad
5.4 Amenazas a ND
5.5 Comparativa IPv4 vs. IPv6
5.6 Aspectos de seguridad con IPv6
5.7 Temas prácticos
5.8 Firewalling
5.9 Modelo de Seguridad Distribuida

5.1 Introducción

Introducción

- Aunque el término Seguridad abarque gran cantidad de temas, en esta sección se abordarán solamente los relacionados con IPv6
- En primer lugar se dará una descripción de IPsec debido a que es obligatoria su implementación en todas las pilas IPv6, proporcionando la posibilidad de su uso a todos los dispositivos IPv6.
- A continuación se tratarán algunas soluciones de seguridad concretas desarrolladas en el contexto de IPv6: Extensiones de Privacidad y SEND.
- Se compararán IPv6 e IPv4 desde el punto de vista de las amenazas a la seguridad.
- Se expondrá un análisis general desde el punto de vista práctico, comparando elementos de seguridad IPv4 e IPv6.
- Por último se introducirá el concepto de Seguridad Distribuida.

5.2 IPsec: La teoría

Seguridad IP (IPsec)

- **Objetivos**:
  - Proporcionar seguridad criptográfica, de calidad e interoperable para IPv4 e IPv6.
  - No afectar negativamente a usuarios, hosts u otros componentes de Internet que no usen IPsec para la protección del tráfico.
  - Los protocolos de seguridad (AH, ESP e IKE) se han diseñado para ser independientes de los algoritmos de cifrado usados. Se define un conjunto de algoritmos por defecto.
- **Conjunto de Servicios de Seguridad**:
  - Control de Acceso
  - Integridad sin-conexión
  - Autentificación del origen de los datos
  - Protección contra reactuación (un tipo de integridad de secuencia parcial)
  - Confidencialidad (cifrado)
  - Confidencialidad de flujo de tráfico limitado

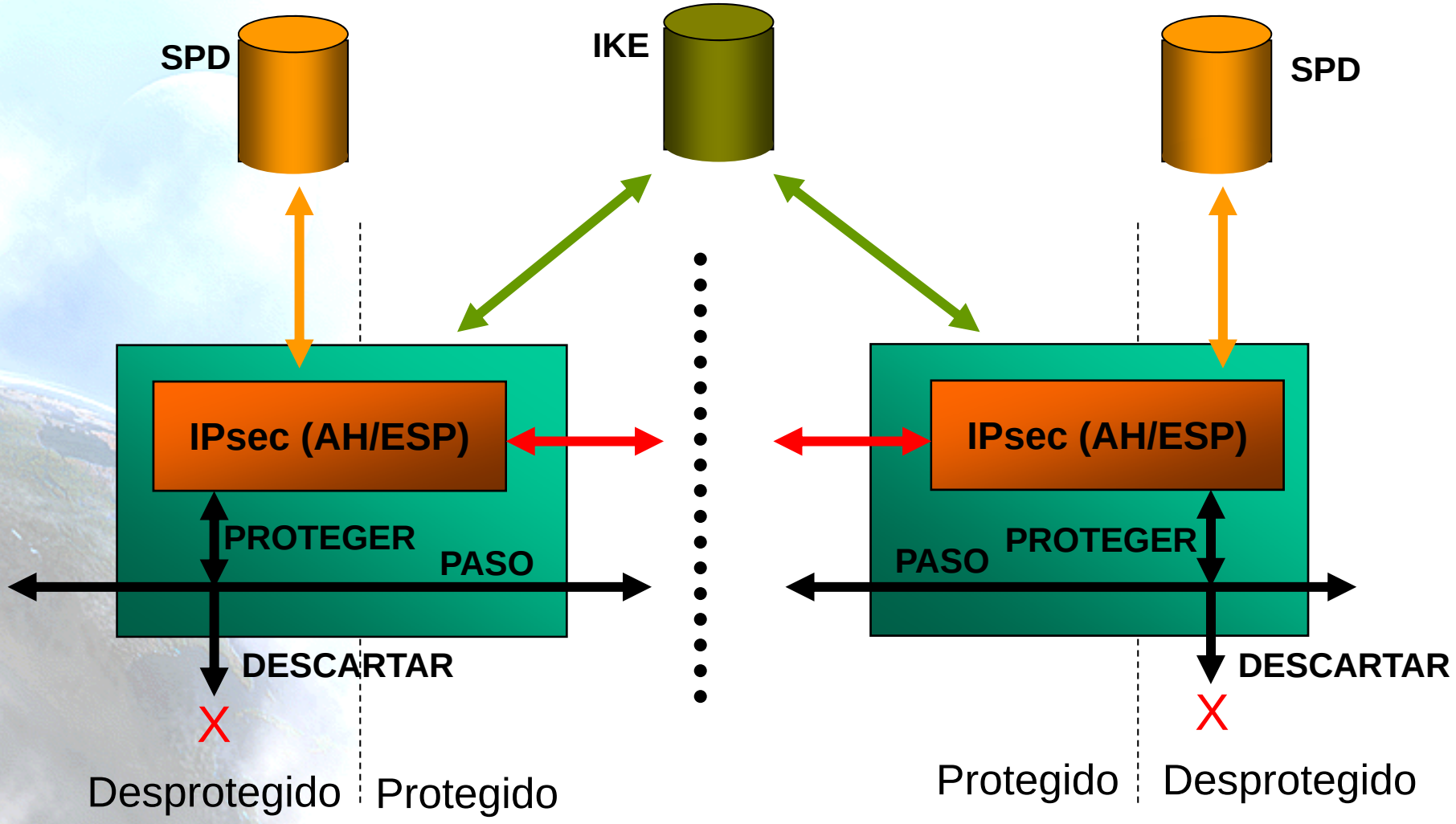
IPsec: Elementos Básicos

- Elementos básicos:
  - **Arquitectura Base** para sistemas conformes con IPsec (RFC4301)
  - **Protocolos de Seguridad:** Authentication Header (AH) (RFC4302) y Encapsulating Security Payload (ESP) (RFC4303)
  - **Asociaciones de Seguridad:** Qué son y como funcionan, cómo se gestionan (RFC4301)
  - **Gestión de Claves**: Manual y Automática (La Internet Key Exchange IKE) (RFC4306)
  - **Algoritmos para autentificación y cifrado**: Se definen algoritmos obligatorios, por defecto, para su uso con AH y ESP (RFC4835) y para IKEv2 (RFC4307)

Visión General (1)

- Una implementación IPsec opera en un host, como una pasarela de seguridad (SG) o como un dispositivo independiente.
- La protección ofrecida por IPsec se basa en los requerimientos definidos en la Security Policy Database (SPD).
- Los paquetes se clasifican basándose en información de las cabeceras IP y 'next layer', para buscar coincidencias en la SPD.
- Cada paquete puede ser DESCARTADO, PROTEGIDO usando los servicios IPsec o permitirse su PASO a través de la protección IPsec.
- IPsec se puede usar para proteger uno o más "caminos":
  - Entre un par de hosts.
  - Entre un par de pasarelas de seguridad.
  - Entre una pasarela de seguridad y un host.

Visión General (2)



PAD (Peer Authorization Database)

- La PAD proporciona un enlace entre la SPD y un protocolo de gestión de asociaciones de seguridad como IKE. Se encarga de varias funciones críticas:
  - Identificar peers o grupos de peers que están autorizados a comunicarse con la entidad IPsec.
  - Especifica el protocolo y el método usado para autentificar cada peer.
  - Proporciona los datos de autentificación para cada peer.
  - Limita los tipos y valores de IDs que puede usar un peer para crear una SA 'hijo', asegurando así que no use identidades, que se busquen en la SPD, que no esta autorizado a usar cuando se crea una SA hijo.
  - Información de localización de pasarela de un peer, e.g., dirección(es) IP o nombres DNS, PUEDEN incluirse para peers que se sabe están "detrás" de una pasarela de seguridad.

Protocolos de Seguridad

- Las implementaciones IPsec DEBEN soportar ESP y PUEDEN soportar AH. AH y ESP pueden aplicarse solas o en combinación con la otra.
- **AH** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
- **ESP** proporciona:
  - Integridad.
  - Autentificación del origen de los datos.
  - Opcionalmente (según criterio del receptor) servicio anti-reactuación.
  - Confidencialidad (NO recomendada sin integridad).
- Ambas ofrecen control de acceso, impuesta a través de la distribución de claves criptográficas y la gestión de flujos de tráfico según dicte la SPD.
- Estos mecanismos están diseñados para ser independientes de los algoritmos.

SA: El Concepto

- La Asociación de Seguridad (Security Association - SA) es un concepto fundamental para IPsec:
  - **Una “conexión” simple que proporciona servicios de seguridad al tráfico que transporta.**
- AH y ESP usan SAs, de forma que todas las implementaciones DEBEN soportar el concepto de Asociación de Seguridad.
- Una de las principales funciones de IKE es el establecimiento y mantenimiento de SAs.
- Para asegurar un comunicación bidireccional típica entre dos nodos con IPsec, se necesitan dos SAs (una para cada dirección). IKE crea pares de SAs.

Identificación de SA

- Cada SA se identifica unívocamente por la terna:
  - Índice de Parámetros de Seguridad (Security Parameter Index - SPI)
    - Cadena de bits asignada a la SA (significado local), como puntero a una base de datos de SAs (SPD o Security Policy Database).
  - Dirección IP Destino
  - Identificador de protocolo de seguridad (AH o ESP)
- La dirección destino puede ser:
  - Dirección Unicast
  - Dirección Broadcast
  - Dirección Grupo Multicast

SA Database (SAD)

- En cada implementación IPsec existe una base de datos de SAs (SAD, Security Association Database).
- Cada entrada define los parámetros asociados con una SA.
- Cada SA tiene una entrada en la SAD.
- La SPD tiene punteros a entradas en la SAD, cuando se tiene que usar IPsec (PROTEGER).

Campos de la SAD (1)

- **Security Parameter Index (SPI):** Un valor de 32 bits seleccionado por el extremo receptor de una SA para identificar unívocamente la SA.
- **Sequence Number Counter:** Un contador de 64 bits usado para generar el número de secuencia transmitido en las cabeceras AH y ESP (los números de secuencia de 64 bits se usan por defecto, pero lo de 32 bitstambién se soportan si se negocian previamente).
- **Sequence Counter Overflow:** Un flag que indica si el desbordamiento del contador de número de secuencia debe generar un evento auditable y evitar el envío de más paquetes por la SA, o si se permite el reinicio del contador.
- **Anti-Replay Window:** Un contador de 64 bits y un bit-map (o equivalente) usado para determinar si un paquete AH o ESP de entrada es un reenvío.
- **AH Information:** Algoritmos de autentificación, claves, tiempos de vida, etc.
- **ESP Information:** Algoritmos de autentificación y cifrado, claves, tiempos de vida, valores iniciales, etc.
- **IPsec Protocol Mode:** Túnel o Transporte.
- **SA Lifetime:** Intervalo de tiempo o bytes de una SA.

Campos de la SAD (2)

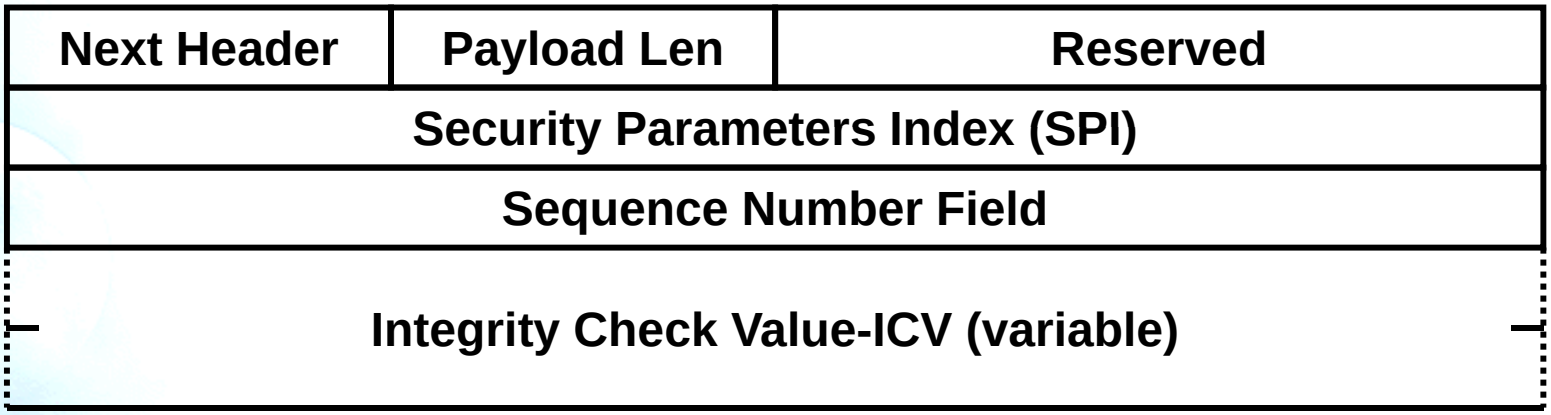
- **Stateful fragment checking flag**: Indica si se aplica o no comprobación de fragmentado a la SA.
- **DSCP values:** El conjunto de valores DSCP permitidos para los paquetes que van sobre esta SA. Si no se especifica ningún valor no se aplica ningún filtro DSCP.
- **Bypass DSCP (T/F)** o mapear a valores DSCP no protegidos si es necesario para restringir el paso de valores DSCP, aplicable a SAs en modo túnel.
- **Tunnel header IP source and destination address:** ambas direcciones deben ser o IPv4 o IPv6.
- **Path MTU:** Tamaño máximo de paquete transmitido sin fragmentar.

Transmisión IPsec

- Cabecera IPsec insertada entre la cabecera original y la carga.
- Si se usa ESP, los datos se cifran y se añade una 'coletilla' IPsec.

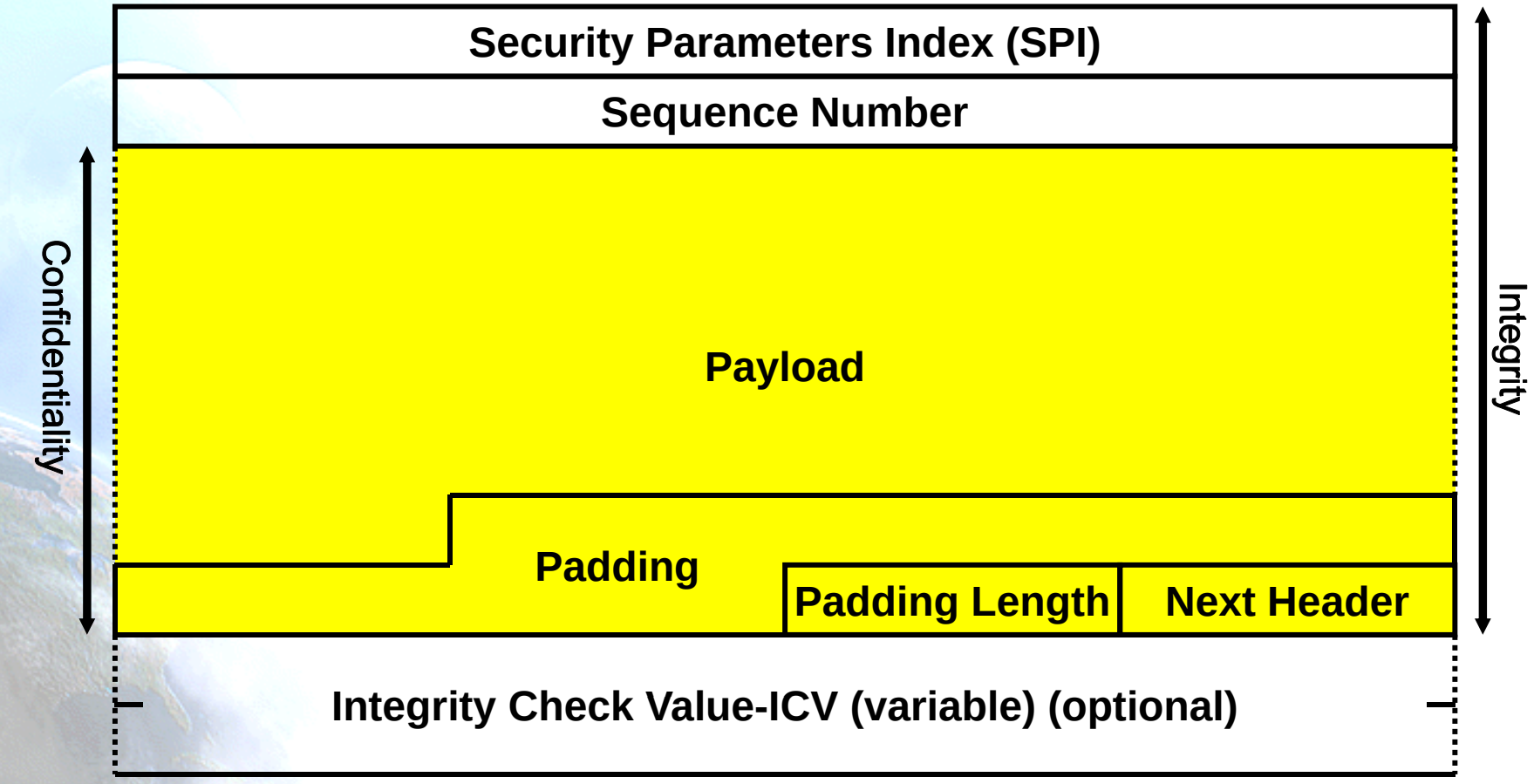
- Valor de Next Header:
  - ESP = 50
  - AH = 51

Cabecera AH (RFC4302)



- **SPI:** Valor arbitrario de 32 bits que usa el receptor para identificar la SA a la que pertenece un paquete que llega, el tipo de protocolo IPsec (AH) también puede ser necesario.
- **Sequence Number:** campo de 32 bits sin signo que contiene un contador que se incrementa en uno por cada paquete enviado, i.e., un número de secuencia de paquete para cada SA.
- **Integrity Check Value (ICV)**: Campo de longitud variable Variable. El campo debe tener un tamaño múltiplo de 32 bits (para IPv4 e IPv6).

Cabecera ESP (RFC4303)



Algoritmos ESP

- Especificados en la SA.
- Algoritmos de Cifrado ESP (RFC4835):
  - **MUST**: NULL (RFC2410), AES-CBC con clave de 128-bit (RFC3602)
  - **MUST-**: TripleDES-CBC (RFC2451)
  - **SHOULD**:AES-CTR (RFC3686)
  - **SHOULD NOT**: DES-CBC (RFC2405)
- Algoritmos de Autentificación ESP (RFC4835):
  - **MUST**: HMAC-SHA1-96 (RFC2404)
  - **SHOULD+**: AES-XCBC-MAC-96 (RFC3566)
  - **MAY**: NULL, HMAC-MD5-96 (RFC2403)

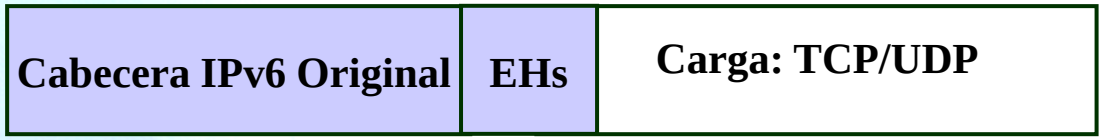
Algoritmos AH

- Especificados en la SA
- Algoritmos de Autentificación AH (RFC4835):
  - **MUST**: HMAC-SHA1-96 (RFC2404)
  - **SHOULD+**: AES-XCBC-MAC-96 (RFC3566)
  - **MAY**: HMAC-MD5-96 (RFC2403)

Modos de Uso

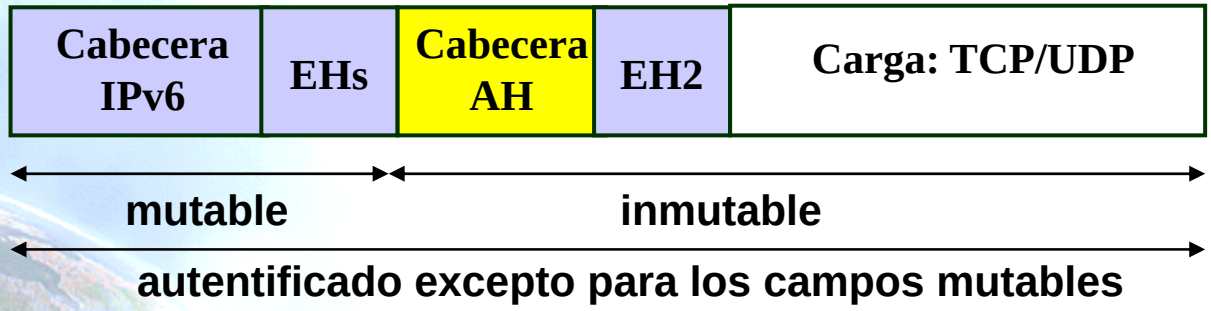
- Cada protocolo soporta dos modos de uso:
  - Modo Transporte (protege principalmente protocolos de capa superior)
    - Directo entre dos sistemas extremo-a-extremo
    - Los dos sistemas remotos deben soportar IPsec!
  - Modo Túnel (protocolos aplicados a paquetes IP encapsulados)
    - Túnel seguro para encapsular paquetes IP inseguros
    - Entre sistemas intermedios (no extremo-a-extremo)

AH en Modo Transporte y Túnel

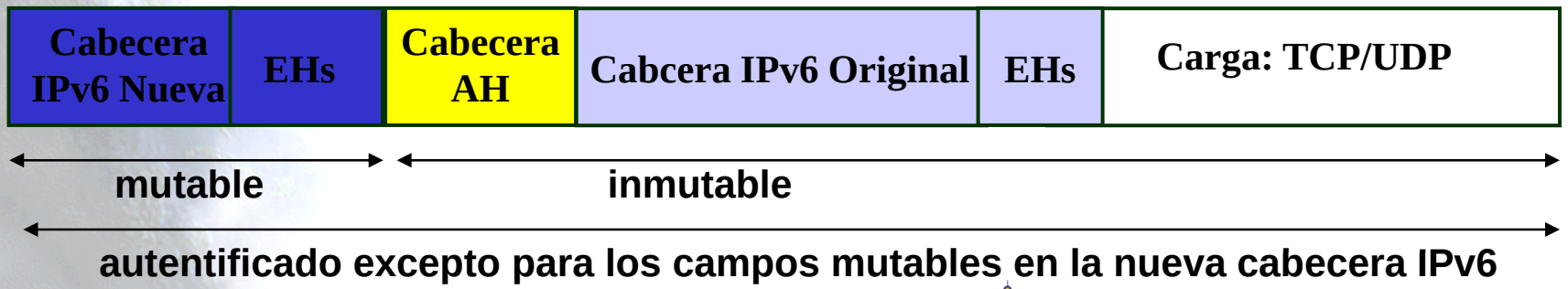


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

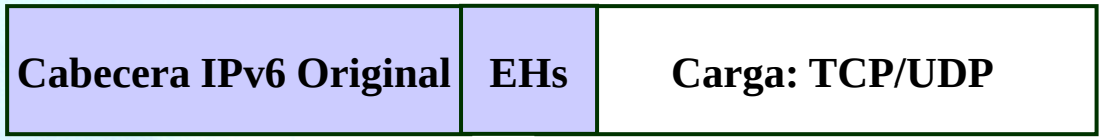
Modo Transporte



Modo Túnel

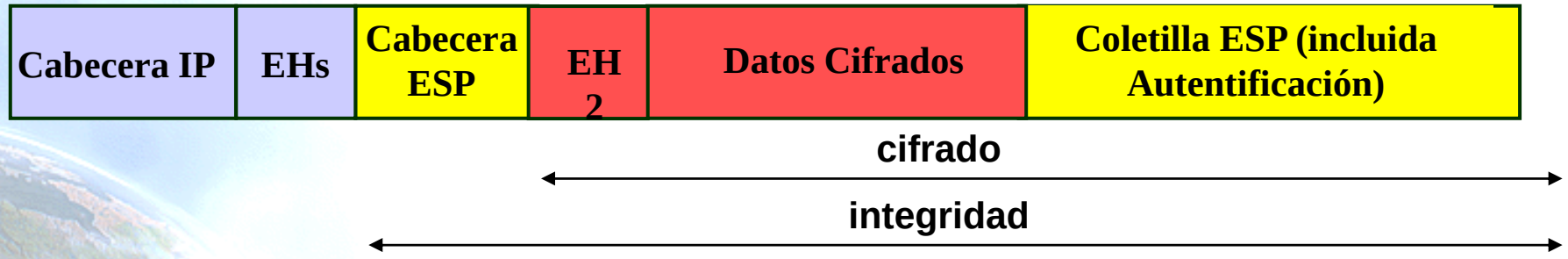


ESP en Modo Transporte y Túnel

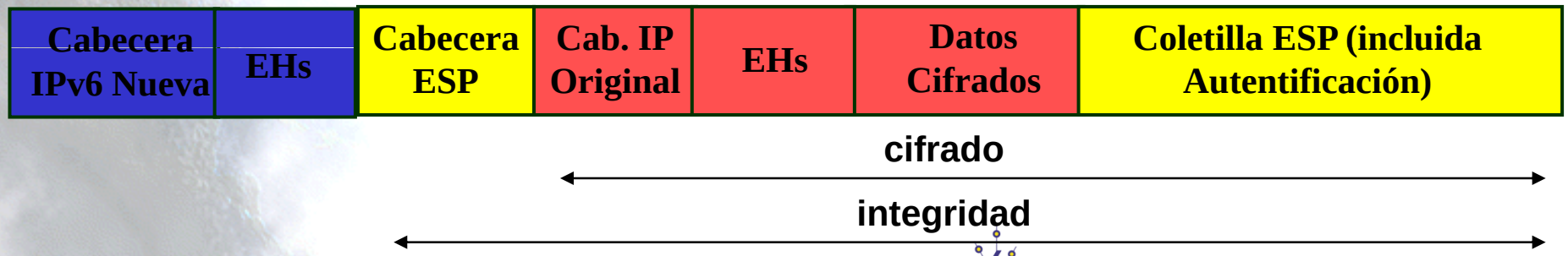


- EHs: Extension Headers: Hop-by-hop, Routing, Fragment, Dest. Option
- EH2: Destination Option Extension Header

Modo Transporte

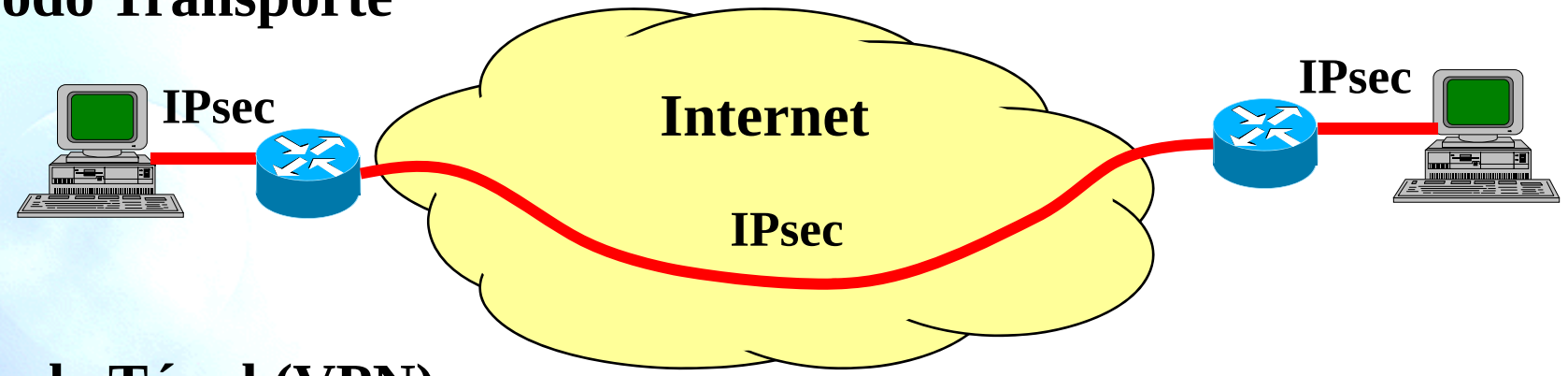


Modo Túnel

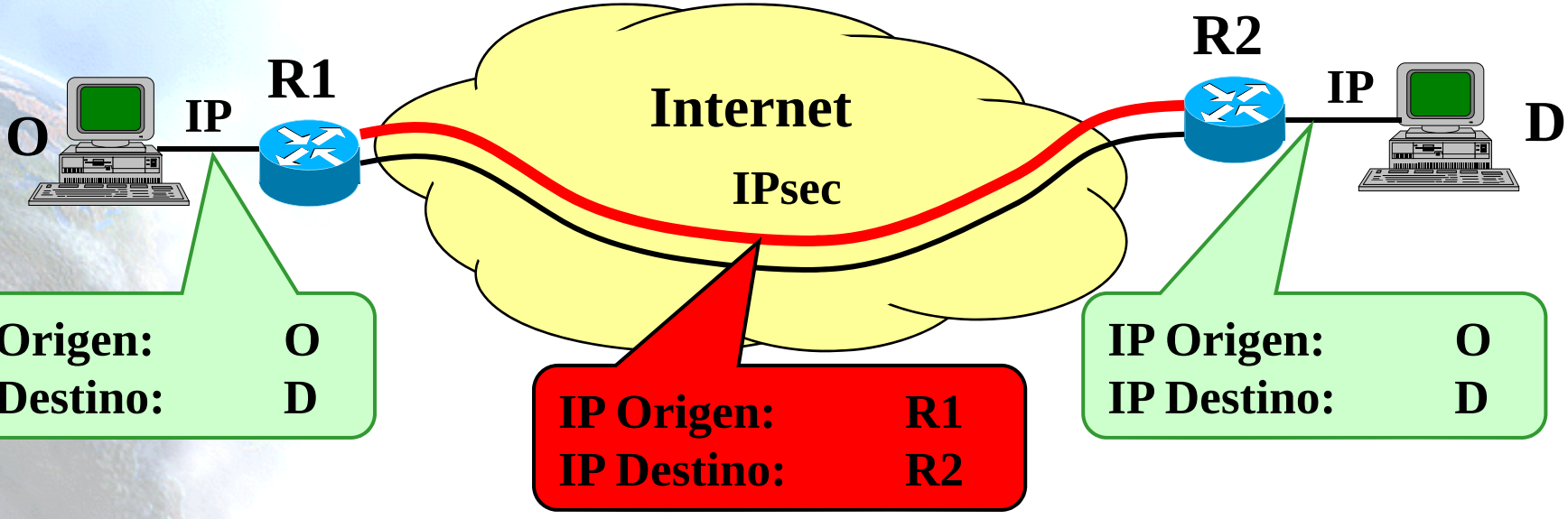


Modo Transporte vs. Túnel

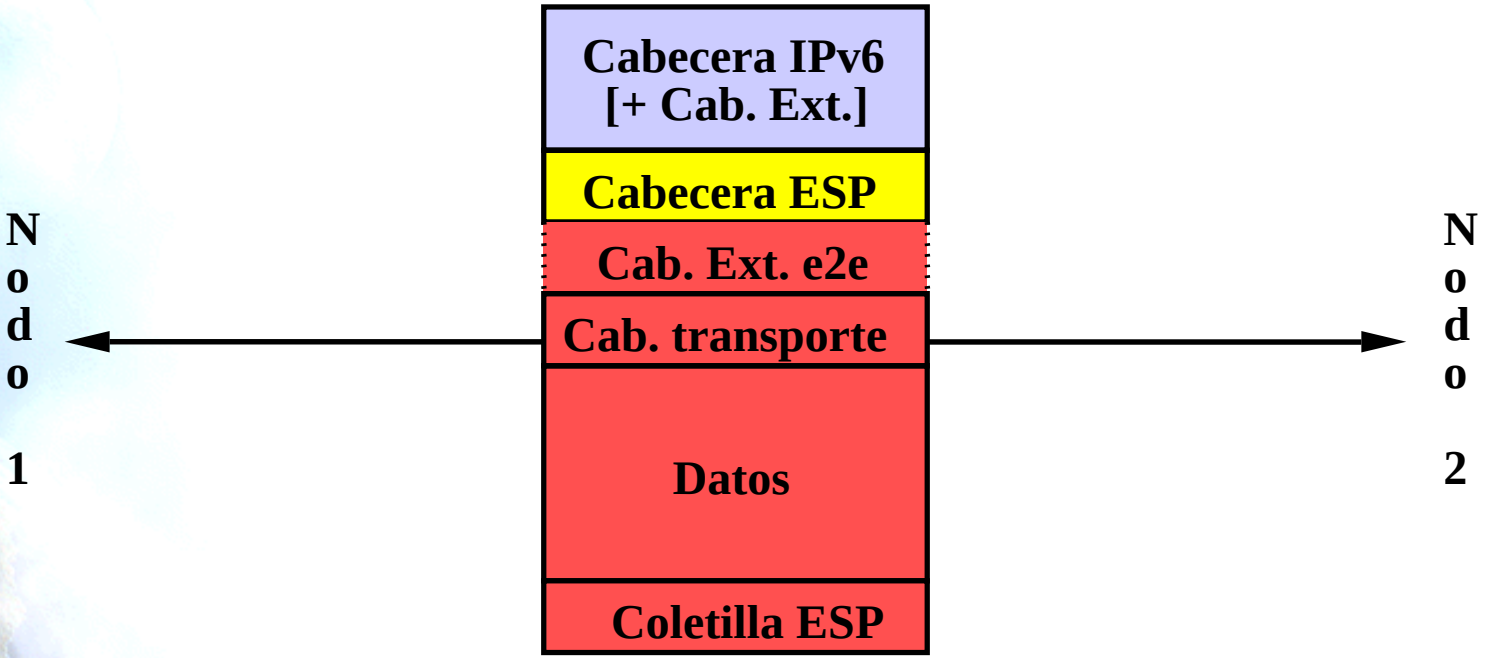
Modo Transporte



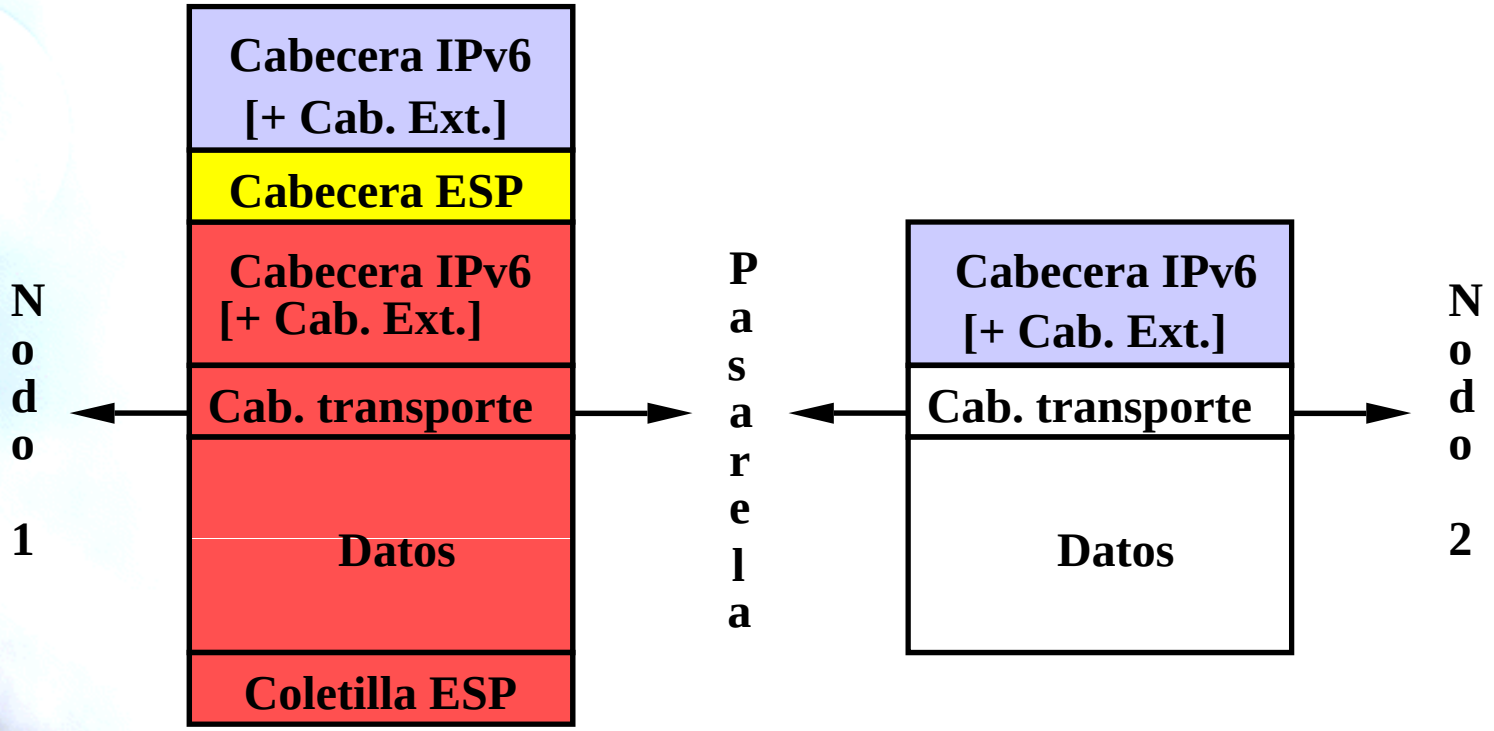
Modo Túnel (VPN):



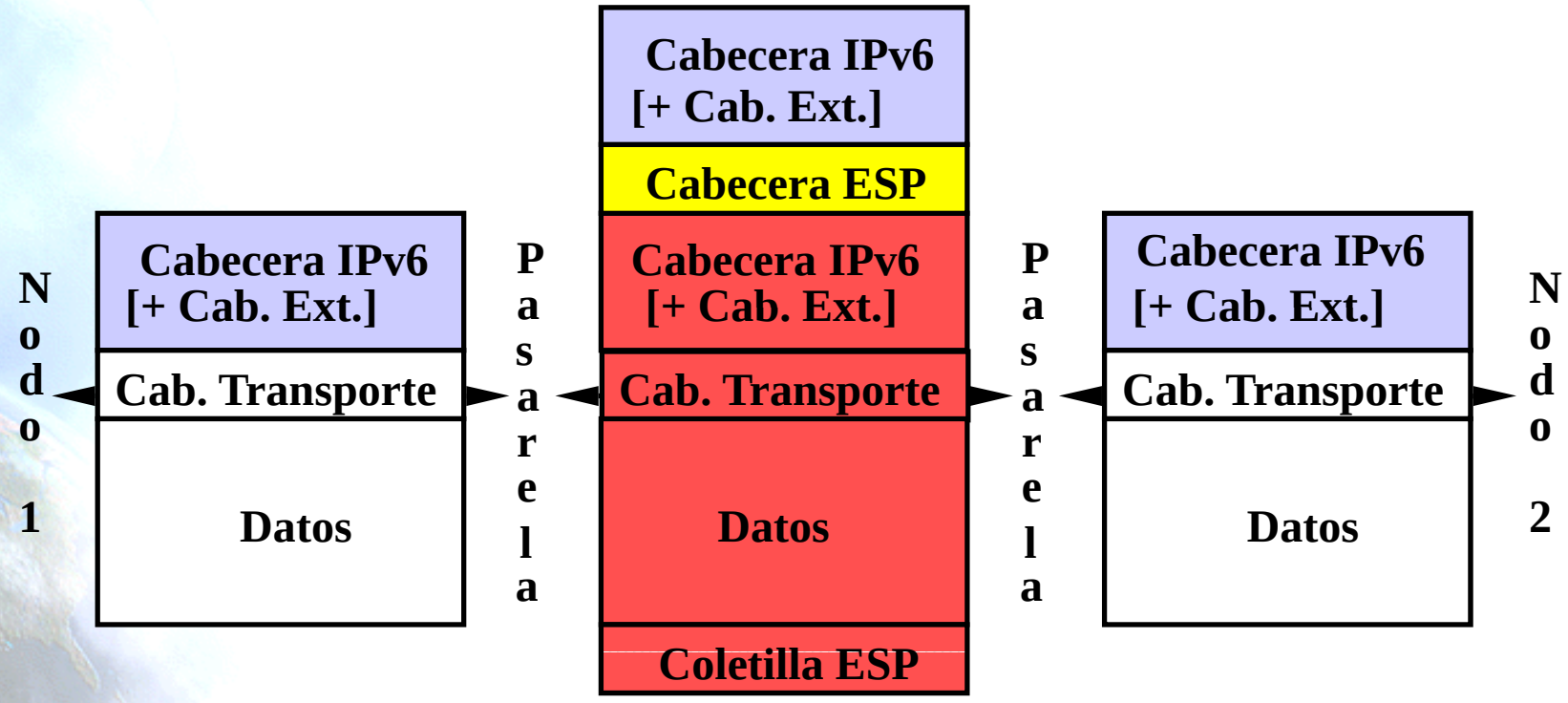
ESP Modo Transporte Extremo-a-extremo



ESP Modo Túnel
Extremo a Pasarela de Seguridad



ESP Modo Túnel
Pasarela a Pasarela



El problema de la clave

- AH y ESP necesitan usar las mismas claves con el fin de establecer la SA entre los nodos extremos
  - En algunos casos esa clave se configura manualmente, pero no es una solución escalable a decenas o cientos de nodos
    - Gestión más sencilla.
    - Cada sistema se configura con las claves propias y de los demás.
  - En ciertos entornos se necesita una solución que sea automática, creando una SA de forma dinámica, pero eso requiere la existencia de un canal seguro entre los nodos con el fin de intercambiar las claves
    - IKE es la solución propuesta para el establecimiento de SA de forma automática
- IKEv1 (RFC4109) es en realidad una combinación de otras piezas:
  - ISAKMP (RFC2408). Marco abstracto para la autenticación e intercambio de claves, diseñado para ser independiente del método particular de intercambio de claves que se vayan a usar
    - “Internet IP Security Domain of Interpretation for ISAKMP” o Internet DOI (RFC2407). Define el uso de los campos de ISAKMP (números de protocols, algoritmos, modos, etc.)
  - OAKLEY (RFC2412). Proporciona métodos seguros para la determinación de claves.
  - SKEME. Proporciona un mecanismo versátil para el intercambio de claves.

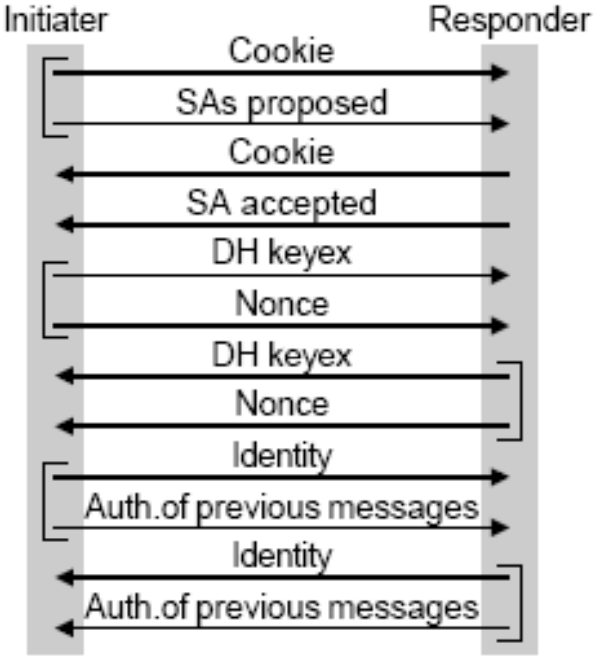
Principios básicos de IKE (1)

- "IKE proporciona un mecanismo seguro para el intercambio de claves entre nodos Ipsec con el fin de permitir el establecimiento y gestión de SA
  - Se trata de un protocolo extremo-a-extremo
  - El bloque fundamental de IKE es la Asociación de Seguridad del protocolo ISAKMP
    - Una SA ISAKMP es bidireccional, a diferencia de una SA IPsec
- IKE proporciona un canal seguro para el intercambio de información para el establecimiento de claves para IPsec
- Los nodos involucrados deben autenticarse mutuamente mediante:
  - "pre-shared secrets" (PSK)
  - Firmas digitales (DSS o RSA)
  - Certificados X.509
  - Encriptación basada en claves públicas
- IKE usa datagramas UDP para el intercambio de mensajes
  - Puerto 500
- La configuración ISAKMP se compone de dos fases
  - La fase 1 es para la configuración de una SA ISAKMP entre los dos nodos (canal seguro)
    - Se ejecuta de forma infrecuente
    - Existen tres modos diferentes de funcionamiento de la fase 1 apropiados para diferentes escenarios/servicios
  - La fase 2 sirve para el establecimiento de la asociación IPsec
    - Se ejecuta más a menudo para generar otras SAs

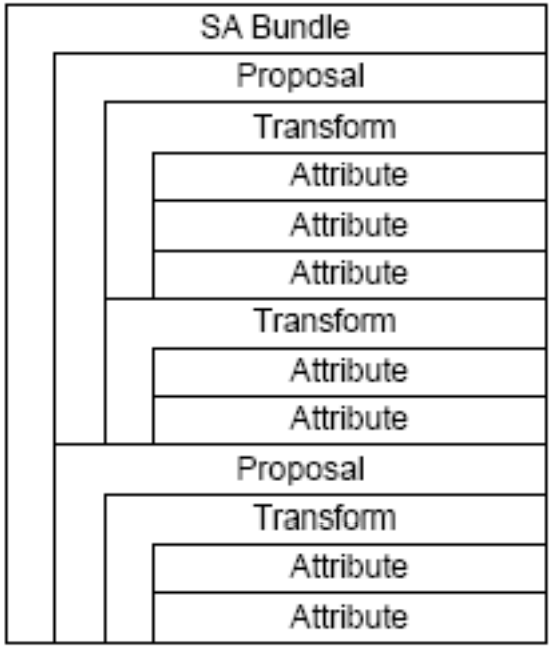
Principios básicos de IKE (2)

- Existen muchísimas variantes posibles debido a las posibles variantes de parámetros
  - Tipos de algoritmos de cifrado
  - Tipos funciones hash
  - Tipos algoritmos intercambio de claves
  - Tipos de autenticación
- ISAKMP se base en valores de jerarquía multinivel
  - Cada propuesta se compone de una transformada con diferentes atributos
  - Cada transformada define
    - Método de cifrado
    - Método de autenticación

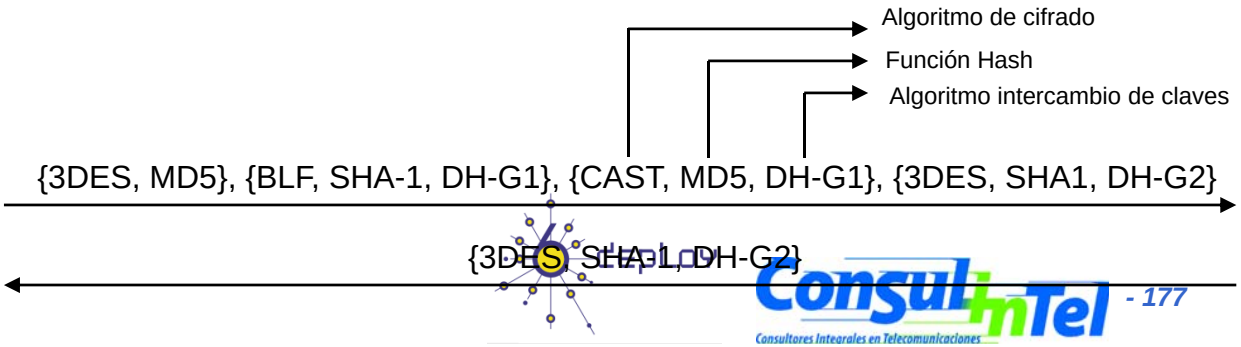
Ejemplo de FASE1



Ejemplo de SA ISAKMP



Ejemplo de negociación de parámetros de seguridad



Objetivos de IKEv2

- IKEv1 es demasiado difícil y extremadamente complicado de depurar en caso de problemas
- IKEv1 no es manejable en entornos de producción con muchos nodos
- La configuración de IKEv1 precisa de ingenieros de red con mucha experiencia
  - Se puede llegar a tardar más de una jornada de trabajo en la configuración de un enlace IPsec con IKEv1 en el caso de usar equipos de fabricantes diferentes
- Al final los usuarios tienden a configurar manualmente las SA IPsec debido a la complejidad de IKEv1
- Como consecuencia se ha definido IKEv2 (RFC4306) con el fin de hacer las cosas más sencillas
  - IKEv2 se define en un solo documento en vez de un conjunto de ellos como en IKEv1
  - Con IKEv2 se simplifica y se mejora IKEv1
  - IKEv2 ofrece un formato de cabeceras y un intercambio de mensajes más simple que IKEv1
  - Soluciona varios problemas de IKEv1

Diferencias de IKEv2 respecto IKEv1

- La principal es que tiene muchas funcionalidades en común con IKEv1 pero de forma más simple:
  - Ocultación de la identidad
  - “perfect forward secrecy” (PFS)
  - Dos fases para el establecimiento de la SA
  - Negociación de las claves
  - IKEv2 usa también el puerto 500 UDP para el intercambio de mensajes, pero **NO** es compatible con los mensajes de IKEv1
- IKEv2 pone más énfasis en VPN (modo túnel)
- Proporciona la posibilidad de atravesar NATs
  - Permite el encapsulamiento de paquetes IKE y ESP en UDP para atravesar NATs
- Su funcionamiento se basa en conocer el estado de la conexión con el fin de prevenir ataques de tipo DoS
- Se añade soporte EAP (RFC2284) como método de autenticación
- Se permite una asignación dinámica de dirección IP posibilitando la actualización de la SA
- Se permite el uso de compresión IP
- Buen soporte para la integración con infraestructuras AAA con el fin de que todo el material criptográfico del usuario resida en dicha infraestructura

5.3 Extensiones de Privacidad

Introducción

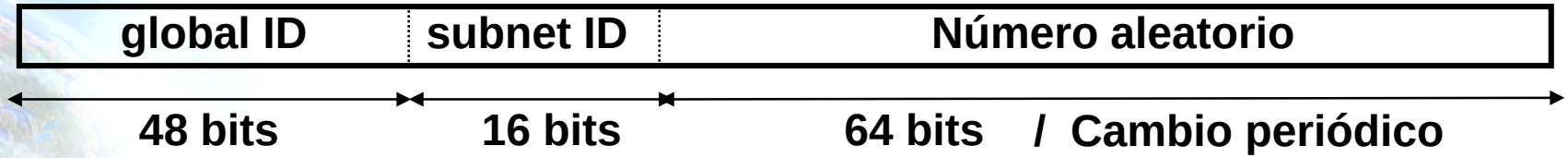
- En la autoconfiguración “stateless” de IPv6 en algunos casos el identificador de interfaz contiene un identificador único del IEEE, lo que permite identificar un nodo a partir de una dirección IP.
- El RFC4941 describe una extensión para la autoconfiguración “stateless” en IPv6 que hace que los nodos generen direcciones de ámbito global que cambian con el tiempo.
- El RFC4941 se basa en generar identificadores de interfaz aleatorios con un tiempo de vida limitado.

¿Por qué Extensiones de Privacidad?

- El problema (con identificadores IEEE)
  - Las direcciones IPv6 en un interfaz dado y generada via “Stateless Autoconfiguration” contienen el mismo ID de interfaz, con independencia del lugar de Internet en el que el dispositivo se conecta. Esto puede facilitar la trazabilidad de dispositivos y/o individuos.
- Posibles Soluciones
  - Usar DHCPv6 para obtener direcciones. El servidor DHCP podría asignar “direcciones temporales” que nunca se renuevan y tienen la condición de temporalidad necesaria
  - Cambiar el ID de interfaz de una dirección IPv6 cada cierto tiempo y generar por tanto nuevas direcciones IPv6 para determinados ámbitos

Extensiones de Privacidad (1)

- Los nodos usan “IPv6 Stateless Autoconfiguration” para generar direcciones sin la necesidad de usar un servidor DHCPv6
  - Las direcciones se forman combinando el prefijo de red con un ID de interfaz
    - En interfaces que contienen ID de IEEE, se usa dicho ID para derivar el ID de interfaz de la dirección IPv6
    - En otros tipos de interfaces, el ID se crea por otros medios, por ejemplo generando números aleatorios



- El uso de extensiones de privacidad hace que los nodos generen direcciones IPv6 partiendo de ID de interfaz que cambian de vez en cuando, incluso si el interfaz contiene un ID de IEEE

Extensiones de Privacidad (2)

1. En realidad no provoca ningún cambio en el comportamiento básico de las direcciones generadas vía “Stateless Autoconfiguration”.
2. Se crean direcciones adicionales basadas en un ID de interfaz aleatorio con el propósito de iniciar sesiones.
   - Estas direcciones aleatorias se suelen emplear durante un período corto de tiempo (desde horas a días) y son deprecadas después de dicho período.
   - Las direcciones deprecadas se pueden seguir usando para sesiones abiertas, pero no para iniciar nuevas conexiones.
   - Periódicamente se generan nuevas direcciones temporales para reemplazar direcciones temporales que ya han expirado.
3. Se produce una secuencia de direcciones globales temporales a partir de una secuencia de IDs de interfaz que aparentemente son aleatorios en el sentido de que es difícil para un observador externo predecir la dirección/identificador futura basada en la actual e igualmente difícil determinar la dirección anterior conociendo la presente.
4. Por defecto, a partir del mismo ID de interfaz aleatorio, se generan tantas direcciones como prefijos se hayan usado para generar una dirección global mediante SAAC.

5.4 Amenazas a ND

Visión General

- El protocolo Neighbor Discovery (ND) (RFC4861) es vulnerable a diversos ataques (RFC3756)
- La especificación original del protocolo ND define el uso de IPsec para proteger los mensajes de ND. Por diversas razones en la práctica esta no es una solución
- SEcure Neighbor Discovery (SEND) (RFC3971), explicado anteriormente, tiene como objetivo proteger ND

Amenazas a ND (1)

- Neighbor Solicitation/Advertisement Spoofing
  - Se hace o bien mandando un NS con una opción de dirección de capa de enlace origen cambiada, o enviando un NA con una opción de dirección de capa de enlace destino cambiada
  - Este es un ataque de redirección/DoS
- Fallo de Neighbor Unreachability Detection (NUD).
  - Un nodo malicioso puede permanecer enviando NAs hechos “a medida” como respuesta a mensajes NS de NUD. Si los mensajes NA no se protegen de alguna manera el atacante puede llevar a cabo el ataque por periodos muy largos de tiempo
  - Este es un ataque DoS (Denegación de Servicio)

Amenazas a ND (2)

- Ataque DoS usando DAD
  - Un nodo atacante puede lanzar un ataque DoS respondiendo a todos los intentos de DAD hecho por un host que llega a la red
  - El atacante puede reclamar la dirección de dos maneras: puede responder con un NS, simulando que también esta haciendo DAD, o bien puede responder con un NA, simulando que ya ha esta usando esa dirección
  - También puede estar presente cuando se use otro tipo de configuración de direcciones, es decir, siempre que se invoque DAD antes de configurar una dirección
  - Es un ataque de tipo DoS

Amenazas a ND (3)

- Encaminador de Último Salto Malicioso
  - Un nodo atacante en la misma subred que un host que intenta descubrir un encaminador de ultimo salto legítimo, se puede hacer pasar por un encaminador IPv6 enviando por multicast un RA o por unicast un RA como respuesta a un RS del nodo que llega a la red
  - El atacante se puede asegurar de que el nodo que llega a la red lo selecciona a él como el encaminador por defecto enviando periódicamente por multicast RAs para el encaminador verdadero pero con tiempo de vida cero. Esto haría que creyese que el router verdadero no quiere cursar tráfico
  - Esta amenaza es un ataque de redirección/DoS

Amenazas a ND (4)

- ‘Muerte’ del encaminador por defecto
  - Un atacante ‘mata’ el(los) encaminador(es) por defecto, haciendo que todos los nodos del enlace asuman que todos los nodos son locales
  - El atacante puede lanzar un ataque DoS clásico contra el encaminador de forma que parezca que no responde. Otra forma sería enviar un RA falso con tiempo de vida cero (zero Router Lifetime)
- El ‘buen’ encaminador se vuelve ‘malo’
  - Un router en el que previamente se confiaba queda comprometido
  - Se aplica el caso de ‘Encaminador de último salto malicioso’
  - Este es un ataque de redirección/DoS

Amenazas a ND (5)

- Mensaje Redirect Falso
  - El atacante usa la dirección en enlace-local del encaminador de primer salto actual para enviar un mensaje Redirect a un host legítimo
  - Debido a que el host identifica el mensaje como proveniente del encaminador por la dirección de enlace-local, acepta el Redirect
  - Siempre que el atacante responda a los mensajes NUD a la dirección de capa de enlace, el efecto de la redirección seguirá vigente
  - Este es un ataque de redirección/DoS

Amenazas a ND (6)

- Prefijo falso en el enlace
  - Un nodo atacante puede enviar un RA especificando que un prefijo de longitud arbitraria pertenece al enlace
  - Si un host que va a enviar un paquete piensa que ese prefijo pertenece al enlace, nunca enviará un paquete con destino a ese prefijo al encaminador. Por el contrario, usará un NS para resolver la dirección, pero el NS no tendrá respuesta, denegando de esta forma el servicio a ese host
  - Este ataque se puede extender a un ataque de redirección si el atacante responde al NS con NAs falsos
  - Este es un ataque DoS

Amenazas a ND (7)

- Prefijo falso para configuración de dirección
  - Un nodo atacante puede enviar un RA especificando un prefijo de red inválido para ser usado por un host para la autoconfiguración de direcciones
  - Como resultado, los paquetes de respuesta nunca llegan al host porque su dirección origen no es valida
  - Este ataque tiene el potencial de propagarse más allá del host atacado si el host realiza una actualización dinámica en el DNS usando la dirección construida con el prefijo falso
  - Este es un ataque DoS

Amenazas a ND (8)

- Parámetros falseados.
  - Un nodo atacante puede enviar RAs con significado válido que dupliquen los RAs enviados por el encaminador por defecto válido, excepto en que los parámetros incluidos están pensados para interrumpir el tráfico legítimo
  - Algunos ataques específicos:
    1. Incluir un 'Current Hop Limit' de uno u otro número pequeño que el atacante sepa causará que los paquetes legítimos se descartarán antes de llegar a su destino
    2. El atacante implementa un servidor o 'relay' DHCPv6 falso y los flags 'M' y/o 'O' están activados, indicando que la configuración 'stateful' de direcciones y/o otros parámetros de realizarse. El atacante puede responder a las peticiones de configuración 'stateful' de un host legítimo con sus respuestas falsas
  - Este es un ataque DoS

Amenazas a ND (9)

- Ataques de Reactuación (Replay)
  - Todos los mensajes de Neighbor Discovery y Router Discovery pueden sufrir ataques de reactuación
  - Un atacante podría capturar mensajes válidos y reenviarlos más tarde
  - En los intercambios de tipo petición-respuesta, como los de ‘Solicitation-Advertisement’, la petición puede contener un valor (nonce) que debe aparecer también en la respuesta. Las respuestas antiguas no son válidas ya que no contienen el valor correcto
  - Los mensajes ‘solitarios’, como los ‘Advertisements’ no solicitados o los mensajes ‘Redirect’, deben protegerse con sellos temporales o contadores

Amenazas a ND (10)

- Ataque DoS a Neighbor Discovery
  - El nodo atacante comienza a fabricar diversas direcciones a partir del prefijo de red y envía paquetes continuamente a esas direcciones. El encaminador de último salto se ve obligado a resolver esas direcciones enviando paquetes NS
  - Un host legítimo que intenta conectarse a la red no será capaz de obtener servicio de ND por parte del encaminador de último salto ya que estará ocupado enviando otras peticiones (NS)
  - Este ataque DoS es diferente de los otros en el sentido de que el atacante puede estar fuera del enlace

5.5 Comparativa IPv4 vs. IPv6

Visión General

- **Seguridad:** incluye diversos procedimientos, mecanismos, prácticas recomendadas y herramientas
- Con **IPv6** hay muchos puntos que serán los mismos que con IPv4, i.e., son “independientes de IP”. Ejemplo, actualizaciones de firmware y software o riesgos de seguridad a nivel de aplicación
- IPv6 introduce nuevos temas a tener en cuenta. Veremos que estos puntos pueden significar una ventaja o desventaja desde el punto de vista de la seguridad

Seguridad IPv6: primer contacto

- Las dos primeras ideas que vienen a la mente de un responsable de seguridad que despliega IPv6 son:
  1. Se utilizan direcciones globales (existe la excepción de las ULAs), i.e., son alcanzables desde cualquier sitio de Internet, en otras palabras, **no hay NAT**.
  2. Todas la pilas IPv6 deben soportar IPsec, como se ha visto.
- La primera puede dar la falsa impresión de peligro y la segunda la falsa impresión de protección. Se profundizará más en esto después.

Clasificación de las Amenazas de Seguridad

- Se establecen tres categorías para las amenazas de seguridad en IPv6:
  1. Amenazas que ya existían con IPv4 y que tienen un comportamiento similar con IPv6.
  2. Amenazas que ya existían con IPv4 y que presentan novedades con IPv6.
  3. Nuevas amenazas que aparecen con IPv6.

Amenazas IPv4 con comportamiento similar con IPv6

- **Sniffing:** IPsec puede ayudar.
- **Ataques a Nivel de Aplicación**: IPsec puede usarse para perseguir al atacante, aunque introduce problemas para los IDS. También puede usarse protección en el nivel de Aplicación.
- **Dispositivos no autorizados**: Se hacen pasar por conmutadores, encaminadores, puntos de acceso o recursos como servidores DNS, DHCP o AAA.
- **Ataques de 'Hombre-en-el-medio'**: IPsec puede ayudar.
- **Ataques por inundación**.

Amenazas IPv4 con diferente comportamiento con IPv6 (1)

- **Escaneo de Red**: El escaneo de una red típica (/64) en la práctica es más difícil. También los ataques automatizados, por ejemplo gusanos que seleccionan direcciones aleatorias para propagarse, se ven dificultados.
- **Ataques de Amplificación Boradcast (Smurf)**: Ataque DoS. Un mensaje echo ICMP se envía a la dirección de broadcast de un prefijo de red con la dirección de origen falseada a la del host víctima. Todos los nodos del prefijo destino envían una echo reply a la víctima. E**n IPv6, no existe el concepto de broadcast.**

Amenazas IPv4 con diferente comportamiento con IPv6 (2)

- **Ataques relacionados con Mecanismos de Transición**: No se utilizan nuevas tecnologías, el mismo tipo de vulnerabilidades que con IPv4:
  - Redes doble-pila pueden ser atacadas usando ambos protocolos.
  - Los túneles IPv6 necesitan nuevos puertos abiertos en los firewalls.

  Recomendaciones:
  - En redes/hosts de doble-pila usar medidas de seguridad similares para IPv4 e IPv6.
  - Controlar el uso de túneles cuando sea posible.
  - Habilitar que los firewalls inspeccionen el tráfico encapsulado.

Nuevas Amenazas IPv6

- Amenazas a ND
- Routing Header Type 0 (RFC5095)
- Mecanismos de Transición, en el sentido de que funcionan encapsulando tráfico y los firewalls y otros dispositivos/software de seguridad deben ser capaces de procesarlos.
- IPsec, en el sentido de enviar datos cifrados que los firewalls no pueden inspeccionar, especialmente firewalls ‘full-state’.

5.6 Aspectos de seguridad con IPv6

Aspectos de Seguridad con IPv6 (1)

- **IPsec**: Como se ha dicho antes es obligatorio en todas las implementaciones de IPv6. Esto puede proporcionar una falsa sensación de seguridad, porque la seguridad la proporciona solamente si se usa IPsec. En la práctica IPsec no se encuentra ampliamente desplegado y en uso debido a la falta de un mecanismo de intercambio de claves a nivel de todo Internet.

  IPsec se configura manualmente para algunas configuraciones concretas y controladas, esto no es escalable.

  Otro aspecto a tener en cuenta es que el tráfico IPsec (ESP) no puede ser inspeccionado por los firewalls.

Aspectos de Seguridad con IPv6 (2)

- **Extrema-a-extremo**: El uso de direcciones IPv6 globales **permite pero no obliga** a todos los nodos a ser alcanzables. El administrador de seguridad/red debe decidir si todos, algunos o ningún tráfico puede alcanzar cada parte de la red.

  Diversos escenarios:

  - **Usuario DSL**: El tráfico debe alcanzar el CPE sin interferencias. El usuario tiene la responsabilidad de filtrar en el CPE.
  - **Centro de Datos**: Entorno controlado donde solo los servicios permitidos deben desplegarse.

Aspectos de Seguridad con IPv6 (3)

- El **nuevo esquema de direccionamiento** implica:
  - El **número de direcciones e**s REALMENTE grande. No tiene sentido el escaneo aleatorio o por fuerza bruta (RFC5157)
  - Cada nodo puede tener **varias direcciones** e incluso identificadores de interfaz aleatorios (RFC4941). Esto dificulta el control sobre un host por medio de su IP
  - El uso de direcciones de enlace-local en una interfaz IPv6, proporciona conectividad IP en un segmento de LAN sin ayuda externa. Como guía, no debe confiarse en sesiones que vengan de direcciones de enlace-local y permitirlas solo para servicios básicos
  - Se han definido direcciones multicast bien conocidas para facilitar la localización de servicios. Esto también facilita la localización de servicios para atacarlos (FF05::2 All routers, FF05::1:3 All DHCP Servers)

Aspectos de Seguridad con IPv6 (4)

- **Cabeceras de Extension (EH)**: este potente y flexible mecanismo debe tenerse en cuenta por los dispositivos de seguridad, es decir, deben ser capaces de inspeccionar la ‘cadena’ de cabeceras.
- **Fragmentación**: En IPv6 solo los hosts finales pueden fragmentar paquetes. Esto reduce los ataques posibles utilizando solapamiento de fragmentos o fragmentos muy pequeños. Las consideraciones para fragmentos desordenados son las mismas que en IPv4 pero en los nodos finales. Los firewalls no deben filtrar fragmentos de paquetes.

Aspectos de Seguridad con IPv6 (5)

- **Autoconfiguración:** En IPv6 se definen distintos medios para la autoconfiguración. DHCP tiene las mismas consideraciones en IPv4 e IPv6. Neighbor Discovery Protocol tiene varias amenazas (como ARP en IPv4), e IPsec y SEND se pueden usar para añadir seguridad.
- **Movilidad IPv6**: IPv6 facilita el despliegue de Movilidad IP aunque algunos elementos necesarios para un despliegue ‘en el mundo real’ están siendo definidos, incluyendo temas de seguridad.

Aspectos de Seguridad con IPv6 (6)

- **Routing Header:** Type 0 Routing Header (RH0) puede ser usada para lograr amplificación de tráfico sobre un camino remoto con el propósito de generar tráfico DoS.

  Se puede construir un paquete que 'oscile' entre dos hosts/routers que procesen RH0 muchas veces. Esto permite que un flujo de paquetes de un atacante se amplifique en el camino entre dos encaminadores remotos. Esto puede usarse para causar congestión sobre un camino remoto arbitrario y por lo tanto actuar como un mecanismo de DoS.

Aspectos de Seguridad con IPv6 (7)

- La gravedad de esta amenaza se consideró suficiente para prohibir el uso de RH0 (RFC5095)
- Sólo afecta a la cabecera de extensión Routing Type 0, de manera que las especificaciones para la Type 2 siguen siendo válidas, usada en MIPv6

5.7 Temas prácticos

Temas Prácticos (1)

- **ICMPv6 es una parte fundamental de IPv6**. Con IPv4 un filtrado de tipo ‘deny_all_ICMP’ podía usarse, pero con IPv6 significaría que funcionalidades básicas dejasen de funcionar.

Type - Code	Descripción	Acción
Type 1	Destination unreachable	ALLOW, de entrada para detectar algunos errores
Type 2	Packet too big	ALLOW, necesario para PMTU discovery
Type 3 - Code 0	Time Exceeded	ALLOW
Type 4 - Code 1 y 2	Parameter problem	ALLOW, para detectar algunos errores
Type 128	Echo reply	ALLOW para **depurar la red** o **Teredo**. De entrada se puede permitir limitando la frecuencia. De salida permitir para algunos **servicios conocidos**.
Type 129	Echo request	ALLOW para **depurar la red** o **Teredo**. De salida se puede permitir limitando la frecuencia. De entrada permitir para algunos **servicios conocidos**.
Type 130,131,132,143	Multicast listener	ALLOW si se despliega Multicast y MLD debe atravesar el firewall
Type 133	Router Solicitation	ALLOW si el firewall interfiere en ND
Type 134	Router Advertisement	ALLOW si el firewall interfiere en ND
Type 135	Neighbor Solicitation	ALLOW si el firewall interfiere en ND
Type 136	Neighbor Advertisement	ALLOW si el firewall interfiere en ND
Type 137	Redirect	NOT ALLOW
Type 138	Renumbering	NO TALLOW
Type 139	Node information Query	NOT ALLOW
Type 140	Node information Reply	NOT ALLOW

Temas Prácticos (2)

- Dependiendo del nivel de control y seguimiento que se requiera se deben usar distintos métodos de configuración de direcciones. De más a menos:
  - Direcciones estáticas.
  - Autoconfiguración ‘Stateful’: DHCPv6.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz a partir de la dirección MAC.
  - Autoconfiguración ‘Stateless’: Identificador de interfaz utilizando las extensiones de privacidad.

Temas Prácticos (3)

- Se recomienda **filtrar los prefijos no asignados**. También el tráfico ULA no debe atravesar Internet. Si se despliega Multicast estos prefijos deben permitirse.

IANA es la encargada de asignar los prefijos de direcciones:

- Espacio Direcciones IPv6: http://www.iana.org/assignments/ipv6-address-space

- Asignaciones Globales Unicast IPv6: http://www.iana.org/assignments/ipv6-unicast-address-assignments

- El filtrado puede ser 'grueso' (Permitir 2000::/3 Global Unicast) o fino (2600:0000::/12, 2400:0000::/12, etc.)

Temas Prácticos (4)

- **Utilizar direcciones difíciles de adivinar**, por ejemplo no usar ::1 para encaminadores o servidores, para dificultar el trabajo del atacante.

  Un ejemplo sería, habilitar la autoconfiguración steteless y después usar esa dirección autoconfigurada en una asignación estática. Esta dirección también se configuraría en el DNS

- **Desplegar Ingress Filtering** (RFC2827, RFC3074) de una manera similar a como se hace para IPv4

Temas Prácticos (5)

- Si se utilizan **Mecanismos de Transición**, asegurarse de que el prefijo correspondiente se anuncia y que su tráfico no se filtra

5.8 Firewalling

Introducción

- Basado en todo lo anterior se darán algunas reglas para ser usadas en los firewalls
- Durante algún tiempo IPv4 e IPv6 coexistirán, así que el escenario más probable será que las redes IPv6 sigan el diseño de las redes IPv4, compartiendo dispositivos de seguridad siempre que sea posible

Consejos (1)

- Ser cuidadoso con el filtrado de ICMPv6 (ver RFC4890)
- Desplegar Ingress filtering (igual que debe hacerse con IPv4)
- Las reglas IPv4 e IPv6 coexistirán, hacerlas coherentes (no permitir todo con IPv6/nada con IPv4).
- Asegurarse de que el firewall soporta:
  - Filtrado por dirección origen y destino
  - Procesado de cabeceras de extensión IPv6 (incluida RH0)
  - Filtrado por información de protocolo de capa superior
  - Inspección de tráfico encapsulado

Consejos (2)

- Considerar el filtrado en tres categorías: Plano de Datos, Plano de Gestión y Plano de Control del Encaminamiento.

5.9 Modelo de Seguridad Distribuida

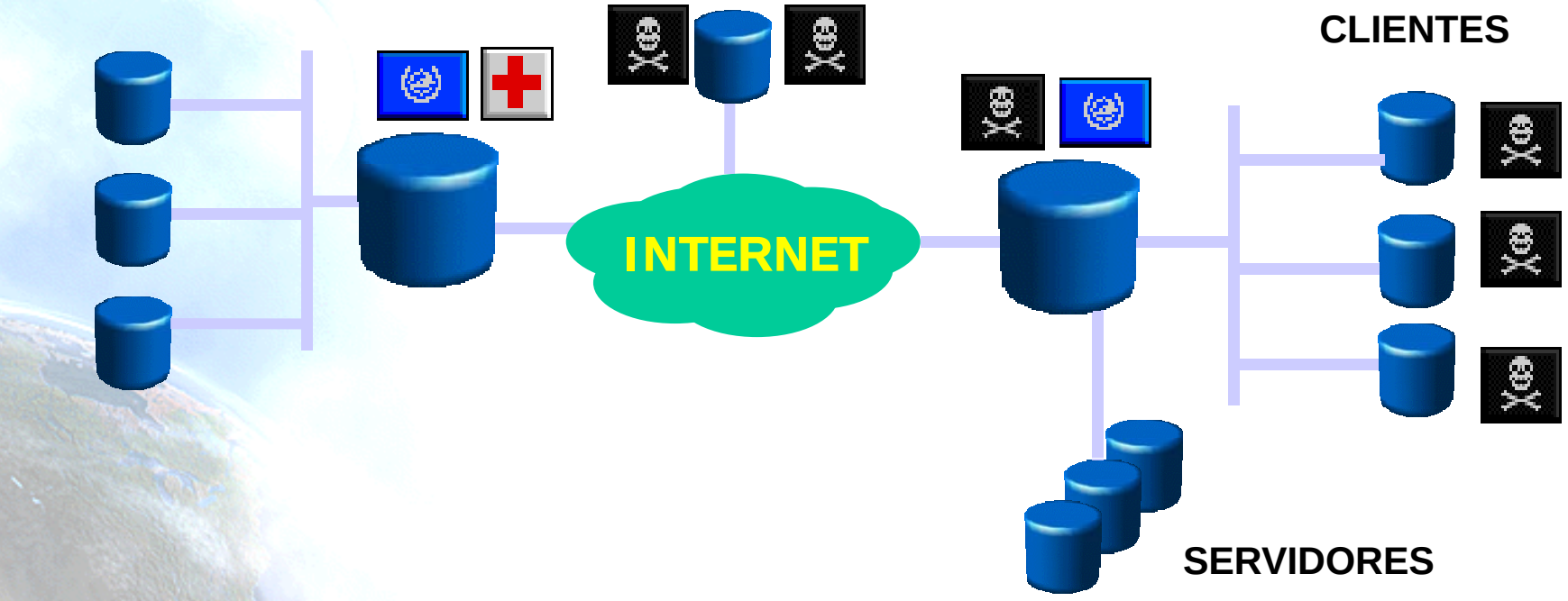
Visión General

- En IPv4 la práctica común es utilizar el **modelo perimetral**, al desplegar seguridad en una red. Este modelo se basa en aislar redes por medio de dispositivos de seguridad a través de los cuales todo el tráfico debe pasar.
- Hoy en día cada vez más herramientas de seguridad se están “moviendo” de la red a los hosts: firewalls, anti-virus, anti-spam, anti-malware, etc.
- Esto conduce al **modelo de seguridad distribuida o de host** en el que la política de seguridad se impone en el host. Esto encaja a la perfección con el modelo extremo-a-extremo que IPv6 ha vuelto a traer.
- También deben tenerse en cuenta los “nuevos” dispositivos IP que usarán las redes IP para conectarse: PDAs, portátiles, domótica, teléfonos móviles, etc. Necesitarán estar protegidos en todas partes!

Consideraciones del Despliegue

- El caso más común es añadir IPv6 a una red IPv4 existente, resultando una red de doble-pila.
- De esta forma nos encontramos con el mismo modelo de seguridad perimetral y dispositivos de seguridad para ser usados en la seguridad IPv6. Esto puede tener algunas ventajas para el personal al cargo y desventajas en caso de falta de soporte IPv6.
- Se espera que en el futuro (próximo) esto cambie debido al despliegue de redes solo IPv6.

Modelo de Seguridad Perimetral (1)

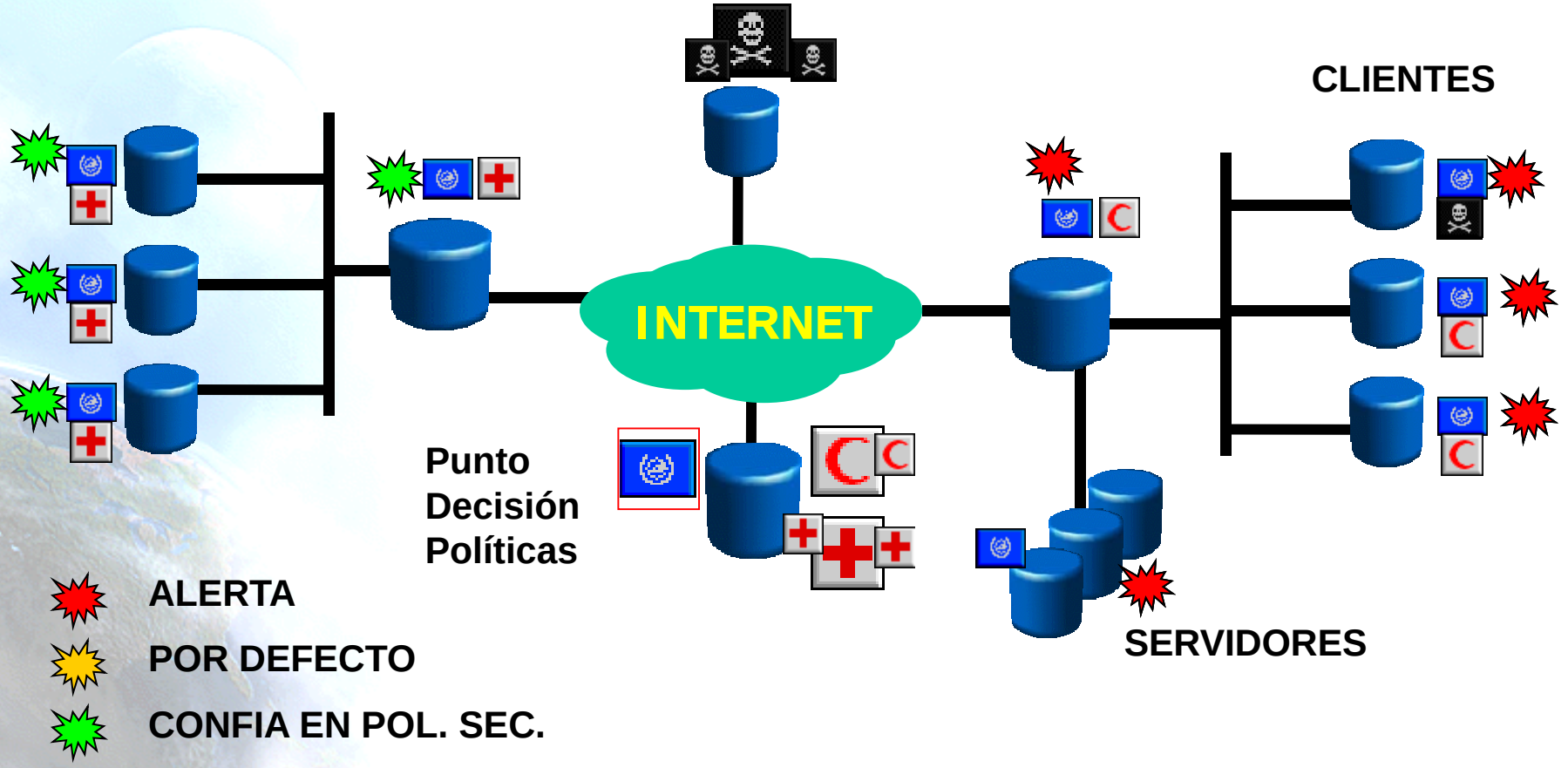


Amenaza Pol. Sec. 1 Pol. Sec. 2 Punto Imposición Política (PIP)

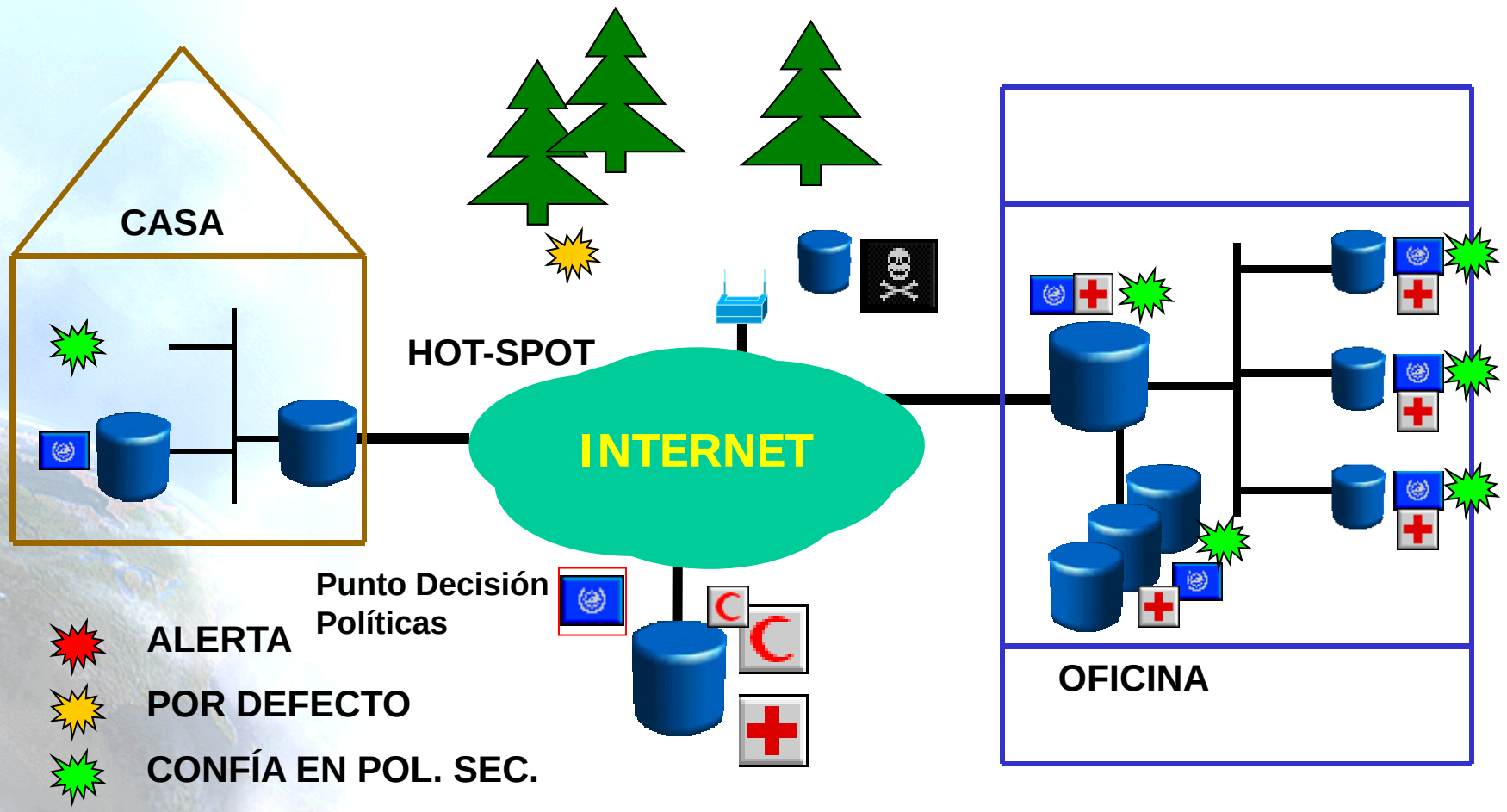
Modelo de Seguridad Perimetral (2)

- La seguridad de un host **depende del punto de la red donde se conecte.**
- **Supuestos principales**:
  - Amenazas vienen de “fuera”.
  - Los nodos protegidos no irán “fuera”.
  - No hay puertas traseras (ADSL, WLAN, etc.).
- **Desventajas principales**:
  - Modelo dependiente del Firewall.
  - No cubre amenazas provenientes de “dentro”.
  - FWs normalmente actúan como NAT/Proxy.
  - Se necesitan soluciones especiales para comunnicaciones seguras en modo transporte.

Modelo de Seguridad Distribuida (1)



Modelo de Seguridad Distribuida (2)



Amenaza Pol. Sec. 1 Pol. Sec. 2 Punto Imposición Política (PIP)

Modelo de Seguridad Distribuida (3)

- **IDEA BÁSICA:** La política de seguridad de define centralmente y de distribuye a los PIPs. Las entidades de red se autentifican para que confíen en ellas.
- **TRES elementos**:
  - Lenguaje de Especificación de Políticas.
  - Protocolo de Intercambio de Políticas.
  - Autentificación de Entidades.
- **Supuestos Principales**:
  - Las amenazas vienen de cualquier parte en la red.
  - Cada host puede ser identificado de forma unívoca y segura.
  - La seguridad se puede aplicar en una o más de las siguientes capas: red, transporte y aplicación.

Modelo de Seguridad Distribuida (4)

- **Desventajas Principales**:
  - Complejidad.
  - Identificación unívoca y segura de hosts no es algo trivial.
  - La actualización de políticas debe llevarse a cabo de una manera eficiente y debe asegurarse que los hosts siguen las políticas.
  - Un host “comprometido” sigue siendo un problema.
  - Es dependiente del Punto de Decisión de Políticas: hay que añadir más complejidad para afrontar esto.

Modelo de Seguridad Distribuida (5)

- **Ventajas principales**:
  - Flexibilidad en la definición de políticas de seguridad
  - Protege contra ataques internos
  - No depende de donde esté conectado el host.
  - Sigue manteniendo un control centralizado.
  - Habilita el modelo de comunicación extremo-a-extremo, tanto seguro como no.
  - Se pueden tomar mejores decisiones basándose en información específica del host.
  - Posibilita una mejor recopilación de información de auditoría.
  - Puede controlar las comunicaciones de un host evitando comportamientos maliciosos en la red local o malas prácticas.
  - Permite desarrollar soluciones de seguridad distribuidas y cooperativas.

Modelo de Seguridad Distribuida(6)

- Existe trabajo en curso que encaja con este modelo:
  1. **Cisco NAC** (Network Access Control): El host debe obtener acceso a la red cumpliendo con una política de seguridad.
  2. **Microsoft NAP** (Network Access Protection): crea políticas para validar la "salud" de un host antes de permitir acceso a la red, actualizar hosts conformes y opcionalmente confinar los host que no cumplan a una red restringida.
  3. **Trusted Network Connect Work Group**: Arquitectura abierta y un conjunto creciente de estándares para la integridad del nodo final.
  4. **IETF NSIS WG**: Trabaja en la dirección de permitir al nodo final, previamente autentificado, a abrir puertos en los firewalls.
  5. **IETF NEA WG**: Revisa el estado de dispositivos finales para monitorizar el cumplimiento de la política de una organización y opcionalmente restringir el acceso hasta que en nodo final se haya actualizado para satisfacer los requisitos.
  6. **IETF IDWG WG** (OLD): define formatos de datos y procedimientos para compartir información de interés a sistema de detección y respuesta de intrusiones, y para sistemas de gestión que pueden necesitar interactuar con ellos.

- El mercado y los estándares parecen ir en la dirección de imponer la política de seguridad en el nodo final por medio del control de acceso a la red.

6. Encaminamiento con IPv6

6.1 Conceptos de Encaminamiento
6.2 RIP
6.3 EIGRP
6.4 OSPF
6.5 IS-IS
6.6 BGP
6.7 Encaminamiento Estático

6.1 Conceptos de Encaminamiento

Visión General Encaminamiento

- Los encaminadores deben saber como llegar al destino final de los paquetes que se le reenvían
- Las rutas estáticas no son adecuadas para redes medianas ni grandes
  - Tampoco para las pequeñas si se producen cambios en la topología de red
- Los protocolos de encaminamiento proporcionan un método automático de generar las tablas de encaminamiento
  - Tienen en cuenta cambio de la topología de red

Tipos de protocolos de encaminamiento

- Atendiendo al ámbito:
  - IGP (Interior Border Gateway)
  - EGP (Exterior Border Gateway)

- En los de tipo IGP
  - Atendiendo a la metodología de propagación
    - Vector Distancia
    - Estado de Link
  - Atendiendo al tipo de rutas que propagan
    - Classful
    - Classless

Criterios de selección IGP

- La selección de uno u otro depende de varios factores:
  - Topología de la intrared
  - Tipos de rutas a propagar
  - Tiempo de convergencia
  - Criterio de cálculo de métricas de la ruta.
  - Escalabilidad
  - Seguridad
- Guía completa en
  - http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2003.htm

Protocolos IGP

	VD	LS	Classful	Classless	Seguridad
RIPv1	X		X		
RIPv2	X			X	
IGRP	X		X		
EIGRP	X			X	X
OSPF		X		X	X
IS-IS		X		X	

Protocolos EGP

- No hay muchas alternativas
- BGP
  - El estándar “de facto”

Encaminamiento IPv6

- Mismo mecanismo CIDR “longest-prefix match” que actualmente en IPv4
- Cambios mínimos respecto de los protocolos existentes para encaminado en IPv4 (gestión de direcciones mayores)
  - Unicast: **RIP, OSPF, IS-IS, BGP4+, …**
  - Multicast: **MOSPF, PIM, …**
- Se puede utilizar la cabecera de routing con direcciones unicast para encaminar paquetes a través de regiones concretas
  - Por ejemplo, para la selección de proveedores, políticas, prestaciones, etc.

6.2 RIP

RIP IPv6

- RIP para IPv6 o RIPng esta definido en el RFC2080: RIPng for IPv6
- Extiende RIPv1 y RIPv2 para soportar
  - Direcciones de 128 bits
  - Encaminamiento de prefijos IPv6
  - Uso de la dirección FF02::9, del grupo multicast all-RIP-routers, como la dirección destino de los mensajes de update de RIP

6.3 EIGRP

EIGRP IPv6

- Enhanced Interior Gateway Routing Protocol (EIGRP) desarrollado por Cisco es una versión mejorada del IGRP
- EIGRP usa al igual que IGRP el algoritmo de vector de distancias e información de distancia, además de usar algunas características asociadas normalmente con los protocolos del estado de enlace
- Las propiedades de convergencia y la eficiencia operativa son mejores en EIGRP que en IGRP
- EIGRP para IPv4 se ejecuta sobre transporte IPv4, comunica solo peers IPv4 y anuncia solo rutas IPv4, mientras que EIGRP para IPv6 hace lo mismo pero para IPv6
- EIGRP para IPv4 y EIGRP para IPv6 se configuran y gestionan de manera separada, aunque la configuración es similar en ambos casos

- EIGRP para IPv6 esta soportado desde las versiones de IOS 12.4(6)T y 12.2(33)SRB

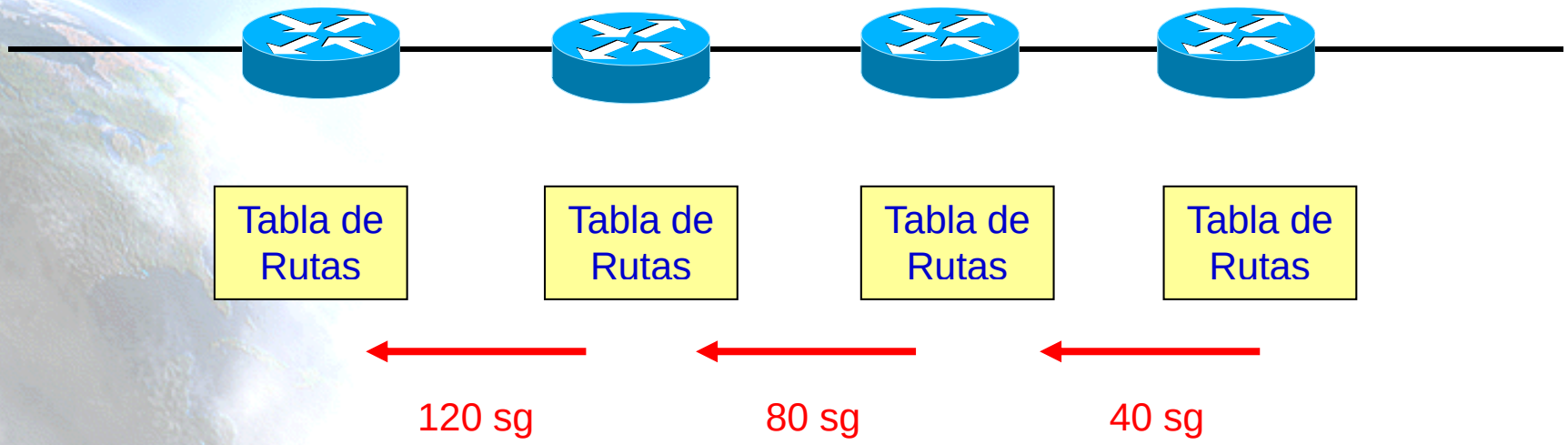
6.4 OSPF

Visión General OSPF (1)

- Protocolo de encaminamiento IGP de tipo “link-state” que intenta dar solución a las necesidades más avanzadas de los Sistemas Autónomos más exigentes:
  - soporte VLSM (Variable Length Subnet Masking)
  - autenticación
  - rápida convergencia cuando se producen cambios en la topología de la red
  - propagación de rutas por medio de multicast
  - marcado de rutas aprendidas de protocolos EGP
  - consideración del ancho de banda en la elección de la mejor ruta
  - etc.
- Los encaminadores conocen la topología de la red por medio del algoritmo SPF

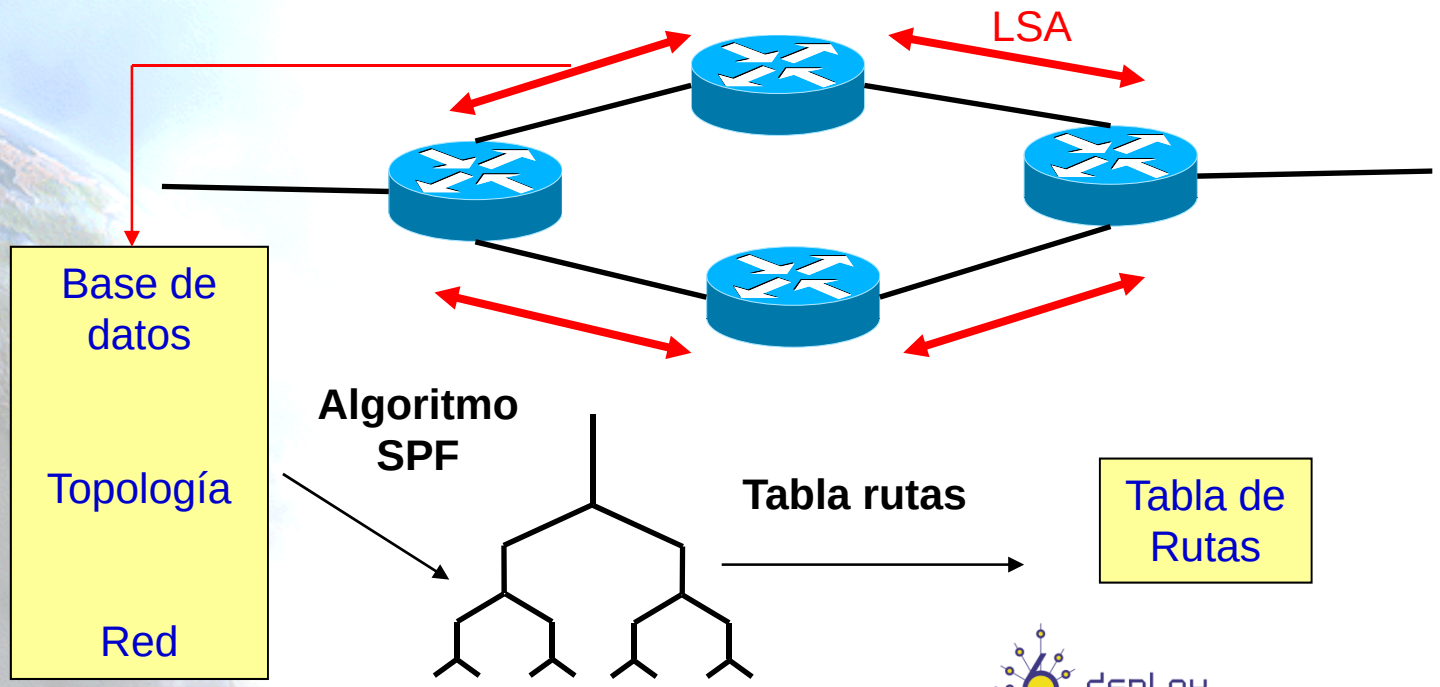
Visión General OSPF (2)

- Los protocolos basados en DV (Distance Vector) envían periódicamente a sus vecinos la tabla de ruta
  - Problemas de ancho de banda
  - Problemas de tiempo de convergencia



Visión General OSPF (3)

- Los protocolos basados en LS (Link-State) solo envían los cambios en los LSA (Link-State Advertisements)
  - Menor ancho de banda
  - Convergencia más rápida
  - Soporta mayores redes



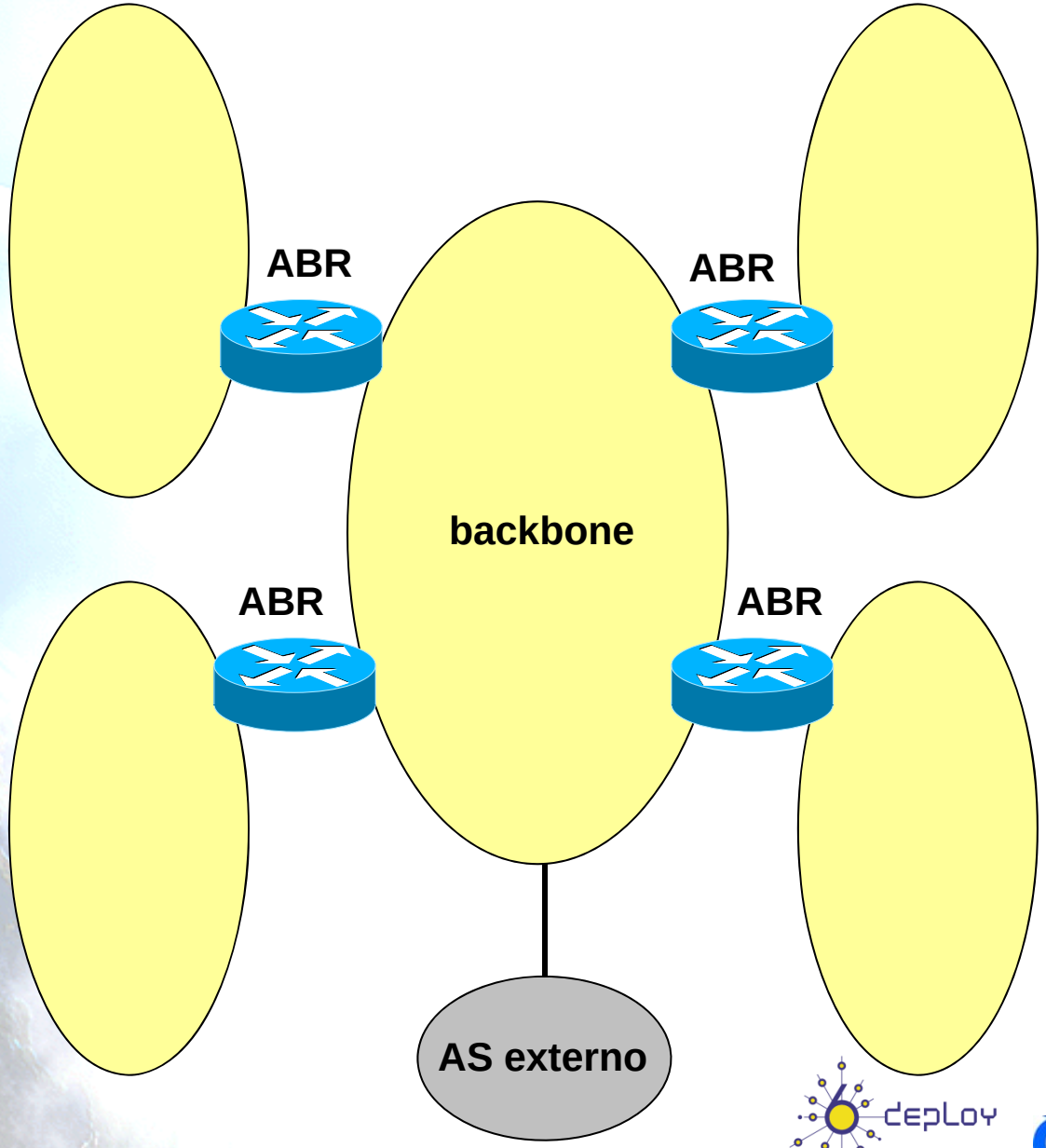
Visión General OSPF (4)

- OSPF utiliza el protocolo Hello para:
  - Determinar qué interfaces recibirán los LSAs
  - Determinar qué otros encaminadores vecinos existen
  - Determinar si los encaminadores vecinos siguen activos (keepalive)
- Los encaminadores envían LSAs (Link-State Advertisements) a todos los encaminadores de la misma unidad jerárquica por medio de una dirección multicast e incluyen entre otros:
  - Prefijo de red
  - Máscara de red
  - Tipo de red
  - Encaminadores conectados
  - Etc.
- Todos construyen la misma base de datos topológica a partir de los LSAs recibidos
  - Se obtiene la nueva tabla de rutas a partir de la nueva topología.

Visión General OSPF (5)

- La métrica de OSPF se calcula como la suma del coste de atravesar diversos nodos hasta el destino final
  - se calcula basándose en el ancho de banda de las interfaces y es configurable por el usuario.
- OSPF divide el AS en pequeñas unidades jerárquicas, cada una de las cuales se conecta al “backbone” por medio de un ABR (Area Border Router)
  - Reduce la carga de procesamiento y memoria

Visión General OSPF (6)



Visión General OSPF (7)

- Los LSAs describen la topología de un área jerárquica
- Existen diversos tipos

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router
2	Network LSA	Interface IP address of the DR
3	Network summary LSA	Destination network number
4	ASBR summary LSA	Router ID of AS boundary router
5	AS external LSA	External network number
7	NSSA external LSA	External network number

OSPF IPv6 (1)

- La versión 3 OSPF, para IPv6 (RFC2740), extiende la versión 2 de OSPF (RFC2328) para soportar el encaminamiento de prefijos IPv6 y las direcciones de 128 bits
  - Muchas de las características de OSPF para IPv6 son las mismas que OSPFv2
  - En OSPF para IPv6 no es necesario crear explícitamente un proceso de encaminamiento. Al habilitar OSPF para IPv6 en un interfaz se creará el proceso de encaminamiento, así como su configuración asociada
  - En OSPF para IPv6 cada interfaz debe de habilitarse usando los comandos en el modo de configuración de interfaz. Esto es distinto de OSPFv2, donde cada interfaz se habilita indirectamente usando de modo de configuración del router
  - En IPv6 se pueden configurar muchos prefijos en una interfaz. Así que en OSPF IPv6, todos los prefijos de una interfaz se incluyen por defecto; es decir que no es posible seleccionar algunos de los prefijos para ser importados dentro de OSPF IPv6: se importan o todos o ningún prefijo de la interfaz
  - A diferencia de OSPFv2, se pueden ejecutar múltiples instancias de OSPF para IPv6 en un link
  - En redes NMBA (Non-Broadcast Multi-Access networks) (punto-multipunto) no se detectan automáticamente los encaminadores vecinos sino que hay que especificarlos manualmente

OSPF IPv6 (2)

- Puesto que en IPv6 una interfaz de red puede tener más de una dirección, los LSAs en OSPFv3 difieren de los de la versión para IPv4

Código	LSA	Link-State ID
1	Router LSA	Originating router ID of the router. En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
2	Network LSA	Interface IP address of the DR En IPv6 no tienen información de la dirección de red y son independientes del protocolo de red.
3	Interarea-prefix LSAs for ABRs	Destination network number. En IPv6 se expresa como prefijo, longitud de prefijo.
4	Interarea-router LSAs for ASBRs	Router ID of AS boundary router
5	Autonomous system external LSAs	Redistributing routes from another AS. En IPv6 se expresa como prefijo, longitud de prefijo y la ruta por defecto, de longitud 0.
8	Link LSA	Local-link flooding scope. Informa de las direcciones link-local de todos los encaminadores del segmento de red
9	Intra-Area-Prefix LSA	Describes association to the router LSA.

Diferencias entre OSPFv3 - OSPFv2 (1)

- El funcionamiento es por link, no por subred IP
  - –Los términos “red” y “subred” usados en OSPF IPv4 deben en general cambiarse por “link”
- Eliminación de la semántica de direccionamiento
  - –Se ha eliminado la semántica de direccionamiento (addressing semantics) de los paquetes OSPF y de los principales tipos de LSA, dejando un núcleo independiente del protocolo de red
- Adición del Flooding scope
  - –El Flooding scope para los LSAs se ha generalizado y ahora esta codificado explícitamente en el LS type field de los LSAs. Así ahora existen tres flooding scopes para los LSAs: Link-local, Area y AS scope

Diferencias entre OSPFv3 - OSPFv2 (2)

- Soporte explicito de múltiples instancias por link
  - –Esto podría usarse en un segmento de un NAP compartido entre varios proveedores – estos podrían ejecutar separadamente varios dominios de ruteo OSPF aun cuando tuvieran uno o mas segmentos de red físicos (o links) en común
  - –Se logra mediante un "Instance ID" contenido en las cabeceras de los paquetes OSPF
  - –En OSPFv2 esto se hace de manera más complicada con el campo de autenticación en la cabecera de OSPF para IPv4
- Uso de direcciones link-local
  - –OSPFv3 asume que cada router tiene asignadas direcciones unicast link-local en cada interfaz física

Diferencias entre OSPFv3 - OSPFv2 (3)

- Autenticación
  - –En OSPFv3 la autenticación se ha eliminado del paquete OSPF en si
  - –Los campos "AuType" y "Authentication" se han eliminado de la cabecera del paquete de OSPF, y todos los campos relacionados con autenticación se han eliminado de las estructuras de áreas e interfaces
  - –OSPFv3 usa las cabeceras de IP Authentication e IP Encapsulating Security Payload para asegurar la integridad, autenticación y confidencialidad en el intercambio de rutas

Diferencias entre OSPFv3 - OSPFv2 (4)

- Cambio del formato del paquete OSPF
  - –OSPFv3 se ejecuta directamente sobre IPv6
  - –Se ha eliminado la semántica de direccionamiento (addressing semantics) de las cabeceras OSPF y de los LSAs de Router y Network LSA, dejando un núcleo independiente del protocolo de red
  - –Toda la información de direccionamiento esta ahora contenida en nuevos LSAs específicos para distribuir la información de las direcciones IPv6 y de los datos necesarios para la resolución del next hop

6.5 IS-IS

Visión General IS-IS (1)

- IS-IS es un protocolo de encaminamiento OSI
- Diseñado para soportar el protocolo CLNP
  - Protocolo de la capa de red similar a IP
- Se ha extendido para soportar también IPv4 y IPv6 (RFC5308)

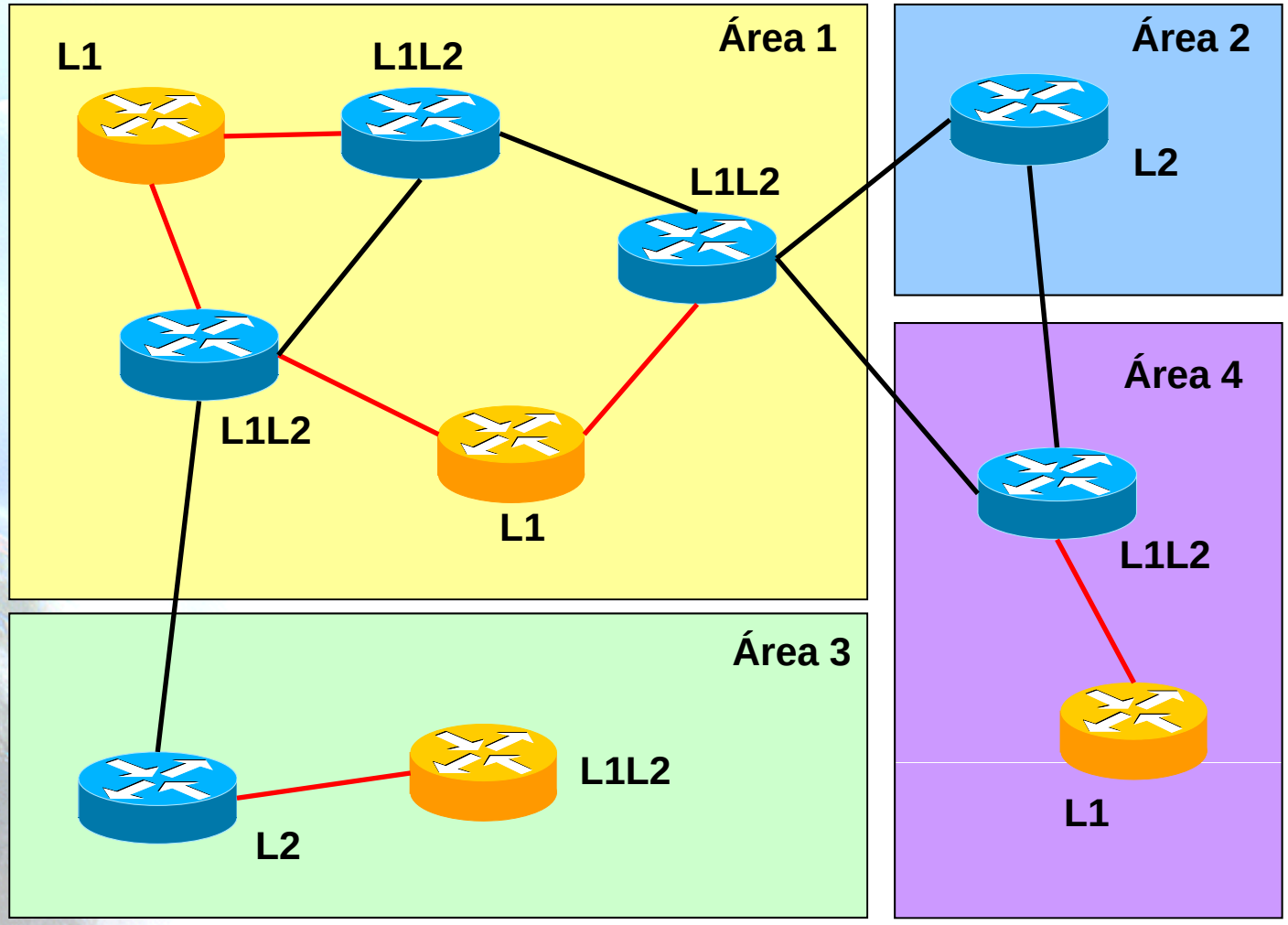
Visión General IS-IS (2)

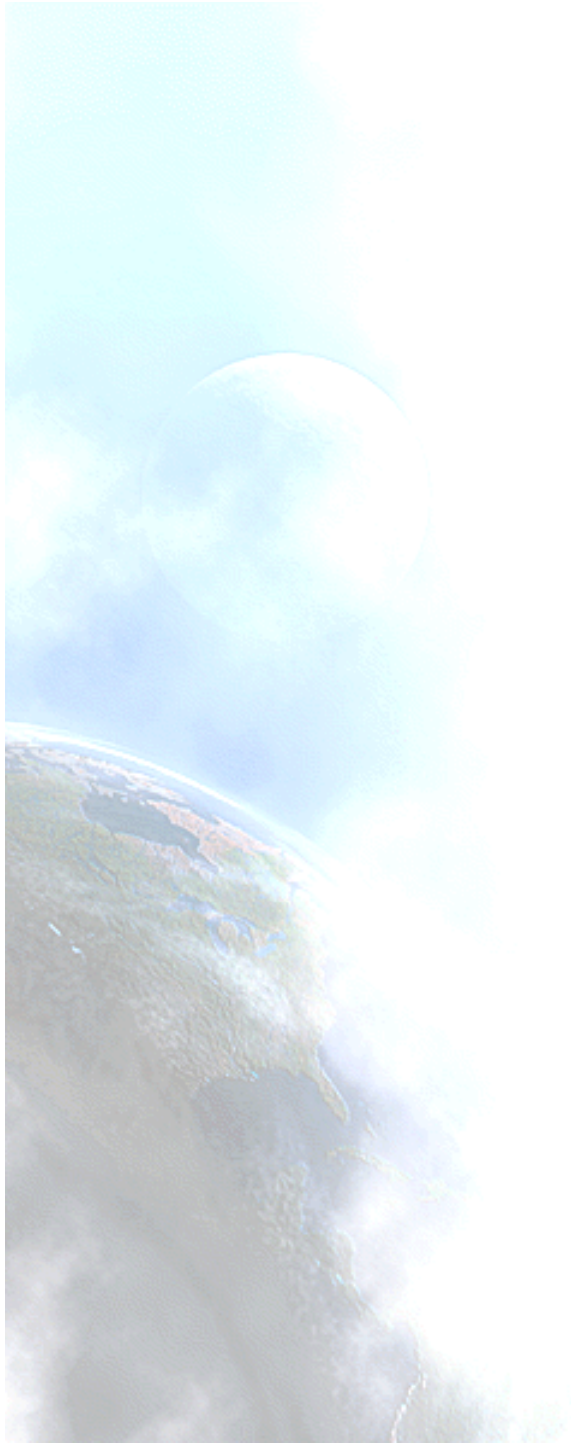
- Características
  - Encaminamiento jerárquico
  - Soporte “classless”
  - Uso de direcciones multicast
  - Autenticación mediante password
  - Soporte de múltiples métricas
  - Cálculo SPF local

Visión General IS-IS (3)

- Similitudes con OSPF
  - Mantienen una base de datos topológica con los mensajes recibidos (LSAs en OSPF y LSPs en ISIS)
  - Ejecutan el algoritmo SPF
  - Los dos usan áreas para formar una topología de red de dos niveles jerárquicos
  - Ambos soportan rutas “classless” y pueden resumir rutas entre áreas
- Diferencias con OSPF
  - Se define dos niveles jerárquicos
    - Nivel 2: Encaminadores del backbone
    - Nivel 1: Encaminadores de área
  - ISIS no requiere de un “backbone” central
  - En ISIS el “backbone” es realmente un conjunto de encaminadores de nivel 2 contiguos
  - Los bordes que definen las áreas están sobre los enlaces entre los encaminadores, no dentro de ellos como en OSPF

Visión General IS-IS (4)



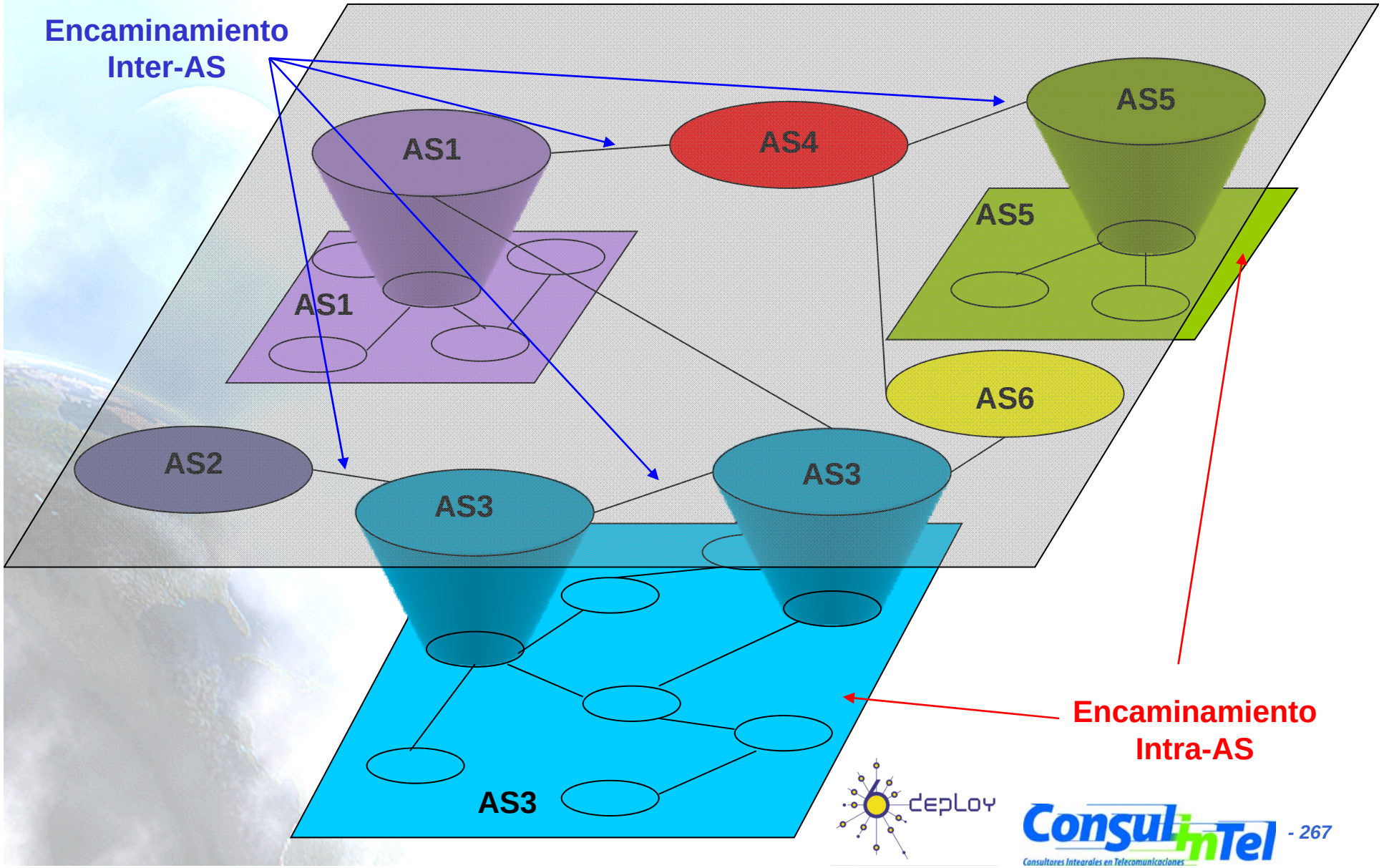


6.6 BGP

Visión General de BGP (1)

- El encaminamiento en Internet se hace a dos niveles
  - Intra-AS => IGP
    - La gestión de cada AS es local, lo cual incluye el tipo de protocolo de encaminamiento usado
  - Inter-AS => EGP
    - Requiere una estandarización para que todos los ASs sean alcanzados por todos.
      - BGP estándar “de facto”

Visión General de BGP (2)



Visión General de BGP (3)

- BGP “Border Gateway Protocol”
  - estándar “de facto”
- Se basa en el PVP (Path Vector Protocol)
  - Similar al Distance Vector
  - Cada encaminador frontera envía a sus vecinos (“peerings”) la ruta completa a un destino, no solo la distancia
  - El camino (path) es una secuencia de ASs hasta el destino
    - Ejemplo: Path(X,Z)=X, Y1, Y2, Y3, Y5, Z

Visión General de BGP (4)

- Path Vector Protocol
  - El encaminador X envía su ruta a Z a su vecino W
  - Si W la acepta, entonces P(W,Z)=X, Path(X,Z)
  - W puede no aceptar dicha ruta
    - Para evitar bucles cerrados
    - Por razones de coste de tráfico
    - Por violación de politicas internas del AS
    - Etc.
- Se puede controlar el tráfico que entra en la red anunciando o no el AS a los vecinos
- Si X no quisiera encaminar tráfico de Z, basta con no anunciar las rutas de Z

Visión General de BGP (5)

- Se utiliza TCP para el intercambio de mensajes BGP
  - OPEN – abre una conexión TCP
  - UPDATE – anuncia o confirma un nuevo camino
  - KEEPALIVE – en ausencia de UPDATES sirve para mantener abierta la conexión TCP y como ACK de un mensaje OPEN
  - NOTIFICATION – informa de errores en mensajes precedentes y para cerrar conexiones

Visión General de BGP (6)

- Atributos del “path”
  - “bien conocidos” – son reconocidos por todos los encaminadores y se pasan a los vecinos
    - Obligatorios y se incluyen en los mensajes UPDATE
  - opcionales – no hay obligación de que los conozcan todas las implementaciones BGP

BGP para IPv6 (BGP4+) (1)

- La versión actual de BGP es la versión 4, i.e. BGP4
  - –BGP4 (BGP para IPv4) se describe en RFC4271
- Las Extensiones Multiprotocolo para BGP, i.e. BGP4+, permiten usar BGP4 con diferentes familias de direcciones (address family), tales como IPv6 y Multicast
  - –Extensiones multiprotocolo para BGP (BGP para IPv6) se describen en RFC4760
    - •Define la extensiones para BGP necesarias para manejar informacion de ruteo sobre distintos protocolos de nivel de red (e.g., IPv6, IPX, L3VPN, etc.)

BGP para IPv6 (BGP4+) (2)

- Las extensiones multiprotocolo para BGP para IPv6 soportan las mismas funcionalidades y características que BGP para IPv4
  - –Las extensiones para IPv6 incluyen el soporte para
    - •La familia de direcciones IPv6 (IPv6 address family) y la network layer reachability information (NLRI)
    - •El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6

- Las extensiones multiprotocolo para BGP para IPv6 Multicast soportan las mismas funcionalidades y características que BGP para IPv4 Multicast
  - –Las extensiones para IPv6 Multicat incluyen el soporte para
    - •La familia de direcciones IPv6 Multicast (IPv6 Multicast address family) y la network layer reachability information (NLRI)
    - •El atributo de next hop (el router siguiente en el camino hacia el destino), que ahora usa direcciones iPv6 Multicast

Características de BGP4+ (1)

- Los únicos componentes de información de BGP que son específicos para IPv4 son los atributos
  1. NEXT_HOP (expresado como una direcion IPv4)
  2. AGGREGATOR (contiene una direcion IPv4)
  3. NLRI (expresado como prefijos de direciones IPv4)
- RFC4760 asume que cualquier router BGP (incluyendo los que soportan el mismo RFC4760) tiene una dirección IPv4 (la cual se usará, entre otras cosas en el atributo de AGGREGATOR)
- Así para habilitar en BGP4 el soporte de ruteo para múltiples protocolos de nivel de red, los dos únicos componentes que hay que agregar a BGP son
  1. La habilidad para asociar un protocolo de red particular con la información del next hop
  2. La habilidad para asociar un protocolo de red particular con la network layer reachability information (NLRI)
- Para identificar un protocolo de red particular asociado con la informacion del next hop y la semantica del NLRI, el RFC4760 usa una combinacion de
  - Una Address Family, como esta definida en “IANA's Address Family Numbers registry“ (**http://www.iana.org/numbers.html**), y
  - Una Subsequent Address Family, como esta descrita en el mismo RFC4760

Características de BGP4+ (2)

- Para proveer compatibilidad con versiones anteriores, así como para simplificar la introducción de las capacidades multiprotocolo en BGP4, el RFC4760 define dos nuevos atributos
  - –Multiprotocol Reachable NLRI (MP_REACH_NLRI), contiene la información de los destinos alcanzables, asi como la información de next hop usada para hacer el reenvió (forwarding) hacia esos destinos
  - –Multiprotocol Unreachable NLRI (MP_UNREACH_NLRI), contiene la información de los destinos inalcanzables
- Ambos atributos son opcionales y no-transitivos
  - –Es decir, un router BGP que no soporta la extensiones multiprotocolo ignorara la información llevada en estos atributos y no la pasará a otros routers BGP

6.7 Encaminamiento Estático

Configuración Rutas Estáticas

- La forma de configurar rutas estáticas es similar a IPv4
  - Default gateway
  - Delegación de prefijos

7. Mecanismos de Transición

7.1 Conceptos de Transición
7.2 Doble Pila
7.3 Túneles
7.4 Tunnel Broker
7.5 6to4
7.6 Teredo
7.7 Softwires
7.8 Traducción
7.9 Seguridad

7.1 Conceptos de Transición

Técnicas de Transición / Coexistencia

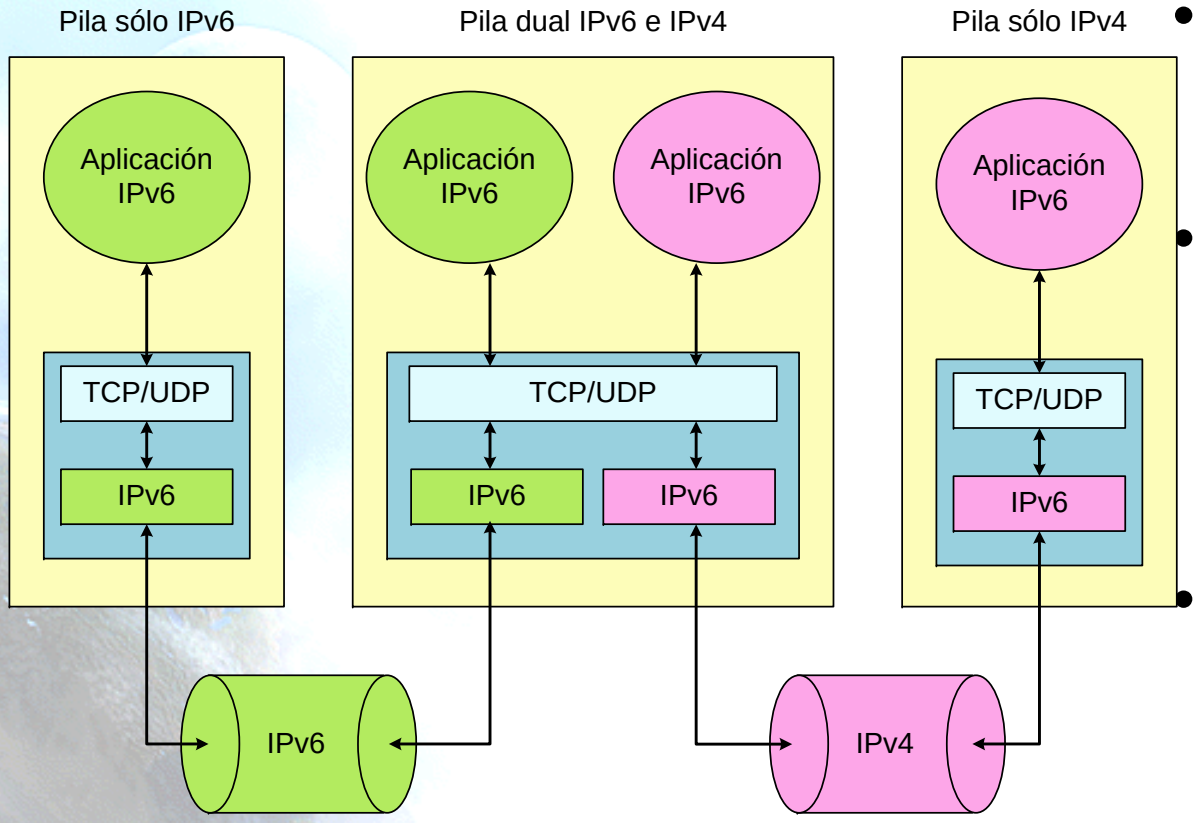
- IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4.
- Coexistirán durante décadas -> No hay un “día D”
- Se han identificado e implementado un amplio abanico de técnicas, agrupadas básicamente dentro de tres categorías:
  1) **Doble-pila**, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.
  2) **Técnicas de túneles**, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más común.
  3) **Técnicas de traducción**, para permitir la comunicación entre dispositivos que son sólo IPv6 y aquellos que son sólo IPv4. Debe ser la última opción ya que tiene problemas.
- Todos estos mecanismos suelen ser utilizados, incluso en combinación.

7.2 Doble Pila

Doble Pila (1)

- Al añadir IPv6 a un sistema, no se elimina la pila IPv4
  - Es la misma aproximación multi-protocolo que ha sido utilizada anteriormente y por tanto es bien conocida (AppleTalk, IPX, etc.)
  - Actualmente, IPv6 está incluido en todos los Sistemas Operativos modernos, lo que evita costes adicionales
- Las aplicaciones (o librerías) escogen la versión de IP a utilizar
  - En función de la respuesta DNS:
    - si el destino tiene un registro AAAA, utilizan IPv6, en caso contrario IPv4
  - La respuesta depende del paquete que inició la transferencia
- Esto permite la coexistencia indefinida de IPv4 e IPv6, y la actualización gradual a IPv6, aplicación por aplicación.

Doble pila (2)



Mécanismo basado en doble pila

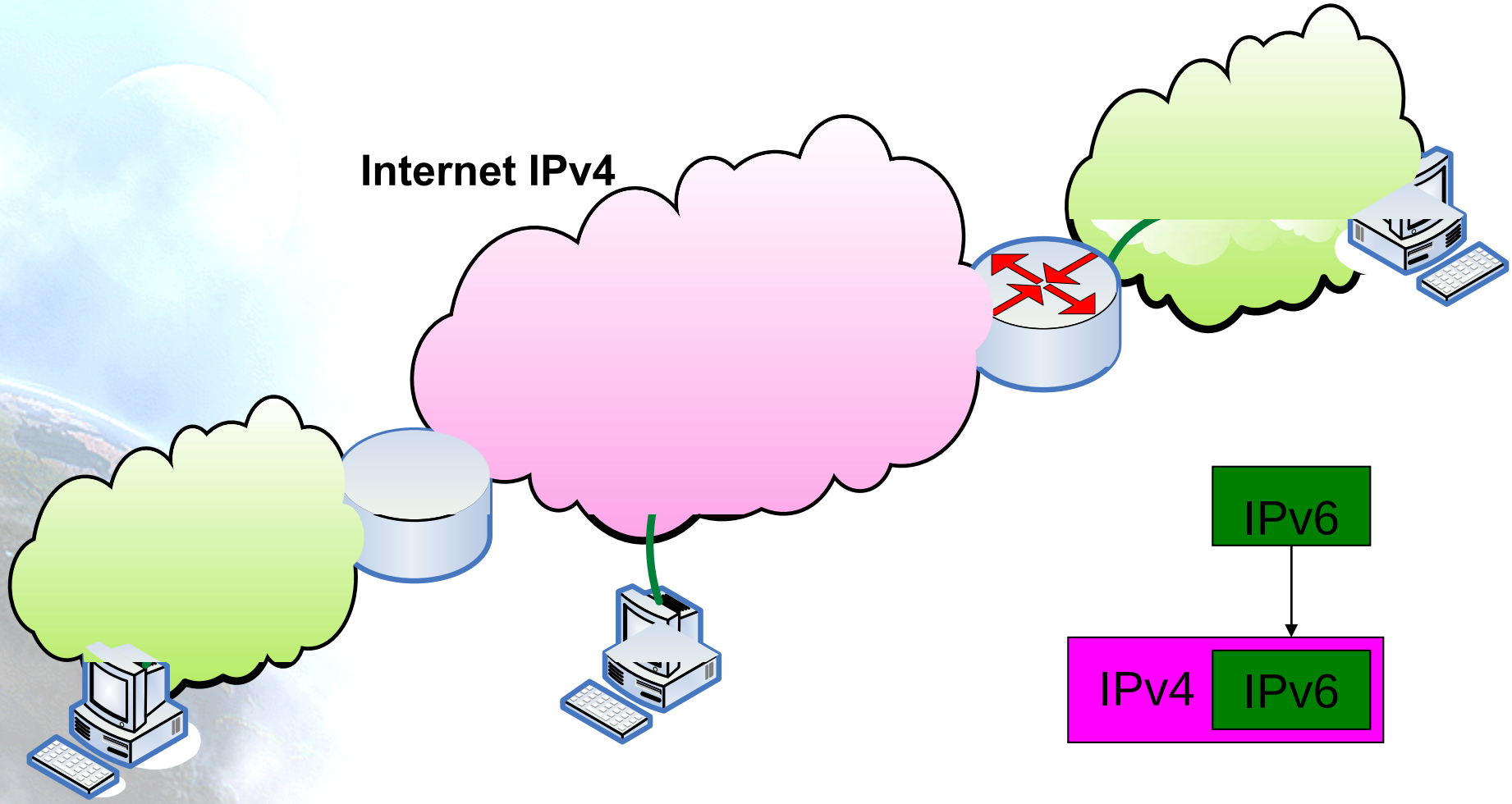
- Los nodos tienen implementadas las pilas IPv4 e IPv6
- Comunicaciones con nodos solo IPv6 ==> Pila IPv6, asumiendo soporte IPv6 en la red
- Comunicaciones con nodos solo IPv4 ==> Pila IPv4

7.3 Túneles

Túneles para Atravesar Routers que no Reenvían IPv6

- Encapsulamos paquetes IPv6 en paquetes IPv4 para proporcionar conectividad IPv6 en redes que solo tiene soporte IPv4
- Muchos métodos para establecer dichos túneles:
  - configuración manual -> 6in4
  - "tunnel brokers" (tipicamente con interfaces web) -> 6in4
  - "6-over-4" (intra-domain, usando IPv4 multicast como LAN virtual)
  - "6-to-4" (inter-domain, usando la dirección IPv4 como el prefijo del sitio IPv6)
- Puede ser visto como:
  - IPv6 utilizando IPv4 como capa de enlace virtual link-layer, o
  - una VPN IPv6 sobre la Internet IPv4

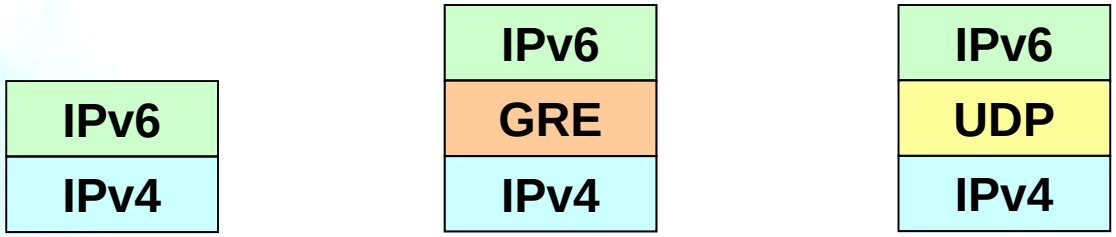
Túneles IPv6 en IPv4 (6in4) (1)



Mécanismo basado en túneles

Túneles 6in4 (2)

- Existen diversas formas de encapsular los paquetes IPv6:



- Lo mismo se aplica para IPv4 usado en redes solo IPv6.

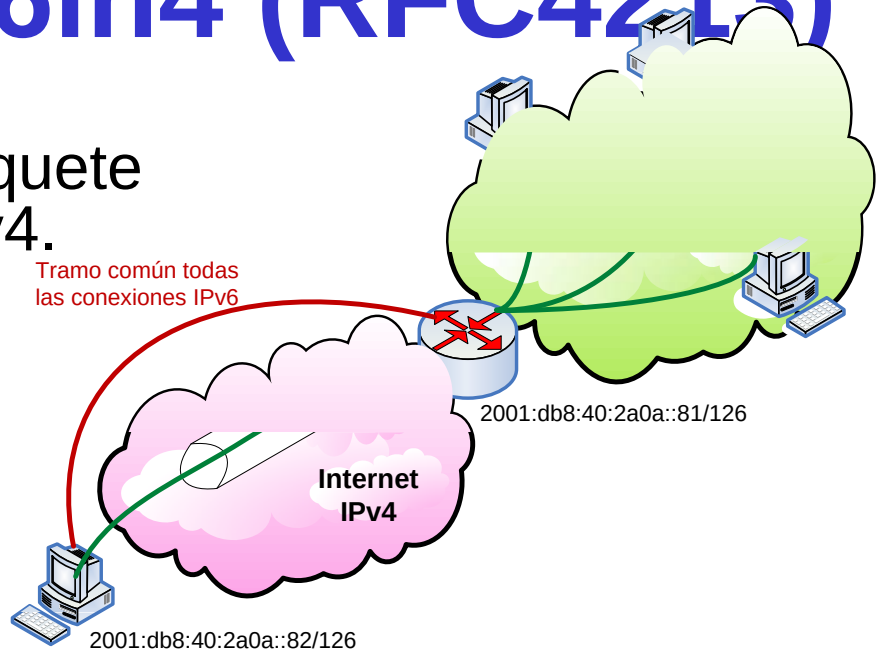
Túneles 6in4 (3)

- Algunos mecanismos de transición basados en túneles
  - 6in4 (*) [6in4]
  - TB (*) [TB]
  - TSP [TSP]
  - 6to4 (*) [6to4]
  - Teredo (*) [TEREDO], [TEREDOC]
  - Túneles automáticos [TunAut]
  - ISATAP [ISATAP]
  - 6over4 [6over4]
  - AYIYA [AYIYA]
  - Silkroad [SILKROAD]
  - DSTM [DSTM]
  - Softwires (*) [SOFTWIRES]

- (*) Más habituales y explicados en detalle a continuación

Detalles Túneles 6in4 (RFC4213)

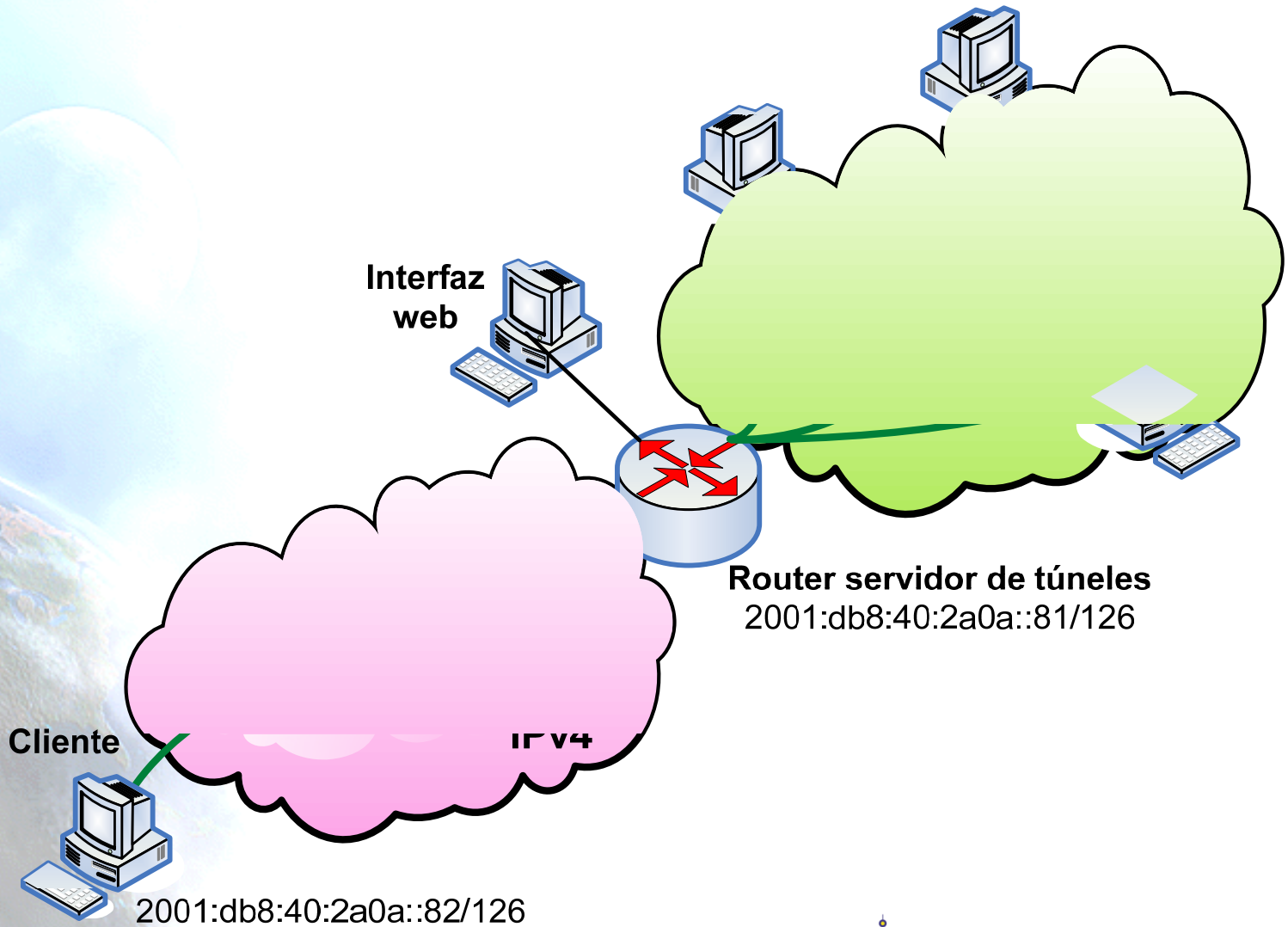
- Encapsula directamente el paquete IPv6 dentro de un paquete IPv4.
- Se suele hacer entre
  - nodo final ==> router
  - router ==> router



- Aunque también es posible para
  - nodo final ==> nodo final
- El túnel se considera como un enlace punto-a-punto desde el punto de vista de IPv6.
  - Solo un salto IPv6 aunque existan varios IPv4.
- Las direcciones IPv6 de ambos extremos del túnel son del mismo prefijo.
- Todas las conexiones IPv6 del nodo final siempre pasan por el router que está en el extremo final del túnel.
- Los túneles 6in4 pueden construirse desde nodo finales situados detrás de NAT
  - La implementación de NAT debe soportar “proto-41 forwarding” [PROTO41] para permitir que los paquetes IPv6 encapsulados atraviesen el NAT.

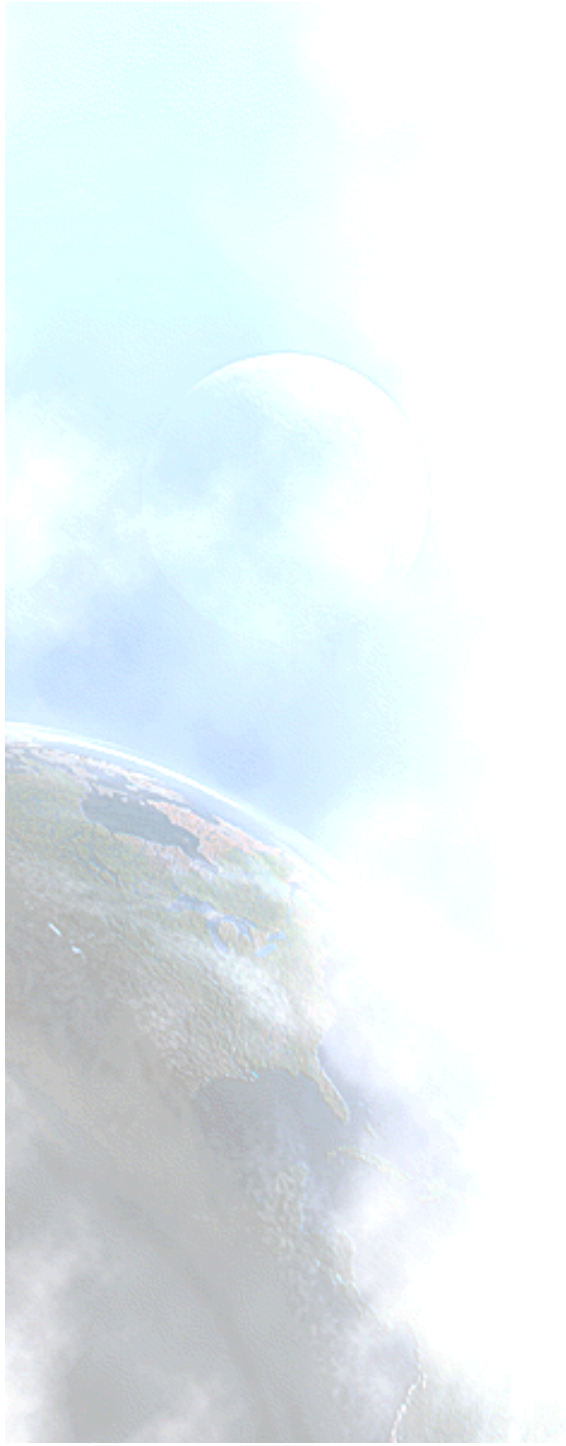
7.4 Tunnel Broker

Tunnel Broker (RFC3053) (1)



Tunnel Broker (RFC3053) (2)

- Los túneles 6in4 requieren la configuración manual de los equipos involucrados en el túnel
- Para facilitar la asignación de direcciones y creación de túneles IPv6, se ha desarrollado el concepto de Tunnel Broker (TB).
  - Es un intermediario al que el usuario final se conecta, normalmente con un interfaz web
- El usuario solicita al TB la creación de un túnel y este le asigna una dirección IPv6 y le proporciona instrucciones para crear el túnel en el lado del usuario
- El TB también configura el router que representa el extremo final del túnel para el usuario
- En http://www.ipv6tf.org/using/connectivity/test.php existe una lista de TB disponibles
- TSP [TSP] es un caso especial de TB que no esta basado en un interfaz web sino en un aplicación cliente que se instala el cliente y se conecta con un servidor, aunque el concepto es el mismo.

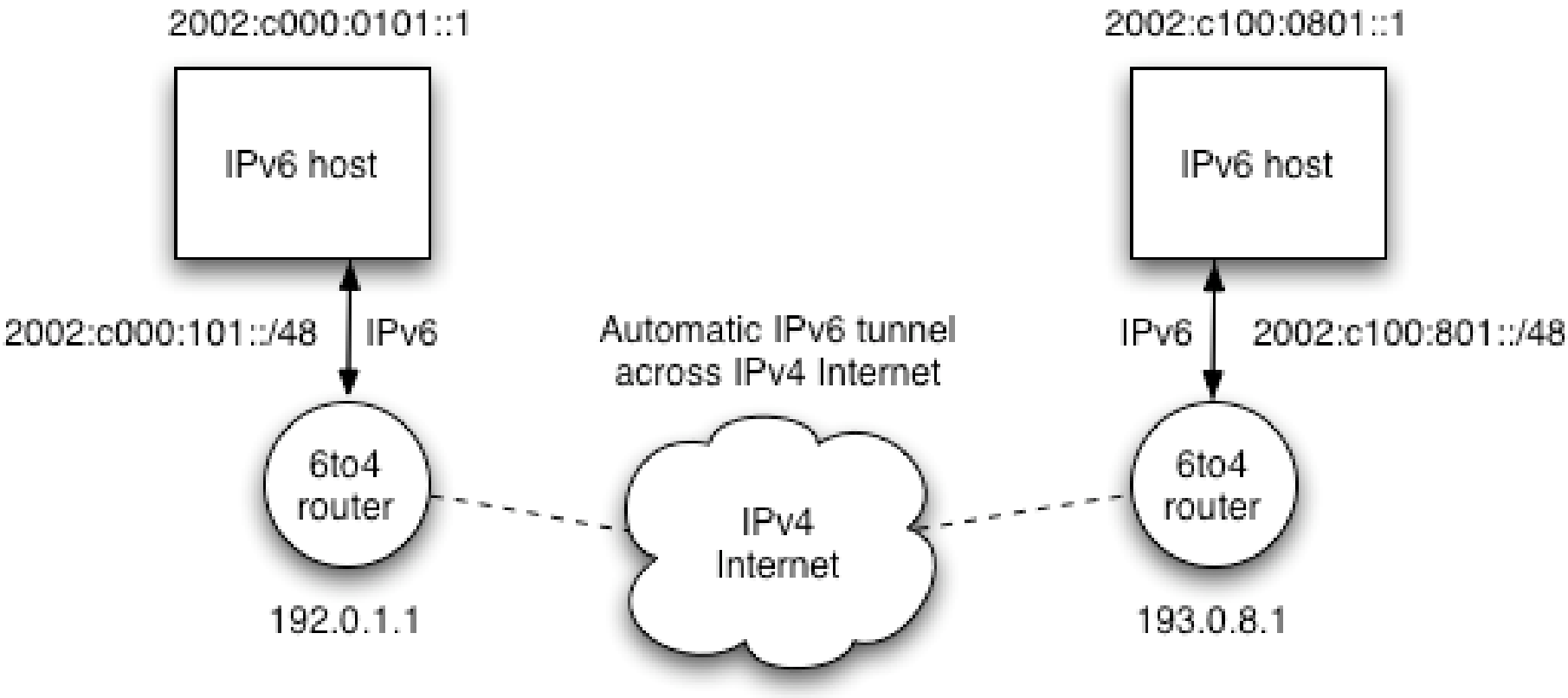


7.5 6to4

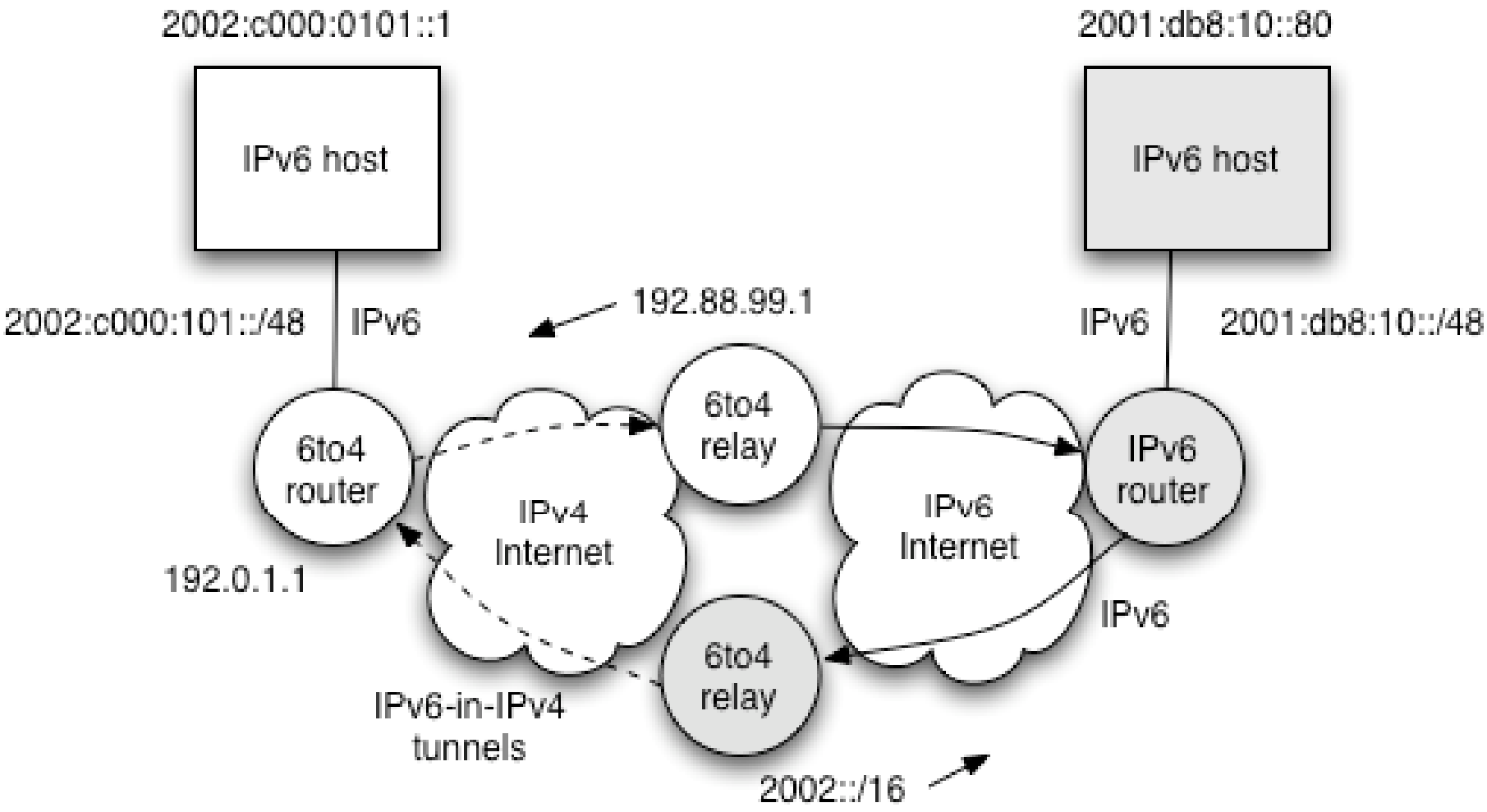
Túneles 6to4 (1)

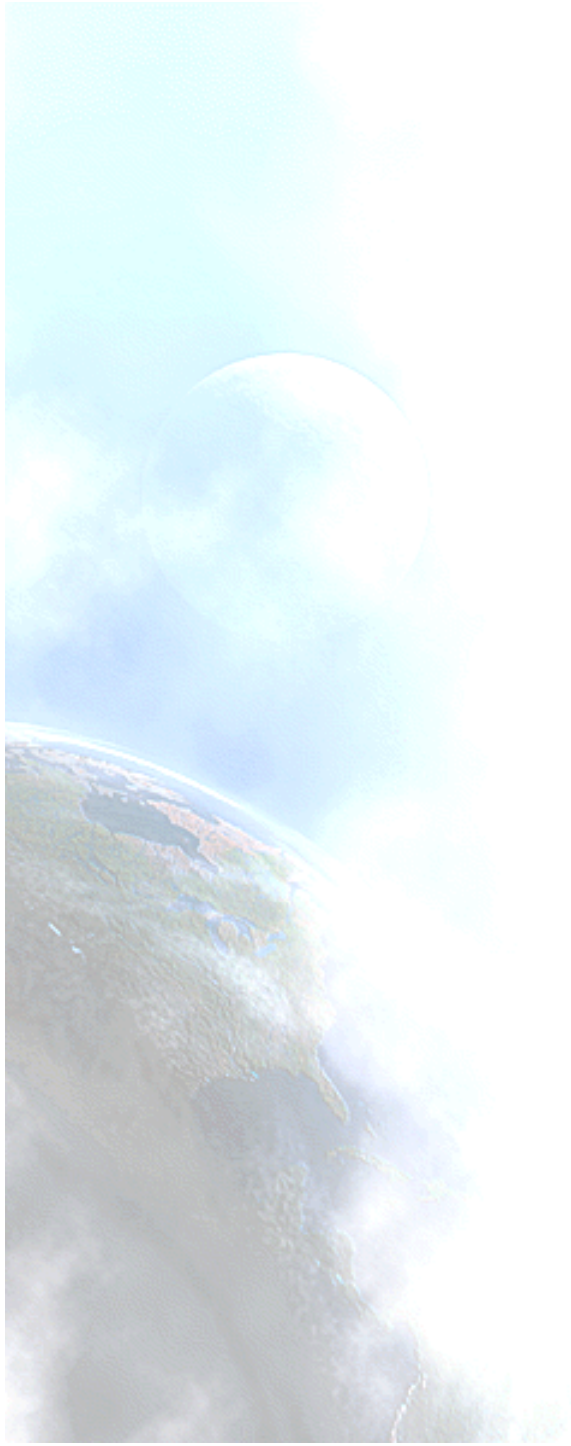
- Definido en RFC3056
- Se utiliza un “truco” para proporcionar direcciones 6to4.
  - Prefijo 6to4: 2002::/16
  - Se usa la IPv4 pública (p.e. 192.0.1.1) para siguientes 32 bits
  - Se obtiene así un prefijo /48 (p.e. 2002:C000:0101::/48)
- Cuando un router 6to4 ve un paquete hacia el prefijo **2002::/16** lo encapsula en IPv4 hacia la IPv4 pública que va en la dirección
- Sigue faltando una cosa: ¿Cómo enviar paquetes hacia una IPv6 “normal”? **Relay 6to4**
- El Relay 6to4 se anuncia mediante:
  - Dirección **IPv4 anycast conocida**: 192.88.99.1 (RFC3068)
  - Prefijo 6to4 (2002::/16)

Túneles 6to4 (2)



Túneles 6to4 (3)



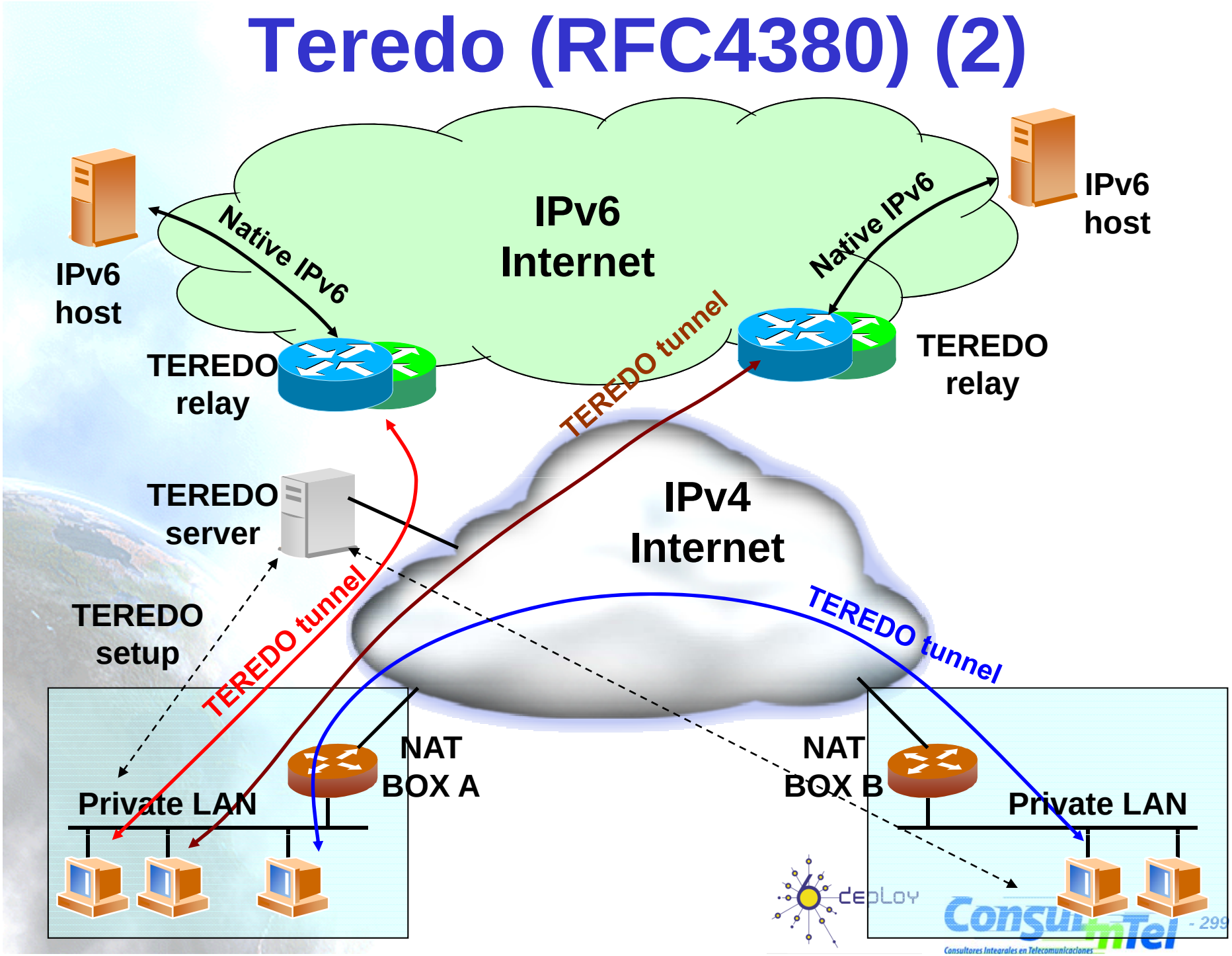


7.6 Teredo

Teredo (RFC4380) (1)

- Teredo [TEREDO] [TEREDOC] está pensado para proporcionar IPv6 a nodos que están ubicados detrás de NAT que no son “proto-41 forwarding”.
  - Encapsulado de paquetes IPv6 en paquetes UDP/IPv4
- Funciona en NAT de tipo:
  - Full Cone
  - Restricted Cone
- No funciona en NATs de tipo
  - Symmetric (Solventado en Windows Vista)
- Intervienen diversos agentes:
  - Teredo Server
  - Teredo Relay
  - Teredo Client
- El cliente configura un Teredo Server que le proporciona una dirección IPv6 del rango 2001:0000::/32 basada en la dirección IPv4 publica y el puerto usado
  - Si el Teredo Server configurado es además Teredo Relay, el cliente tiene conectividad IPv6 con cualquier nodo IPv6
  - De lo contrario solo tiene conectividad IPv6 con otros clientes de Teredo
- Actualmente Microsoft proporciona Teredo Servers públicos y gratuitos, pero no Teredo Relays

Teredo (RFC4380) (2)



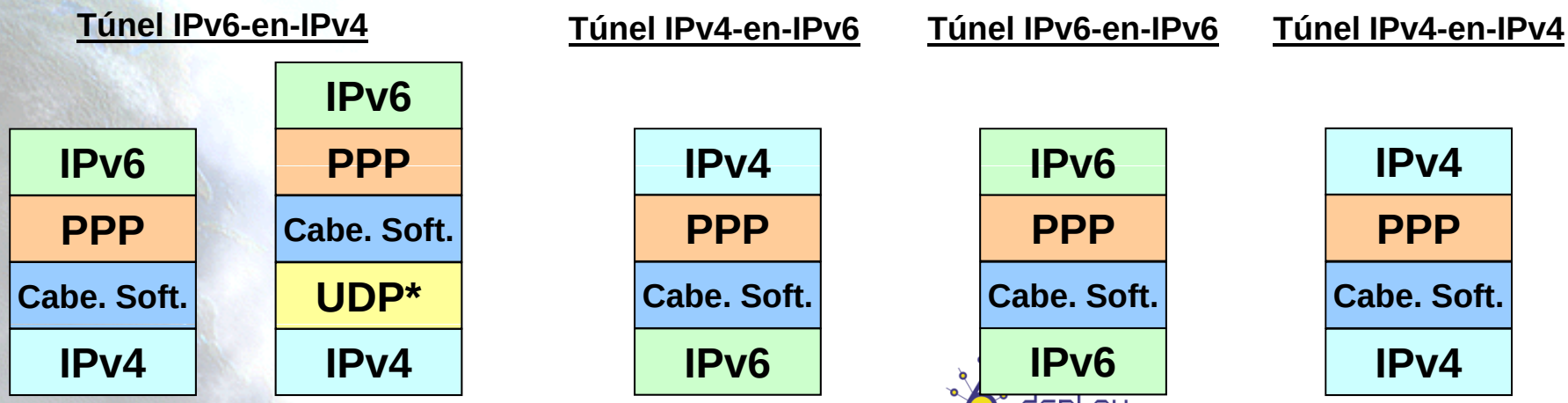
7.7 Softwires

Softwires

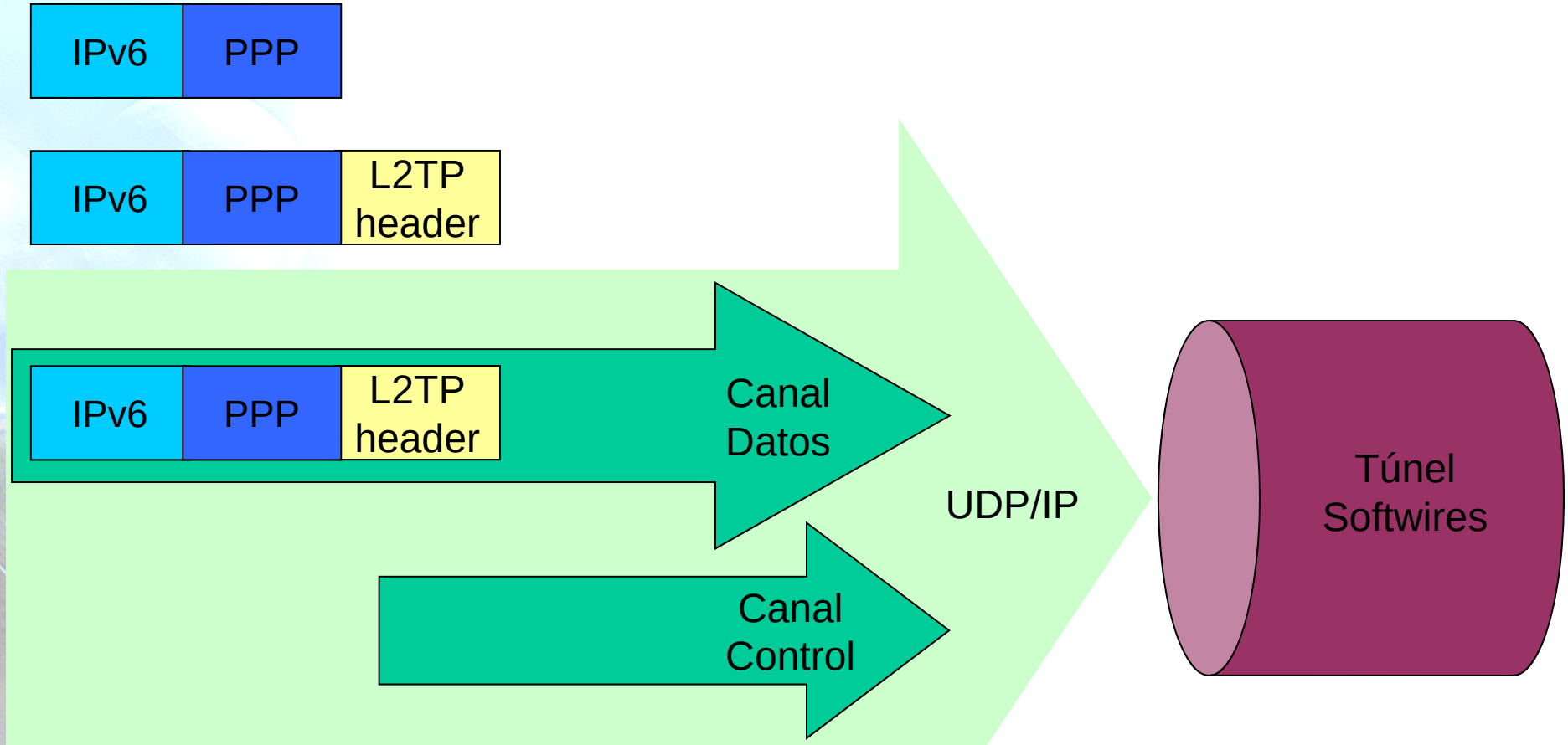
- Protocolo que esta siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
  - Mecanismo de transición “universal” basado en la creación de túneles
    - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
    - Permite atravesar NATs en las redes de acceso
    - Proporciona delegación de prefijos IPv6 (/48, /64, etc.)
    - Autenticación de usuario para la creación de túneles mediante la interacción con infraestructura AAA
    - Posibilidad de túneles seguros
    - Baja sobrecarga en el transporte de paquetes IPv6 en los túneles
    - Fácil inclusión en dispositivos portátiles con escasos recursos hardware
  - Softwires posibilitará la provisión de conectividad IPv6 en dispositivos como routers ADSL, teléfonos móviles, PDAs, etc. cuando no exista conectividad IPv6 nativa en el acceso
  - También posibilita la provisión de conectividad IPv4 en dispositivos que solo tienen conectividad IPv6 nativa
- En realidad Softwires no es un nuevo protocolo, sino la definición de cómo usar de una forma diferente protocolos ya existentes con el fin de proporcionar conectividad IPv6 en redes IPv4 y viceversa
- Sofwires se basa en **L2TPv2** (RFC2661) y **L2TPv3** (RFC3991)

Encapsulamiento de Softwires basado en L2TPv2

- El funcionamiento se especifica en draft-ietf-softwire-hs-framework-l2tpv2
- Existen dos entidades:
  - Softwires Initiator (SI): agente encargado de solicitar el túnel
  - Softwires Concentrator (SC): agente encargado de crear el túnel (tunnel end point)
- Se utiliza PPP para transportar paquetes IPx (x=4, 6) en paquetes IPy (y=4, 6)
  - Opcionalmente se puede encapsular los paquetes PPP en UDP en caso de que haya que atravesar NATs



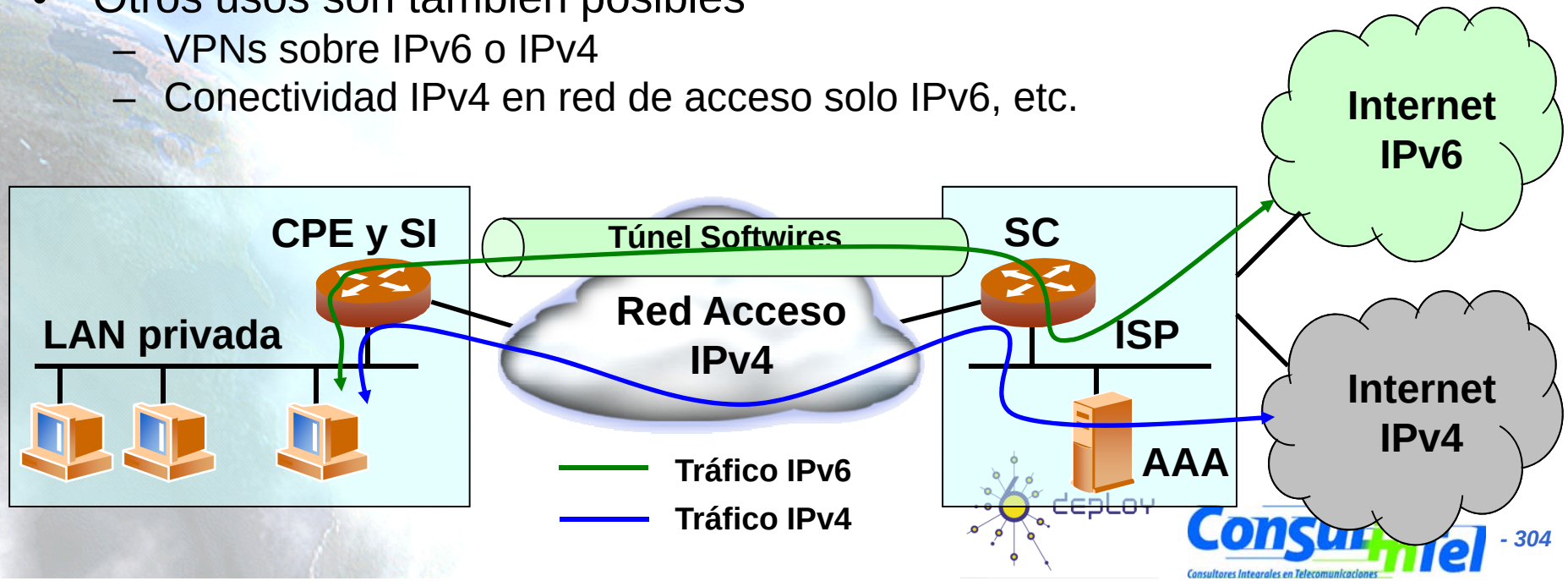
Softwires basado en L2TPv2



- Existe un plano de control y otro de datos
- Se usa PPP como protocolo de encapsulamiento

Ejemplo de uso de Softwires

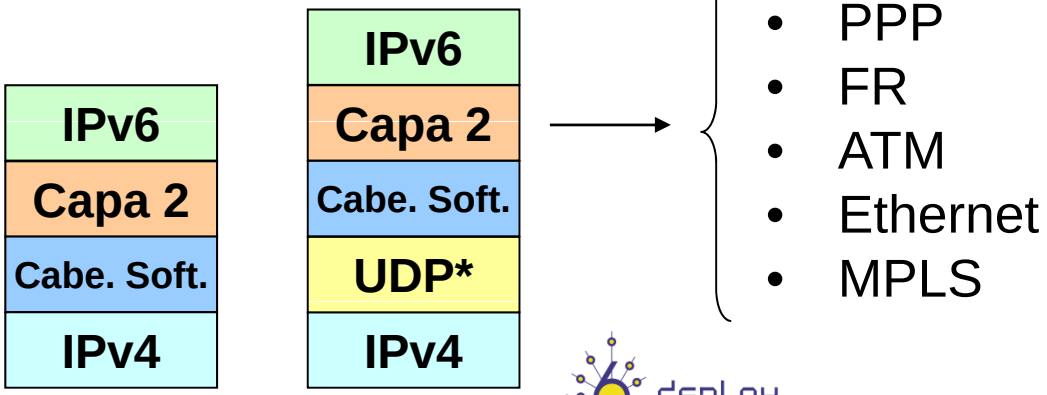
- Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4
  - El SC está instalado en la red del ISP (DSLAM, Router de agregación u otro dispositivo)
  - El SI está instalado en la red del usuario
    - CPE típicamente. También es posible otro dispositivo diferente en la red del usuario
  - El SC proporciona conectividad IPv6 al SI, y el SI hace de encaminador IPv6 para el resto de la red de usuario
  - Se usa delegación de prefijo IPv6 entre el SC y el SI para proporcionar un prefijo (típicamente /48) a la red del usuario
    - DHCPv6 PD
- Otros usos son también posibles
  - VPNs sobre IPv6 o IPv4
  - Conectividad IPv4 en red de acceso solo IPv6, etc.



Encapsulamiento de Softwires basado en L2TPv3

- Misma filosofía y componentes que con L2TPv2, pero con las particularidades de L2TPv3
  - Transporte sobre IP/UDP de otros protocolos de capa 2 diferentes a PPP
    - HDLC, PPP, FR, ATM, Ethernet, MPLS, IP
  - Formato de cabeceras mejorado para permitir un tratamiento más rápido en los SC
    - Permite velocidades del rango de T1/E1, T3/E3, OC48
  - Mínimo overhead en los paquetes encapsulados (solo de 4 a 12 bytes extra)
  - Otros mecanismos de autenticación diferentes a CHAP y PAP
    - EAP

Túnel IPv6-en-IPv4



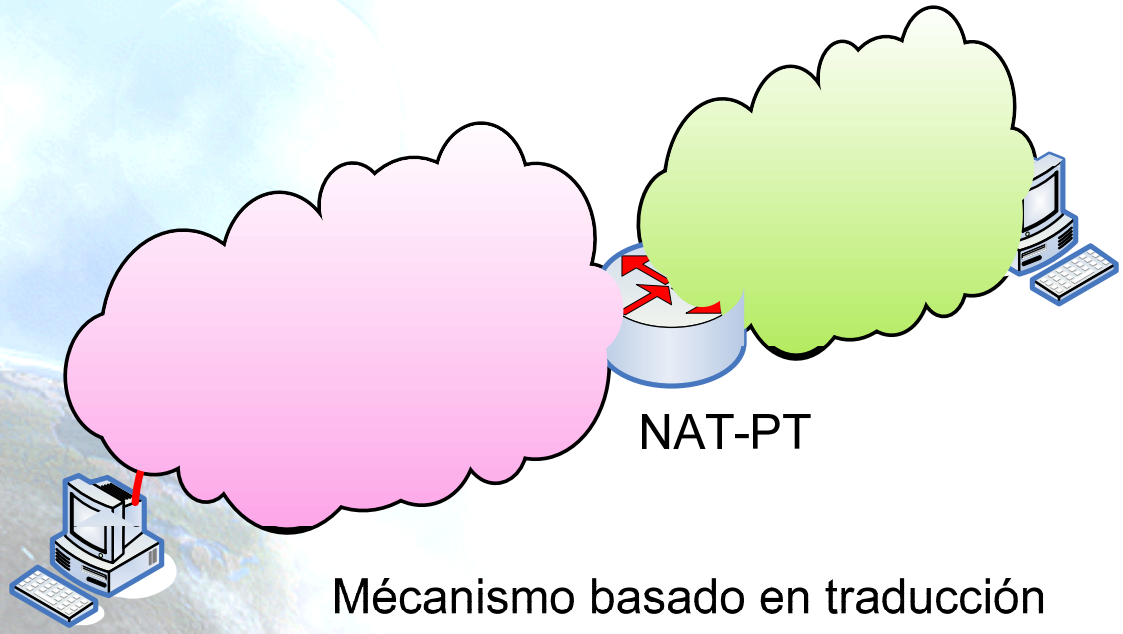
*** Opcional**

7.8 Traducción

Traducción

- Se puede utilizar traducción de protocolos IPv6-IPv4 para:
  - Nuevos tipos de dispositivos Internet (como teléfonos celulares, coches, dispositivos de consumo).
- Es una extensión a las técnicas de NAT, convirtiendo no sólo direcciones sino también la cabecera
  - Los nodos IPv6 detrás de un traductor tienen la funcionalidad de IPv6 completa cuando hablan con otro nodo IPv6.
  - Obtienen la funcionalidad habitual (degradada) de NAT cuando se comunican con dispositivos IPv4.
  - Los métodos usados para mejorar el rendimiento de NAT (p.e. RISP) también se pueden usar para mejorar la rendimiento de la traducción IPv6-IPv4.

Traducción IPv4/IPv6 (obsoleto)



Mécanismo basado en traducción

- Diferentes soluciones, pero tiene en común que tratan de traducir paquetes IPv4 a IPv6 y viceversa
  - [SIT], [BIS], [TRT], [SOCKSv64]
- La más conocida es NAT-PT [NATPT], [NATPTIMPL]
  - Un nodo intermedio (router) modifica las cabeceras IPv4 a cabeceras IPv6
  - El tratamiento de paquetes es complejo
- Es la peor solución puesto que la traducción no es perfecta y requiere soporte de ALGs, como en el caso de los NATs IPv4
  - DNS, FTP, VoIP, etc.

7.9 Seguridad

Seguridad en los mecanismos de transición

- La seguridad en las comunicaciones es un objetivo que debe garantizarse en un entorno hostil como es en la actualidad Internet
- Cada protocolo/mecanismo utilizado introduce nuevas amenazas y/o oportunidades que nodos malintencionados puedan aprovechar para comprometer la seguridad
- Los mecanismos de transición IPv6 no son una excepción y se han realizado análisis de posibles amenazas y recomendaciones de seguridad sobre los más empleados
  - Túneles 6in4
  - Túneles 6to4
  - Teredo

Seguridad en túneles 6in4 (RFC4891) (1)

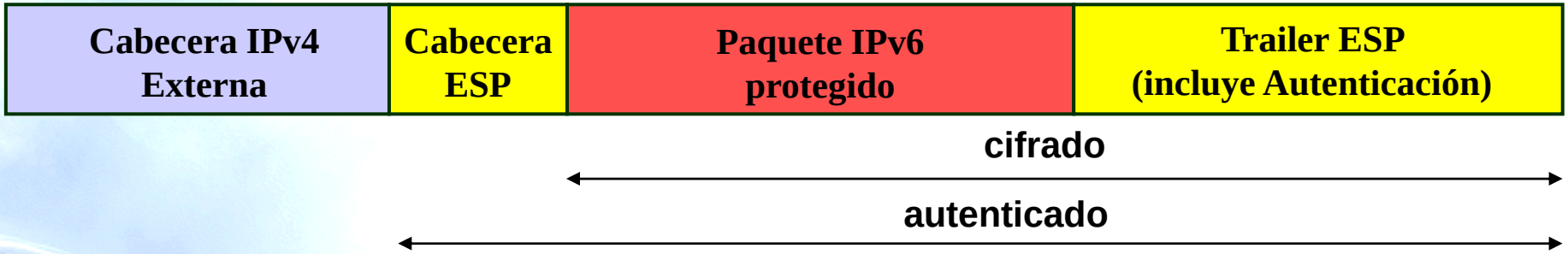
- Existen básicamente dos tipos de amenazas para los túneles de tipo 6in4
  - **La dirección IPv4 del paquete** (cabecera externa) **se puede suplantar** ("spoofing")
    - Esta amenaza se pude minimizar mediante dos mecanismos:
      - Filtrado de ingreso en todos los ISP ➔ No se cumple en el 100% de los casos
      - Filtrado de ingreso en el nodo final del router ➔ Solo se aceptan paquetes cuya dirección IPv4 origen sea la configurada en el túnel
  - **La dirección IPv6 del paquete encapsulado** (cabecera interna) **se puede suplantar** ("spoofing")
    - Esta amenaza se pude minimizar mediante: Filtrado de ingreso en el nodo final del router ➔ Solo se aceptan paquetes cuya dirección IPv6 origen sea la configurada en el túnel
- En la práctica es necesario emplear algún método que permita eliminar esas amenazas, puesto que las medidas minimizadoras no son suficientes o no se usan en todos los casos
  - Se recomienda usar **IPsec** en los túneles 6in4 para garantizar la seguridad en el túnel ➔ RFC4891
- La protección en el túnel debe aplicarse a los tres posibles tipos de tráfico IPv6: Tráfico IPv6 global unicast/anycast, Tráfico IPv6 link-local y Tráfico IPv6 multicast

Seguridad en túneles 6in4 (RFC4891) (2)

- IPsec se puede usar de dos formas para proteger los túneles 6in4:
  - Modo transporte (recomendado)
  - Modo túnel
- Con IPsec se garantiza entre los extremos del túnel:
  - integridad
  - confidencialidad
  - autenticidad
  - protección contra réplica
- Para poder emplear IPsec en túneles 6in4 es necesario:
  - Usar implementación IPsec que cumpla con RFC4301
    - Dicho RFC actualiza el RFC2401 y añade funcionalidades nuevas necesarias en túneles 6in4
  - En caso de usar IKE como protocolo de gestión de claves para la negociación de SAs IPsec, se recomienda IKEv2 (RFC4306)
- Se recomienda usar ESP en vez de AH ya que aunque la cabecera AH garantiza la integridad de ciertos campos de la cabecera externa IPv4, esta será descartada en cualquier caso en el extremo final del túnel.

IPsec con modo transporte en túneles 6in4

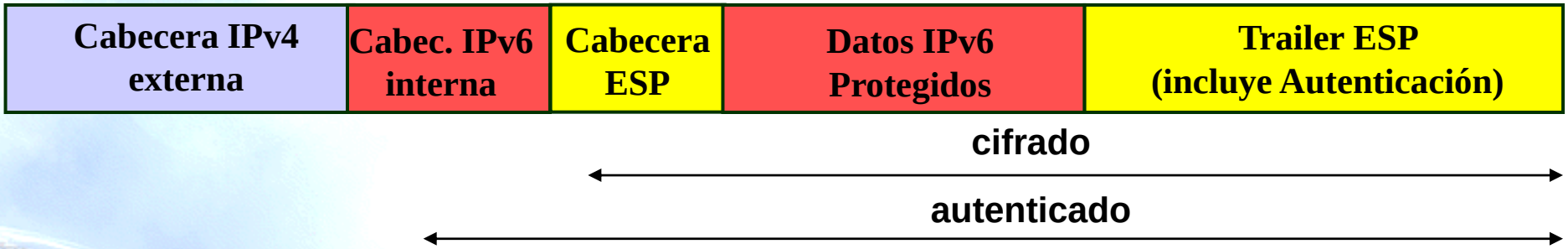
Ejemplo del Modo Transporte con ESP



- Modo transporte
  - Se emplea ESP o AH dependiendo del grado de seguridad deseado
  - La SA se define mediante (entre otros):
    - IPv4 origen
    - IPv4 destino
    - Tipo de tráfico: IPv6, (protocolo 41)
  - En el receptor, cuando un paquete IPsec se acepta se garantiza que viene de la dirección IPv4 adecuada
  - Con IPsec en modo transporte no se evita la suplantación de la dirección IPv6 del paquete encapsulado (“inner IPv6 source”)
    - Se puede resolver fácilmente mediante filtrado de ingreso en el interfaz del túnel

IPsec con modo túnel en túneles 6in4

Ejemplo del Modo Túnel con ESP



- Modo túnel
  - Se emplea ESP o AH dependiendo del grado de seguridad deseado
  - La SA se define mediante (entre otros):
    - IPv6 origen
    - IPv6 destino
  - En el receptor, cuando un paquete IPsec se acepta se garantiza que viene de la dirección IPv6 adecuada
  - Con IPsec en modo túne no se evita la suplantación de la dirección IPv4 del paquete (“outer IPv4 source”)
    - Pero no es ningún problema puesto que la SA IPv6 garantiza que el paquete viene del nodo adecuado

Seguridad en túneles 6in4 (RFC4891) (3)

- El modo transporte es el recomendado puesto que existen diversos inconvenientes con el uso del modo túnel:
  - La mayoría de implementaciones de IPsec NO modelan la SA en modo túnel como un interfaz de red
    - Es necesario identificar todo el tráfico link-local y multicast resultando en una lista de SAs demasiado extensa
    - No es posible implementarlo en túneles 6in4 entre túneles puesto que el tráfico que transporta no es de un determinado prefijo IPv6, sino que el tráfico potencial a transportar es en la práctica toda la Internet IPv6
      - Puede haber en el túnel paquetes IPv6 dirigidos/recibidos a/desde cualquier nodo IPv6
- Para proteger túneles 6in4 se recomienda por tanto:
  - Configuración manual del túnel
  - Usar IPsec en modo transporte con ESP
    - RFC4301
  - Configurar filtrado en el ingreso de paquetes IPv6 en la interfaz del túnel
  - Usar IKEv2 en caso de gestión automática de claves

Seguridad en túneles 6to4 (RFC3964) (1)

- Las amenazas identificadas en los túneles 6to4 son motivadas fundamentalmente por el comportamiento específico de los nodos 6to4:
  - Cualquier encaminador 6to4 debe aceptar paquetes 6to4 de cualquier otro encaminador 6to4 o “relay” 6to4
  - Cualquier encaminador 6to4 debe aceptar paquetes de cualquier otro encaminador IPv6 nativo
- Las **amenazas** identificadas son de **tres tipos**
  - **Ataques de denegación de servicio (DoS)**
    - Un nodo malicioso genera tráfico que impide la provisión del servicio 6to4 en el nodo atacado
  - **Ataques de denegación de servicio por reflexión (Reflection DoS)**
    - Un nodo malicioso retransmite/refleja tráfico de otros nodos benignos (no sospechosos) impidiendo la provisión del servicio 6to4 en el nodo atacado
  - **Robo de servicio**
    - Un nodo/red/operador hace uso no autorizado del servicio 6to4
- Los tipos de ataques que explotan dichas amenazas son:
  - Ataques con mensajes ND
  - Suplantación de tráfico
  - Reflexión de tráfico desde nodos 6to4
  - Ataque mediante direcciones IPv4 broadcast
  - Robo del servicio 6to4

Seguridad en túneles 6to4 (RFC3964) (2)

- Esos ataques pueden ir dirigidos contra:
  - Redes 6to4
  - Redes IPv6 nativas
  - Redes IPv4
- Algunas soluciones que mitigan los ataques
  - No se deben permitir mensajes ND en las interfaces 6to4
    - En caso contrario habría que usar IPsec o SEND para protegerlos
  - Filtrado de ingreso de paquetes en redes IPv4 e IPv6
  - Filtrado de salida de paquetes IPv6 6to4 si no existe un encaminador/relay 6to4 en la red
  - Los Relays 6to4 deben tirar los paquetes que vienen a través de una interfaz IPv6 nativa cuya dirección IPv6 origen es 6to4
  - Los Relays 6to4 deben tirar los paquetes que vienen a través de una interfaz 6to4 cuya dirección IPv6 origen no es 6to4 y/o la dirección origen IPv4 no concuerda con la dirección IPv4 embebida en la dirección IPv6
  - Limitación del ancho de banda en los 6to4 relays
  - Filtrado en relays 6to4 de paquetes IPv6 cuya dirección destino no es 192.88.99.1

Seguridad en TEREDO

- Teredo es un tipo especial de túnel IPv6 que encapsula los paquetes IPv6 en paquetes IPv4-UDP con el fin de atravesar los NATs
- Como consecuencia este mecanismo en sí mismo abre una puerta en los sistemas de defensa perimetrales (firewalls) a cierto tipo de trafico
  - Tráfico IPv6 benigno
  - Tráfico IPv6 maligno con deseo de vulnerar nodos/servicios
- De este modo cierto tipo de tráfico pasa por los sistemas perimetrales sin ningún tipo de control, sin que el administrador de la red/seguridad pueda saber qué tipo de tráfico IPv6 atraviesa su red
  - Hasta la fecha no existen dispositivos capaces de inspeccionar el tráfico TEREDO, de manera que no es posible aplicar políticas de seguridad al tráfico IPv6 encapsulado con ese método
- Por este motivo, en caso de permitir el uso TEREDO en los nodos finales dentro de una red, es altamente recomendable:
  - El nodo final esté adecuadamente protegido
    - Puesta al día de actualizaciones de software, sistema operativo, etc.
    - Instalación de mecanismos de protección adecuados (anti-virus, etc.)
  - El administrador de red/seguridad debe estar al corriente de las posibles vulnerabilidades introducidas por TEREDO
    - draft-ietf-v6ops-teredo-security-concerns

Referencias Transición (1)

- [6in4] RFC1933, RFC4213
- [6to4] RFC3056
- [6over4] RFC2529
- [AYIYA] draft-massar-v6ops-ayiya-02
- [BIS] RFC2767
- [DSTM] draft-ietf-ngtrans-dstm-10
- [ISATAP] RFC5214
- [NATPT] RFC2766, RFC4966
- [NATPTIMPL]
  - http://www.ipv6.or.kr/english/download.htm ==> Linux 2.4.0
  - http://www.ispras.ru/~ipv6/index_en.html ==> Linux y FreeBSD
  - http://research.microsoft.com/msripv6/napt.htm Microsoft
  - ftp://ftp.kame.net/pub/kame/snap/kame-20020722-freebsd46-snap.tgz ==> KAME snapshot (22.7.2002)
  - http://ultima.ipv6.bt.com/
- [PRIVACY] RFC3041
- [PROTO41] draft-palet-v6ops-proto41-nat
- [SIIT] RFC2765
- [SILKROAD] draft-liumin-v6ops-silkroad-02

Referencias Transición (2)

- [SOCKSv64] RFC3089
- [SOFTWIRES] RFC5571
- [STATELESS] RFC4862
- [STATEFUL] RFC3315
- [STUN] RFC3489
- [TB] RFC3053
- [TEREDO] RFC4380
- [TEREDOC] http://technet.microsoft.com/es-es/library/cc722030%28WS.10%29.aspx
- [TRT] RFC3142
- [TSP] draft-vg-ngtrans-tsp-01, http://www.hexago.com/index.php?pgID=step1
- [TunAut] RFC1933
- Windows IPv6
  - http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_ip_v6_add_utils.mspx
  - http://www.microsoft.com/technet/community/columns/cableguy/cg0902.mspx

Bloque 2

Otros Aspectos Avanzados

8. Calidad de Servicio (QoS)

8.1 Conceptos de QoS

8.2 Soporte QoS en IPv6

8.3 Aspectos prácticos

8.1 Conceptos de QoS

Conceptos de QoS (1)

- Calidad: Entrega fiable de datos ("mejor de lo normal")
  - Pérdida de datos
  - Latencia
  - "Jittering"
  - Ancho de banda
- Servicio: Cualquier cosa ofrecida al usuario
  - Comunicaciones
  - Transporte
  - Aplicaciones

Conceptos de QoS (2)

- Calidad de Servicio es una medida del comportamiento de la red con respecto a ciertas características de algunos servicios definidos !!!!!

- Conceptos comunes a todas las definiciones de QoS:
  - Diferenciación de Tráfico y Tipo de Servicio
  - Los usuarios pueden ser capaces de tratar una o más clases de tráfico de forma diferente

Aproximaciones a QoS en IP

Dos aproximaciones básicas desarrolladas en IETF

- "Integrated Service" (int-serv)
  - "Ajuste fino" (por-flujo), especificaciones cuantitativas (p.ej., x bits por segundo), usa señalización RSVP
- "Differentiated Service" (diff-serv)
  - "Ajuste basto" (por-clase), especificaciones cualitativas (p.ej., mayor prioridad), no hay señalización explícita

8.2 Soporte QoS en IPv6

Soporte IPv6 para Int-Serv

Campo Flow Label de 20 bits para identificar flujos específicos que necesitan un tratamiento especial de QoS

- Cada fuente especifica su propio valor de Flow Label; los encaminadores usan la Dirección Origen + Flow Label para identificar los distintos flujos
- El valor 0 en el Flow Label se usa cuando no se requiere una QoS especial, lo cual es el caso más común de momento
- Esta parte de IPv6 no está estandarizada aún y puede cambiar su semántica en el futuro.

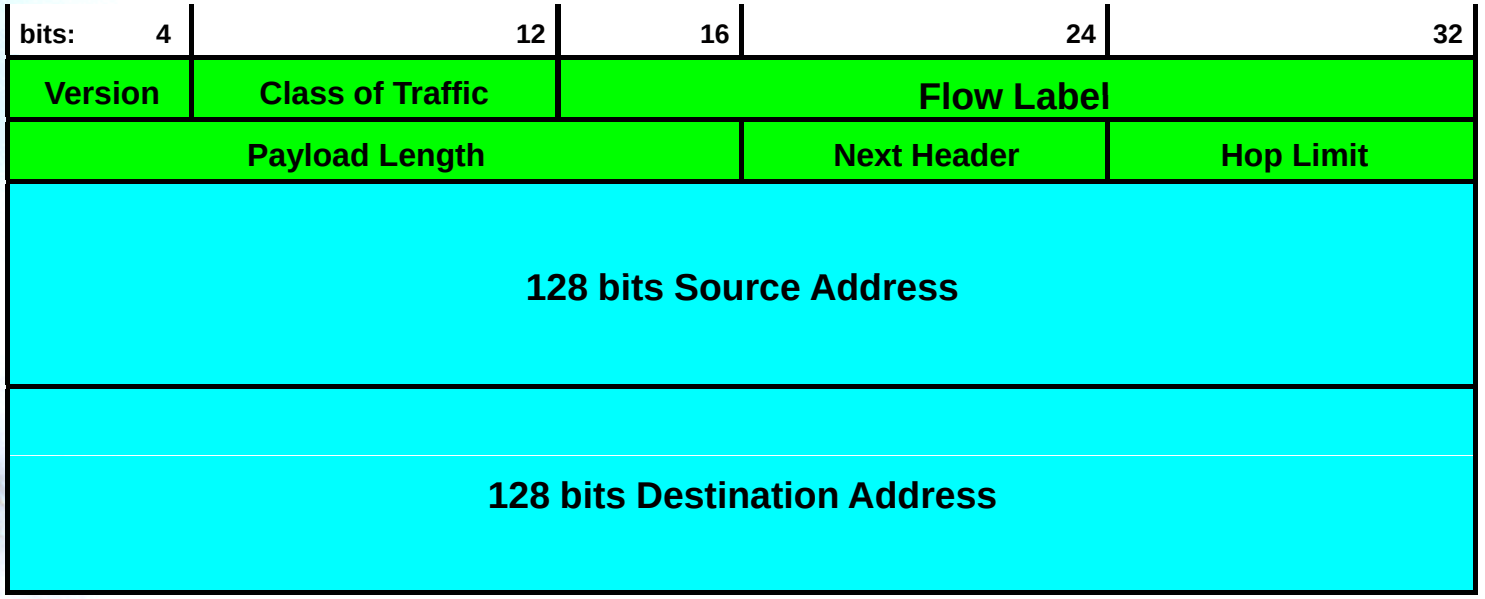
Suporte IPv6 para Diff-Serv

Campo Traffic Class de 8 bits para identificar clases de paquetes específicas que necesitan un tratamiento especial de QoS

- Tiene el mismo significado que la definición nueva del octeto Type-of-Service en IPv4
- Puede ser inicializada por un nodo o un encaminador en la ruta hacia el destino. También puede ser rescrito por cualquier encaminador en la ruta hacia el destino.
- El valor 0 en el campo Traffic Class se usa para especificar que no es necesario un tratamiento especial de QoS, lo cual es lo más común en la actualidad

IPv6 Flow Label

- El campo “Flow Label” de 20 bits habilita la clasificación eficiente de flujos IPv6 basados solo en los campos principales de la cabecera IPv6 que tienen posiciones fijas



IPv6 Flow Label (RFC3697)

- RFC3697 específica
  - El campo “IPv6 Flow Label”
  - Requisitos mínimos para:
    - Nodos IPv6 fuente que etiquetan flujos
    - Nodos IPv6 que retransmiten paquetes ya etiquetados
    - Métodos de establecimiento de estados de flujo
- RFC3697 menciona algunos ejemplos de posibles usos del “flow labeling”

Flow Labels (1)

- Generalidades
  - Un flujo es una secuencia de paquetes enviados desde una fuente particular a un destino unicast, anycast o multicast particular, que la fuente desea etiquetar como un flujo
    - Un flujo podría consistir en todos los paquetes de una conexión específica o “media stream”
    - Sin embargo, un flujo no es necesariamente un “mapeo” 1:1 a una conexión
  - Tradicionalmente, los clasificadores de flujo se han basado en tuplas de 5: dirección fuente, dirección destino, puerto origen, puerto destino y tipo de protocolo de transporte
    - Pero alguno de estos campos puedes no estar disponibles debido a la existencia de fragmentación, encriptación o aun estando disponibles, su localización detrás de una secuencia de cabeceras de extensión IPv6 puede resultar ineficiente
    - Además, si los clasificadores son tales que solo se fijan en las cabeceras de la capa IP, la introducción de otros protocolos de transporte alternativos no será problemática

Flow Labels (2)

- IPv6 Flow Label
  - En IPv6 se usan tuplas de 3: campo Flow Label, dirección fuente y dirección destino
  - Esto permite la clasificación eficiente de flujos IPv6
  - Solo se usan campos de posiciones fijas en la cabecera IPv6
- El mínimo soporte de flujos IPv6 consiste en la etiquetación de los flujos
  - Los nodos IPv6 que soporten la etiquetación de flujos DEBEN ser capaces de etiquetar flujos conocidos (por ejemplo, conexiones TCP, aplicaciones de streaming, etc.)
  - Incluso si el nodo por sí mismo no requiriera ningún tratamiento específico de flujos

Especificación de Flow Label (1)

- El campo “Flow Label” en la cabecera IPv6 es usado por una fuente para etiquetar los paquetes de un determinado flujo
- Un “Flow Label” de valor cero se usa para indicar que el paquete no pertenece a ningún flujo determinado
- Los clasificadores de paquetes usan la tupla de 3 campos para identificar el flujo al que pertenece un determinado paquete
- Los paquetes se procesan de una determinada forma especificada en los nodos con capacidad de procesar flujos
- El valor del “Flow Label” configurado por la fuente DEBE entregarse sin modificar en el nodo destino
- Los nodos IPv6 NO DEBEN asumir ninguna matemática ni ninguna propiedad especifica de los valores asignados al “Flow Label” por los nodos fuente

Especificación de Flow Label (2)

- El rendimiento de los encaminadores NO DEBE depender de la distribución de los valores del “Flow Label”
- Los nodos que mantienen un estado de flujos dinámico NO DEBEN asumir que los paquetes que lleguen después de 120 sg o más de un paquete previo de un flujo, aún pertenece al mismo flujo, a no ser que el método de establecimiento de estados de flujo defina un tiempo de vida mayor o que el estado se haya refrescado dentro del tiempo de vida
- El uso del campo “Flow Label” no implica necesariamente ningún requisito en la reordenación de paquetes
  - Especialmente, el valor cero no implica que es aceptable la reordenación significativa de paquetes
- Si un nodo IPv6 no proporciona un tratamiento específico para flujos DEBE ignorar el campo “Flow Label” cuando reciba o retransmita un paquete

8.3 Aspectos prácticos

QoS para IPv6 en Cisco

- Soporte Cisco de Quality of Service (QoS) en redes IPv6
  - Basado en Differentiated Services (DiffServ)

- Características disponibles
  - Clasificación de paquetes (Packet classification)
  - Conformado de tráfico (Traffic shaping)
  - Políticas en tráfico (Traffic policing)
  - Marcado de paquetes (Packet marking)
  - Encolado (Queueing)
  - Weighted Random Early Detection (WRED)-based drop

- Características no disponibles
  - Compressed Real-Time Protocol (CRTP)
  - Network-based application recognition (NBAR)
  - Committed access rate (CAR)
  - Priority queueing (PQ)
  - Custom queueing (CQ)

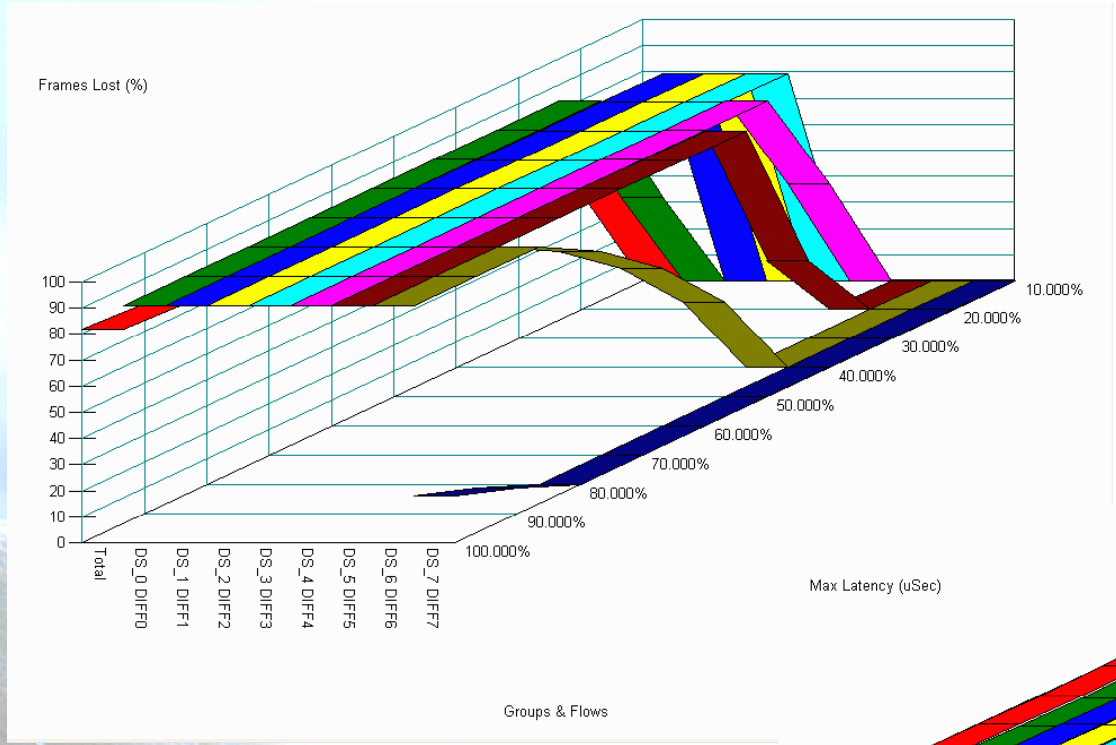
Pasos generales para implementar QoS (IPv4 e IPv6)

1. Conocer que aplicaciones necesitan QoS
2. Comprender las características de las aplicaciones para definir que herramientas de QoS les son apropiadas
3. Crear clases basadas en criterios apropiados a la red. En particular, si la red transporta tráfico IPv4 e IPv6, decidir si ambos se tratan de la misma o distinta forma, y especificar criterios de coincidencia (match) apropiados:
   - Si se tratan ambos protocolos de la misma forma se pueden usar criterios de coincidencia como: match precedence, match dscp, set precedence, y set dscp
   - Si se tratan de forma separada se pueden usar criterios de coincidencia como match protocol ip and match protocol ipv6 in a match-all class map
4. Definir políticas para cada clase
5. Configurar las políticas para tratar el trafico
6. Aplicar las políticas

- En resumen:
  - Definir clases de tráfico (traffic classes)
  - Definir y configurar políticas de trafico (traffic policies - policy maps)
  - Aplicar las políticas de tráfico a las interfaces

Al aplicar herramientas de QoS, trabajar desde el extreme (Edge) hacia el centro (Core)

Ejemplo diferenciación de Tráfico



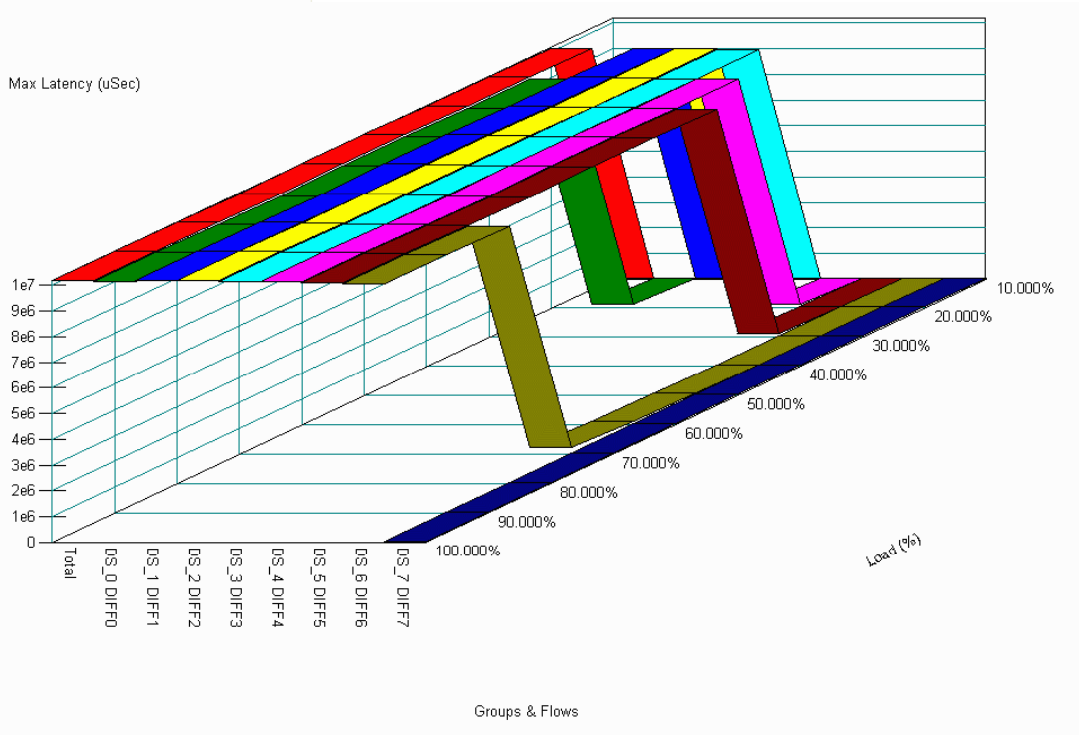


Tabla de valores

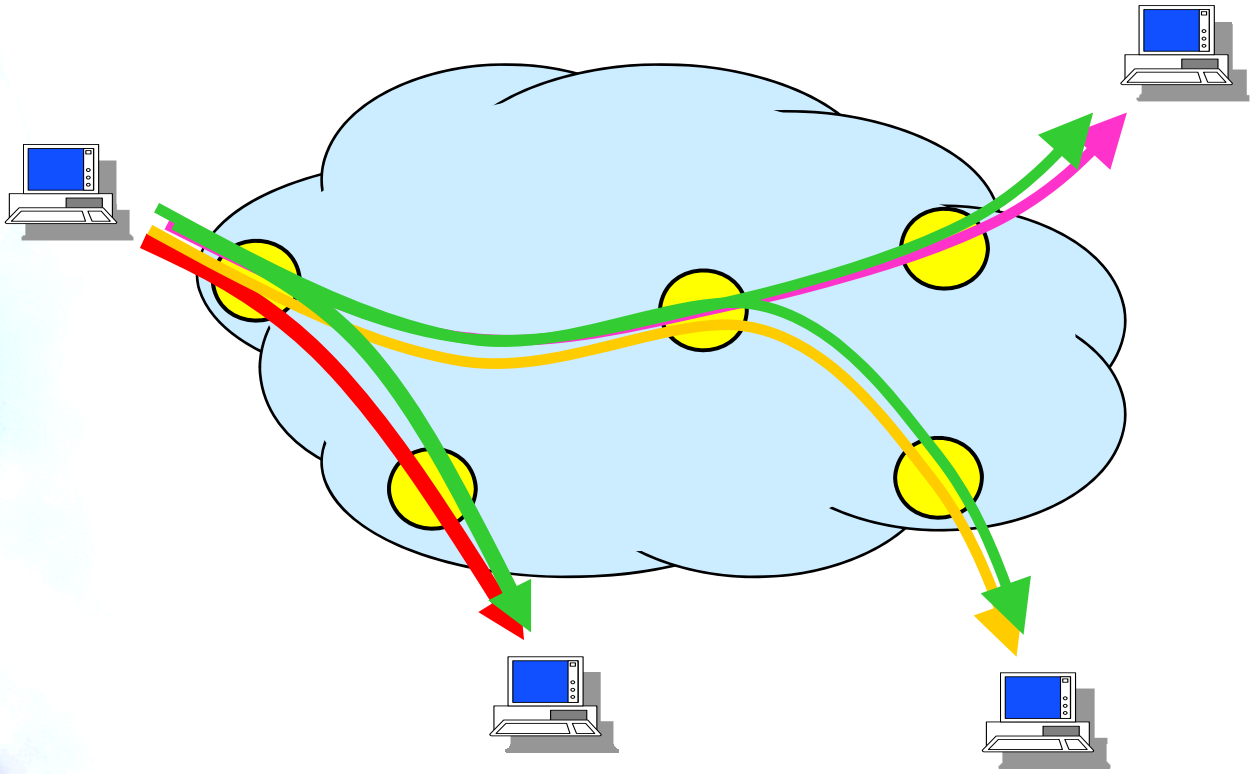
IP Precedence (Decimal)	IP Precedence (Binary)	Traffic Class (Binary)	Traffic Class (Decimal)	DSCP (Binary)	DSCP (Decimal)
0	**000**	**000000**00	0	**000000**	0
1	**001**	**001000**00	32	**001000**	8
2	**010**	**010000**00	64	**010000**	16
3	**011**	**011000**00	96	**011000**	24
4	**100**	**100000**00	128	**100000**	32
5	**101**	**101000**00	160	**101000**	40
6	**110**	**110000**00	192	**110000**	48
7	**111**	**111000**00	224	**111000**	56

9. Multicast

9.1 Conceptos Multicast
9.2 Direcciones Multicast
9.3 Multicast Listener Discovery
9.4 Encaminamiento Multicast
9.5 PIM-ASM
9.6 PIM-SSM
9.7 Aspectos prácticos

9.1 Conceptos Multicast

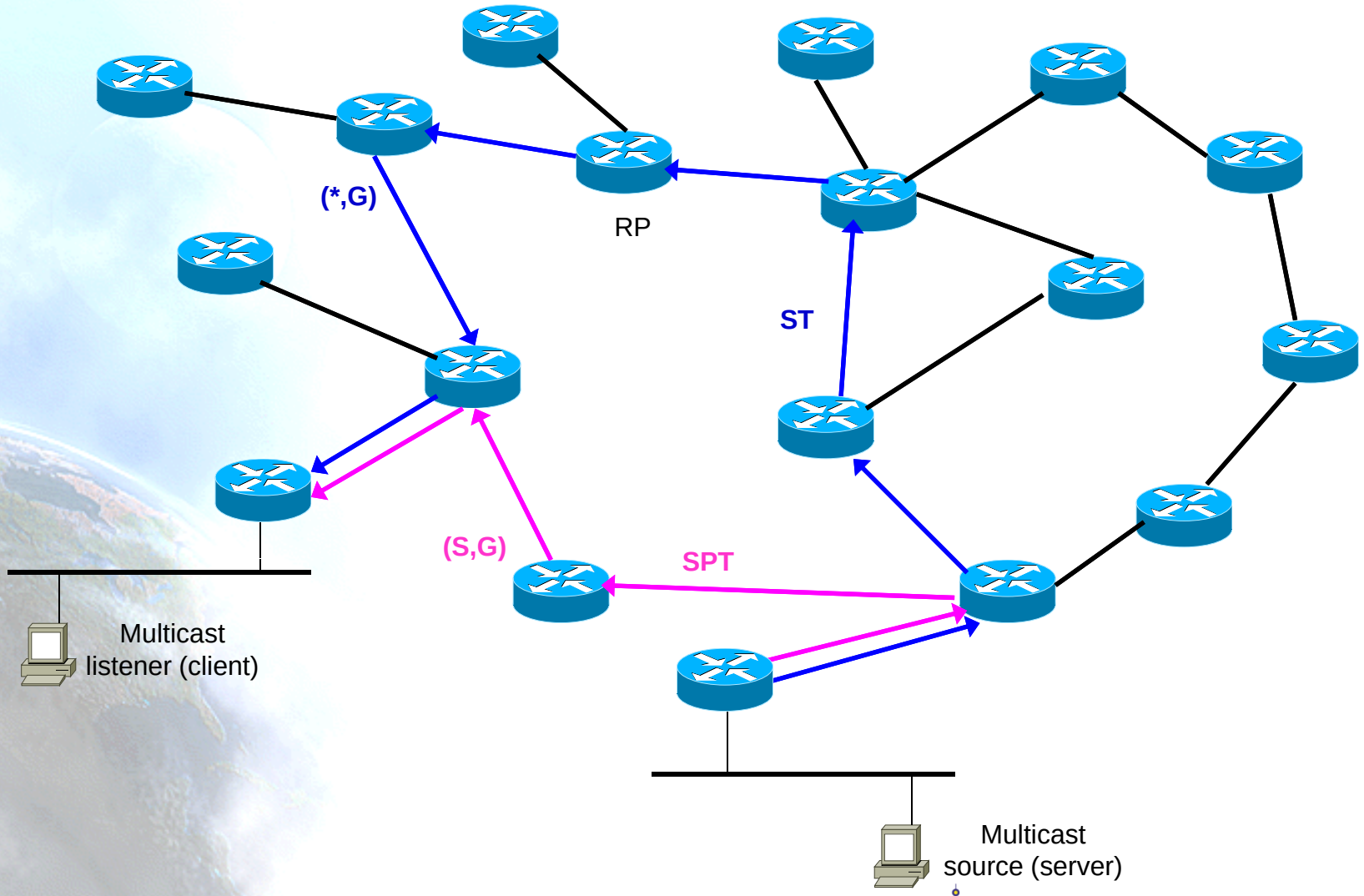
¿Qué es Multicast?



Aplicaciones

- Sistemas Distribuidos
- Video bajo Demanda (VoD)
- Difusion Radio/TV
- Conferencias Multipunto (voice/video)
- Juegos en Red
- Funciones de nivel de Red

Conceptos Multicast (1)



Conceptos Multicast (2)

- **Multicast Distribution Tree** (MDT)
  - Es el camino de distribución multicast que se usa para entregar información multicast en las redes que tienen participantes multicast
  - Tiene forma de árbol con el fin de evitar bucles multicast cerrados en la red
  - La raíz del MDT es la fuente del grupo multicast
- **Shortest Path Tree** (SPT)
  - Es el MDT que tiene la fuente la fuente del grupo multicast como raíz y a los participantes multicast como hojas del árbol
  - Se representa como (S,G)
- **Shared Tree** (ST)
  - Es el MDT resultante de tener una única raíz, denomiada “Rendez-vous Point” cuando hay más de una fuente para el mismo grupo multicast

¿Cómo funciona?

- El nodo se une/abandona un grupo multicast.
- No hay ninguna restricción acerca del número de grupos o del número de miembros por grupo.
- Enviar paquetes al grupo no significa que se pertenezca a él.
- La dirección de destino es una dirección multicast que representa a todo el grupo multicast.
- Los servicios multicast no están orientados a conexión por lo que no se puede emplear TCP.

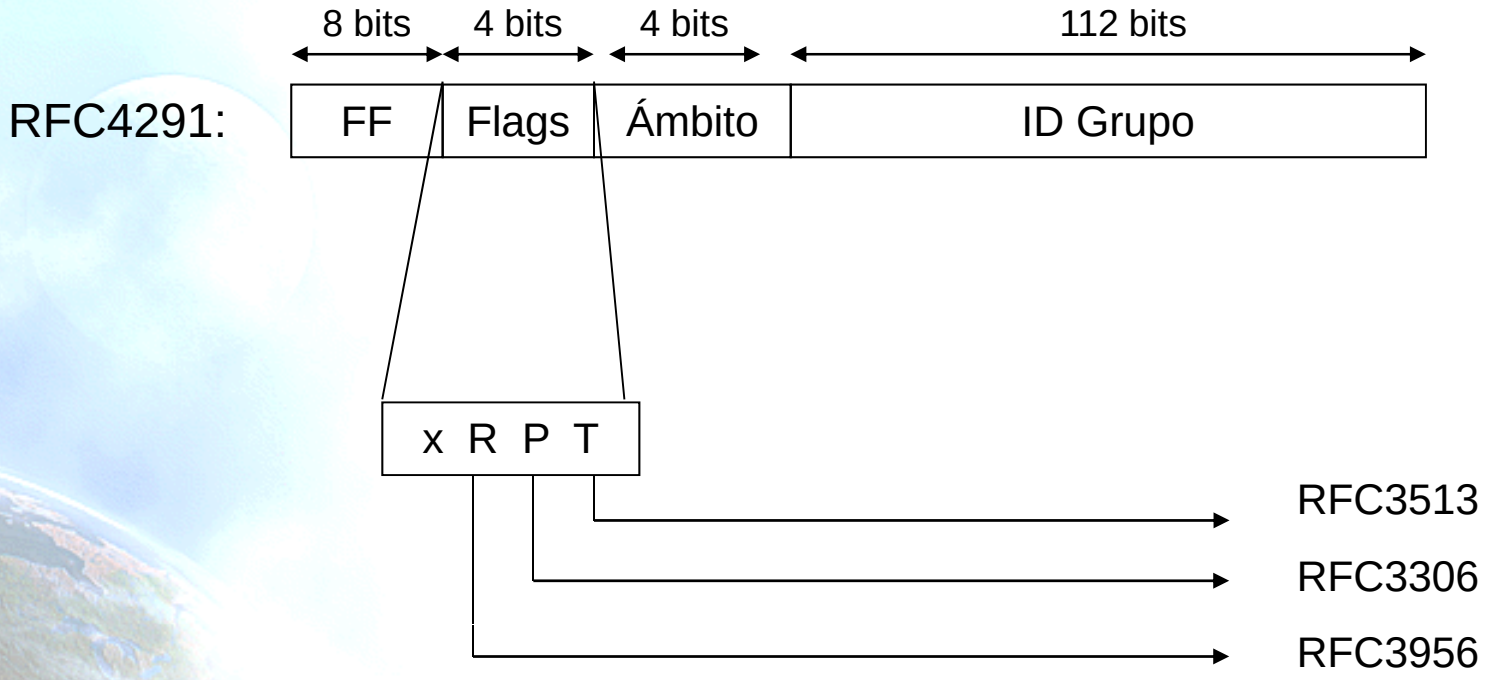
9.2 Direcciones Multicast

IPv4 vs. IPv6

- IPv4
  - Broadcast
    - Limitado: 255.255.255.255
    - Dirigido: <network>11..1
  - Multicast
    - Clase D:

      224.0.0.0 - 239.255.255.255
- IPv6
  - Multicast
    - FF….

Direcciones Multicast IPv6



Direcciones Multicast Reservadas (1)

- Node-Local Scope
  - FF01::1 Todos los nodos de la red
  - FF01::2 Todos los encaminadores de la red
- Link-Local Scope
  - FF02::1 Todos los nodos de la red
  - FF02::2 Todos los encaminadores de la red
  - FF02::4 Encaminadores DVMRP
  - FF02::5 Encaminadores OSPFIGP
  - FF02::6 Encaminadores designados OSPFIGP
  - FF02::9 Encaminadores RIP
  - FF02::B Mobile-Agents
  - FF02::D Todos los encaminadores PIM
  - FF02::1:2 Todos los DHCP-agents
  - FF02::1:FFXX:XXXX Solicited-Node Address

Direcciones Multicast Reservadas (2)

- Site-Local Scope
  - FF05::2 Todos los encaminadores
  - FF05::1:3 Todos los DHCP-servers
  - FF05::1:4 Todos los DHCP-relays

- Variable Scope Multicast Addresses
  - FF0X::101 Network Time Protocol (NTP)
  - FF0X::129 Gatekeeper
  - FF0X::2:0000-FF0X::2:7FFD Multimedia Conference Calls
  - FF0X::2:7FFE SAPv1 Announcements
  - FF0X::2:8000-FF0X::2:FFFF SAP Dynamic Assignments

Direcciones Multicast Importantes

- FF01::1, FF02::1 Todos los nodos
- FF01::2, FF02::2, FF05::2 Todos los encaminadores

- Dirección (SN) multicast a partir de la unicast
  - Si la dirección acaba en “XY:ZTUV”
  - La SN es: FF02::1:FFXY:ZTUV

- Cada nodo IPv6 debe unir la dirección SN a todas sus direcciones unicast y anycast.

9.3 Multicast Listener Discovery

Multicast Listener Discovery (1)

- MLD (RFC2710) permite que cada encaminador IPv6 aprenda que direcciones multicast hay con nodos que escuchan por ellas, en cada uno de los links a los que el encaminador está unido
- Esta es una función obligatoria en los nodos IPv6
- En IPv6 se usa MLD en vez de IGMP
- Version actual MLDv2: RFC3810 e interopera con MLDv1
  - Soporta source-filtering pero requiere PIM-SSM
- Source Address Selection for the Multicast Listener Discovery (MLD) Protocol: RFC3590
- Internet Group Management Protocol Version 3 (IGMPv3) y Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source Specific Multicast: RFC4604

Multicast Listener Discovery (2)

- MLDv1 en IPv6 es equivalente a IGMPv2 en IPv4
- MLDv2 en IPv6 es equivalente a IGMPv3 en IPv4, y funciona con PIM-SSM (PIM Source Specific Mode)

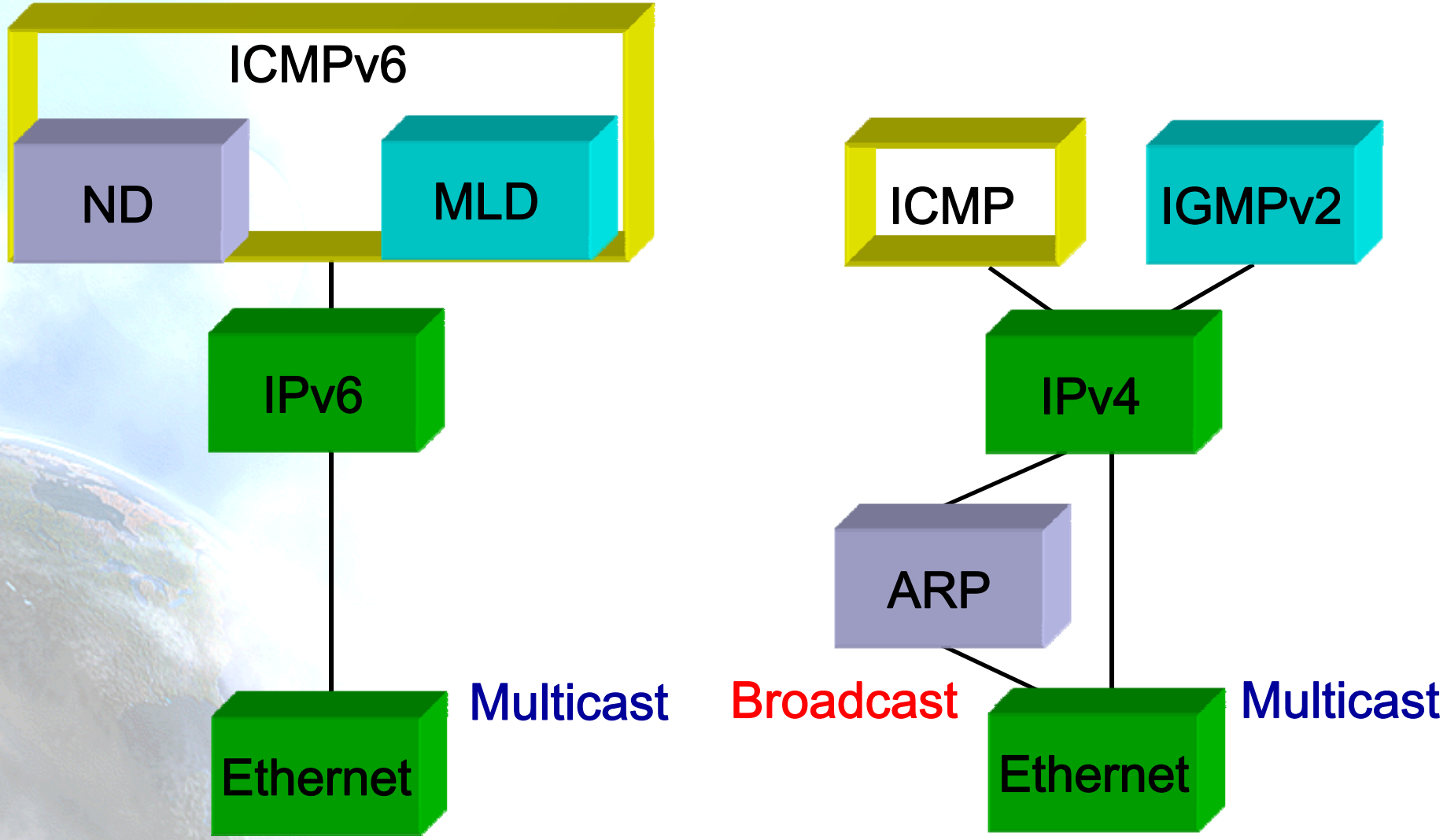
- A diferencia de IGMP en IPv4, MLD usa ICMPv6 para enviar sus mensajes
  - Todos los mensajes MLD son locales al enlace con un hop-limit de 1

- Solo hay Tres tipos de mensajes ICMPv6
  - Query enviadas periódicamente por los encaminadores
  - Report, enviados por los nodos en respuesta a las peticiones de los encaminadores o cuando los nodos quieren unirse a un grupo multicast. Llevan información acerca de los grupos multicast que el nodo está interesado en recibir
  - Done para indicar que el nodo está interesado en abandonar un grupo multicast

Mensajes MLD

- 1. Query (Type = decimal 130)
  - General Query
    - El campo de la dirección multicast tiene el valor cero
    - De esta forma el encaminador pregunta qué grupos multicast tienen participantes en la red local
  - Group Specific
    - El campo de la dirección multicast tiene la dirección multicast IPv6 específica
    - De esta forma el encaminador pregunta si un grupo multicast específico tiene participantes en la red local
- 2. Report (Type = decimal 131)
  - El campo de la dirección multicast tiene la dirección multicast IPv6 específica en la que el nodo participante está interesado
- 3. Done (Type = decimal 132)
  - El campo de la dirección multicast tiene la dirección multicast IPv6 específica en la que el nodo participante está interesado en abandonar

Plano de Control IPv4 vs. IPv6



9.4 Encaminamiento Multicast

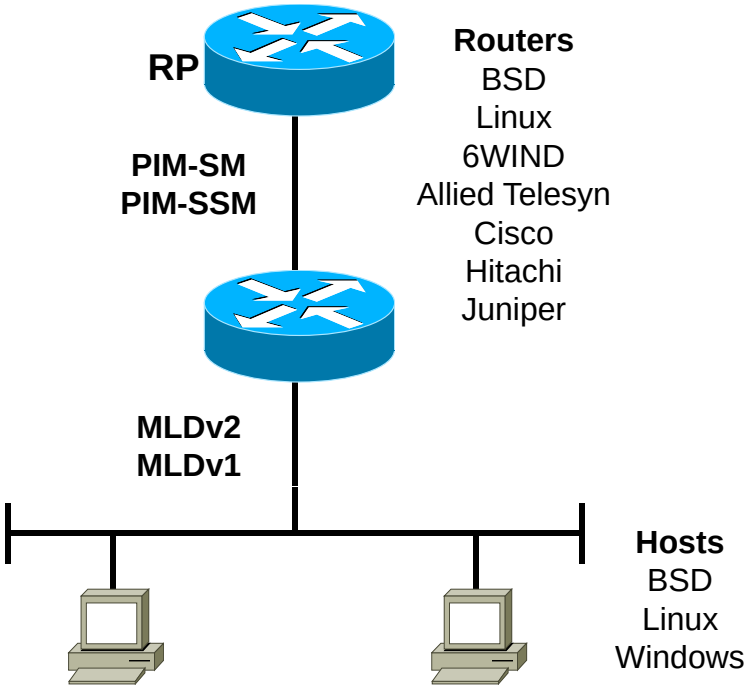
Encaminamiento Multicast

- Los encaminadores escuchan todos los grupos
- Protocolos de construcción del árbol multicast
  - Dense Mode: Adecuados para dominios densamente poblados
    - DVMRP (Distance Vector Multicast Protocol)
    - PIM-DM (Protocol Independent Dense Mode)
    - MOSPF (Multicast Open Shortest Path First)
  - Sparse Mode: Dominios no densamente poblados y dispersos
    - CBT
    - PIM-SM
      - ASM, requiere un Rendez-vous Point (RP). Aplicaciones muchos-a-muchos. Multiples fuentes transmiten a múltiples participantes (mismo grupo (*,G))
      - SSM, (PIM-SSM). Aplicaciones uno-a-muchos. Un única fuente transmite a muchos partipantes. (mismo grupo (S,G)). ASM y SSM peden usarse simultáneamente. Si se usa ASM, SSM va implícito puesto que es una sub-parte
      - Bidir (PIM-Bidir). Aplicaciones muchos-a-muchos. Los miembros de un grupo pueden ser a la vez fuentes y receptores
- Se permiten túneles multicast sobre redes IPv6 unicast
- Protocolos de Encaminamiento Inter-Dominio Multicast
  - Se usa MBGP cuando la topología de red unicast no es la misma que multicast
    - Construcción de túneles entre encaminadores separados por dominios no muliticast

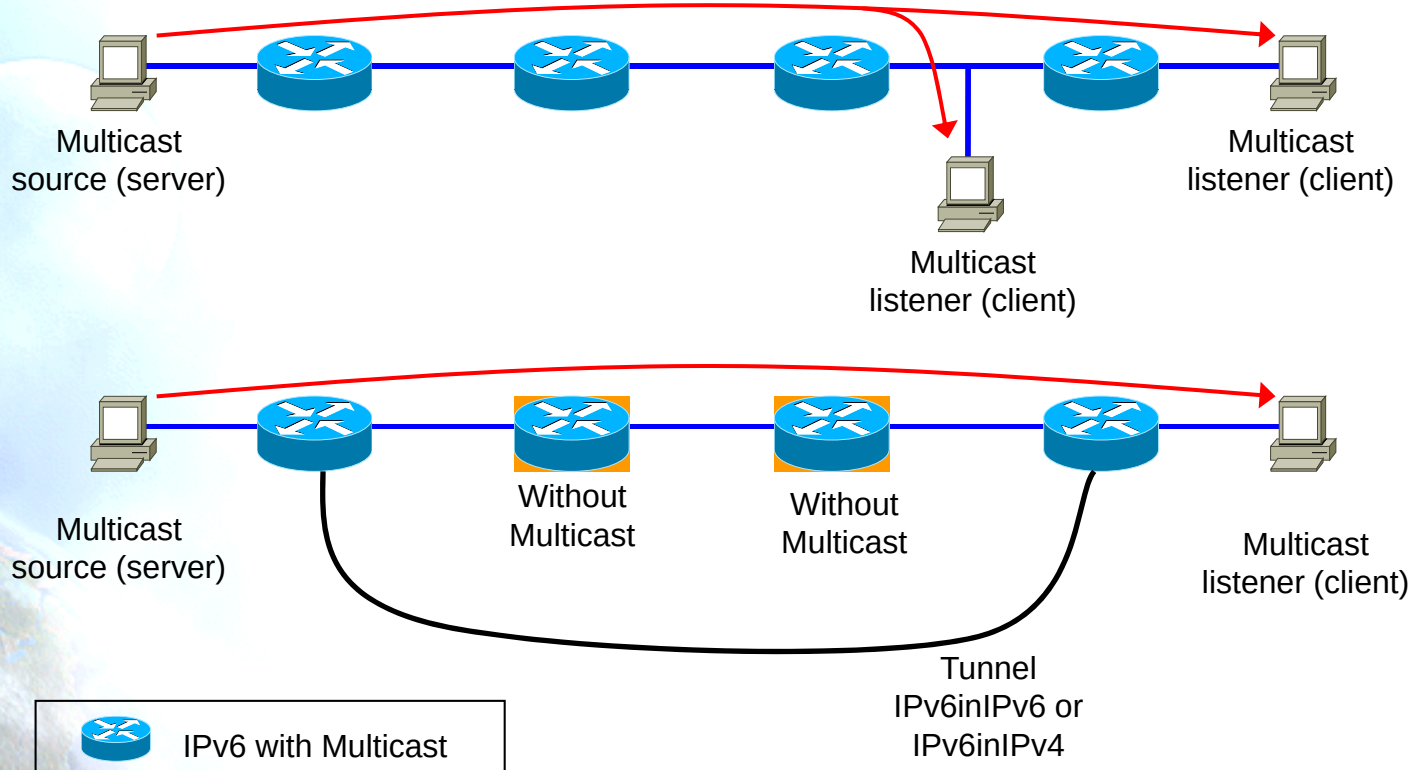
Ámbitos Multicast y protocolos

- Ambito local
  - MLD en IPv6, equivalente a IGMP
- Intra-dominio
  - PIM-SM
    - ASM
    - SSM (PIM-SSM) (Requiere MLDv2)
- Inter-dominio
  - PIM-SM-ASM requiere Embedded RP (RFC3956) para que todos los RP puedan contactar mutuamente
  - PIM-SSM no necesita nada especial para aplicaciones de una única fuente
  - MBGP necesario si la topología unicast difiere de la multicast.
    - Creación de túneles entre encaminadores separados por dominios sin soporte multicast

Escenario Básico Multicast IPv6

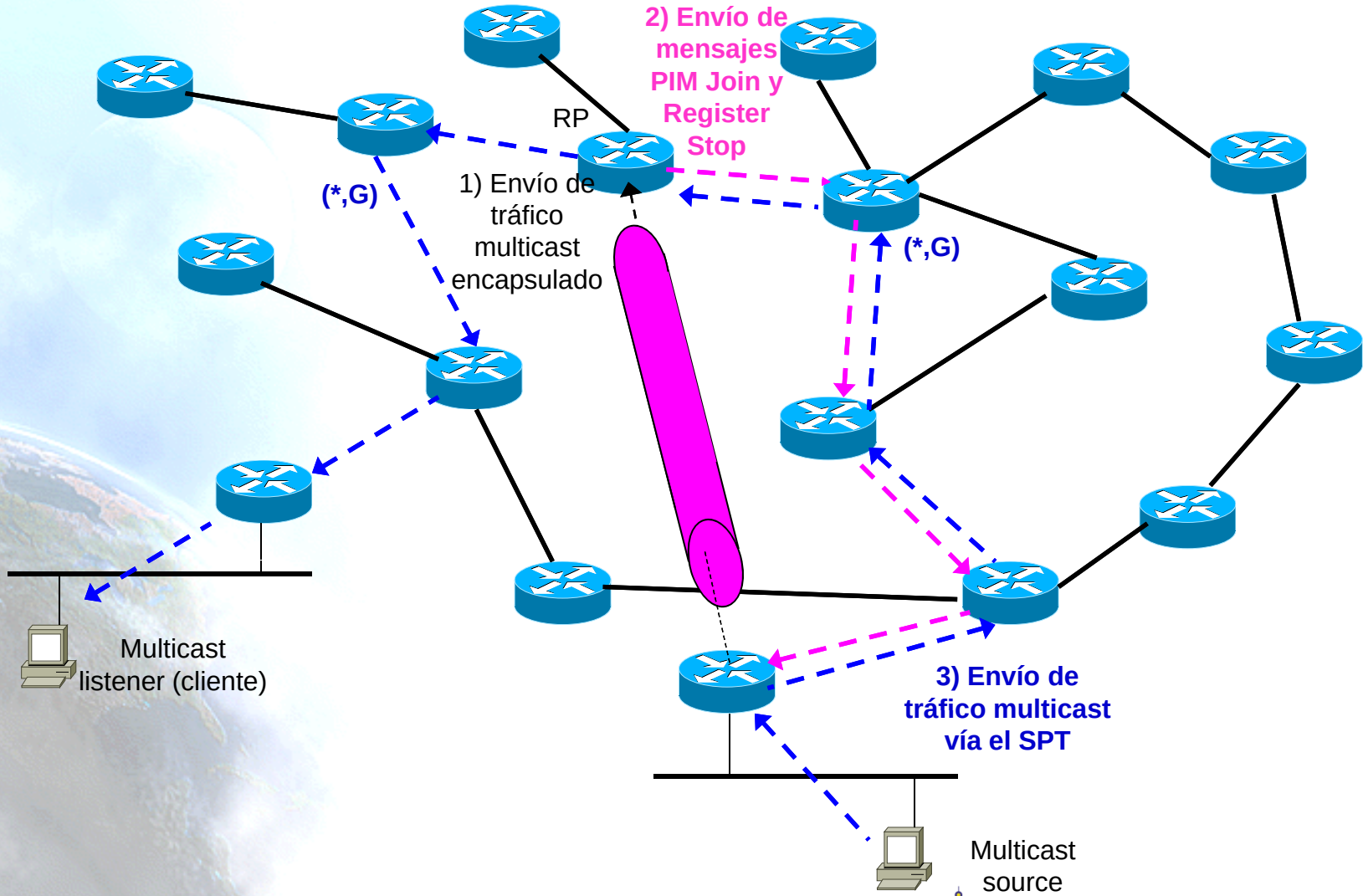


Escenarios Multicast IPv6

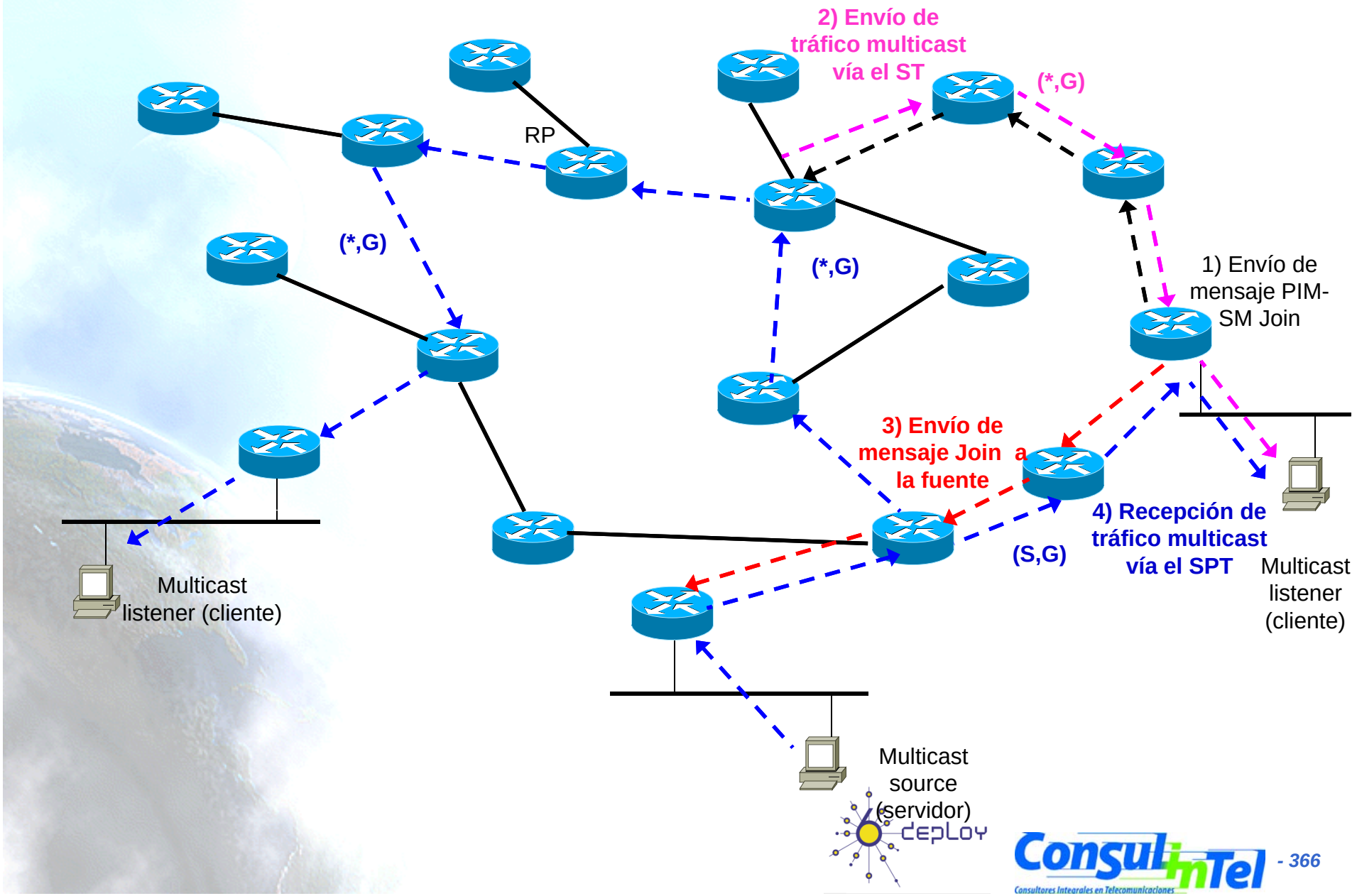


9.5 PIM-ASM

PIM-ASM: Registro de la fuente



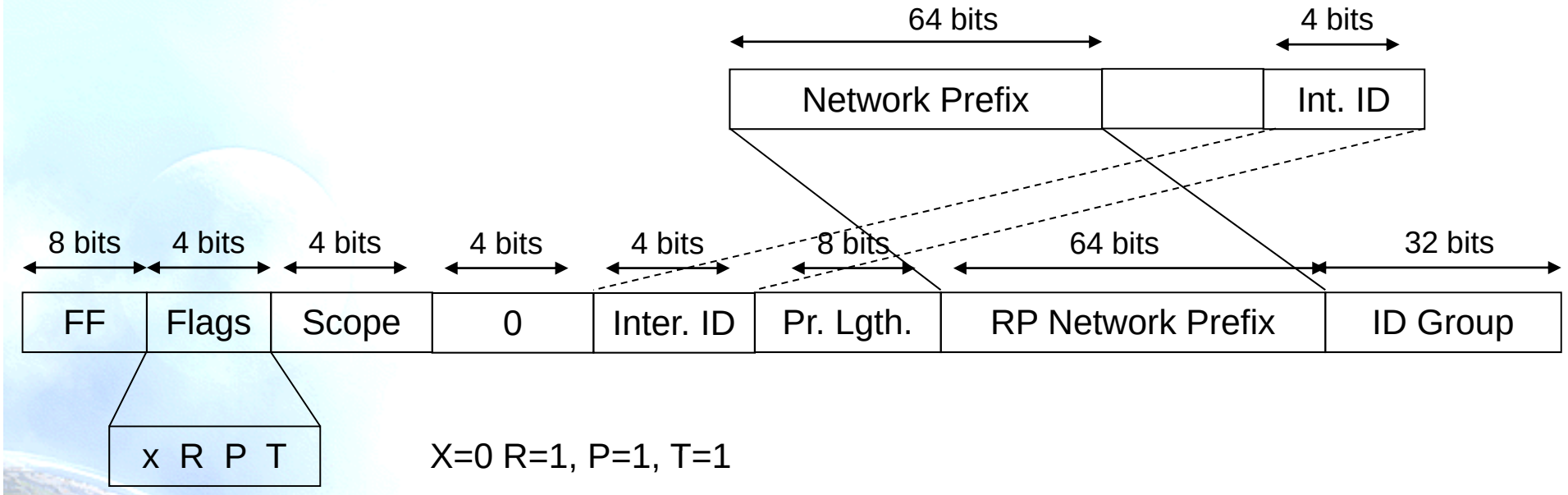
PIM-ASM: Unión del cliente



PIM-ASM

- Las acciones más importantes en PIM-ASM son:
  - Registro de la fuente en el RP
    - Es necesario registrar la fuente multicast en el RP antes de enviar paquetes multicast al grupo
    - El registro en el RP se hace a través de un túnel unidireccional entre el encaminador que alberga la fuente (Designated Router, DR) y el RP
    - El registro se hace encapsulando el trafico multicast y enviándolo por el túnel hasta el RP
    - El RP construye el (S,G) SPT enviando mensajes PIM Join
    - El RP avisa a la fuente del grupo (S,G), para detener la encapsulación del tráfico multicast, enviando mensajes de Register Stop
    - La fuente de (S,G) envía del trafico multicast hacia el RP vía el SPT entre ellos
  - Unión del cliente (listener) al grupo multicast
    - Una vez que el cliente expresa vía MLD su interés en unirse al grupo multicast (*,G), su DR envía mensajes PIM-SM Join al RP para construir el ST
    - Una vez que los mensajes de PIM-SM llegan al RP, el tráfico multicast se envía por el ST recién construido
    - Cuando el tráfico multicast llega al DR, este extrae la fuente multicast y entonces puede enviar los mensajes PIM-SM join a la fuente para construir el SPT y recibir trafico vía el SPT mas que por el ST
      - Optimización de prestaciones

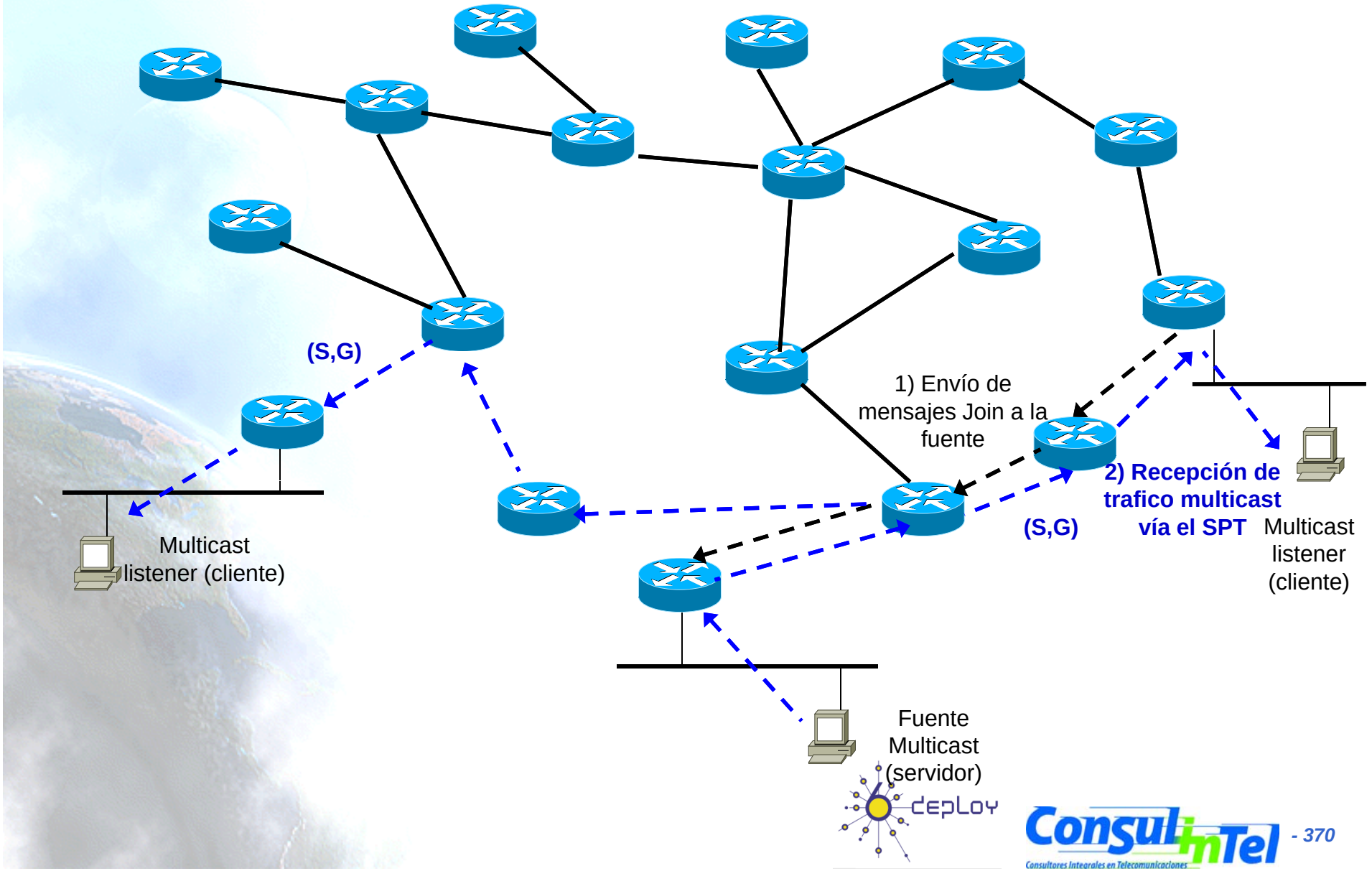
RP Embebido



- RP en PIM-ASM se puede configurar manualmente
- Embedded RP es otra opción en PIM-ASM para especificar el RP para un grupo multicast (*,G)
- Es un procedimiento para incluir la dirección IPv6 unicast del RP dentro de la dirección de un grupo multicast
- Se basa en las direcciones del grupo multicast con un prefijo-unicast descrito en el RFC 3306
  - Existen además algunas banderas que indican la presencia de la dirección del RP dentro de la dirección del grupo multicast

9.6 PIM-SSM

Funcionamiento de PIM-SSM



PIM-SSM

- Los clientes conocen información sobre el grupo y la fuente del grupo al que quieren unirse
- El funcionamiento es similar al de PIM-SM cuando los clientes del DR envían mensajes de PIM-SM Join a la fuente para construir el SPT
- No hay necesidad de un RP
  - La implementación y la gestión es más sencilla

9.7 Aspectos prácticos

Aplicaciones Multicast IPv6 (1)

- Beacon
- MAD FLUTE
- pcm6cast
- Freamp
- Windows Media Player
- VLC
- VIC, RAT, SDR, NTE, WBD
- VRVS (alfa)
- ISABEL
- Mas Información http://www.m6bone.net

Aplicaciones Multicast IPv6 (2)

- Iperf (Gracias a Carlos Barcenilla, UPM)

```
[pc1 iperf]#./iperf -c ff16::2222 -u -V -T 5
------------------------------------------------------------
Client connecting to ff16::2222, UDP port 5001
Sending 1470 byte datagrams
Setting multicast TTL to 5
UDP buffer size:  110 KByte (default)
------------------------------------------------------------
[  3] local 2001:db8::2115 port 32768 connected with ff16::2222 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  1.25 MBytes  1.05 Mbits/sec
[  3] Sent 893 datagrams
(none):/usr/apps/iperf #


[pc2 iperf]# ./iperf -s -u -B ff16::2222 -V -T 5
------------------------------------------------------------
Server listening on UDP port 5001
Binding to local address ff16::2222
Joining multicast group  ff16::2222
Receiving 1470 byte datagrams
UDP buffer size: 64.0 KByte (default)
------------------------------------------------------------
```

Aplicaciones Multicast IPv6 (3)

- **ssmping/ssmpingd**
- Verifica si hay conectividad SSM entre dos hosts IPv4/IPv6
- Se ejecuta "ssmping <host>“, entonces ssmping se une a la dupla (S,G) donde (hosts,ff3e::4321:1234)
- http://www.venaas.no/multicast/ssmping/

```
[consulintel@lacnic ssmping-0.6]$ ./ssmping -6 -I eth0 -c 50 2001:800:40:2b18:2b0:d0ff:fe16:76fc
ssmping joined (S,G) = (2001:800:40:2b18:2b0:d0ff:fe16:76fc,ff3e::4321:1234)
pinging S from 2001:1820:1a::2
  unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=0 dist=10 time=164.701 ms
  unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=1 dist=10 time=173.912 ms
multicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=1 dist=5 time=174.710 ms
  unicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=2 dist=10 time=193.795 ms
multicast from 2001:800:40:2b18:2b0:d0ff:fe16:76fc, seq=2 dist=5 time=195.473 ms

[consulintel@lacnic ssmping-0.6]$ ./ssmping -6 -I eth0 -c 50 2001:800:40:2a0a:2c0:26ff:fe50:2115
ssmping joined (S,G) = (2001:800:40:2a0a:2c0:26ff:fe50:2115,ff3e::4321:1234)
pinging S from 2001:1820:1a::2
  unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=0 dist=9 time=163.997 ms
  unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=1 dist=9 time=161.113 ms
multicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=1 dist=4 time=162.104 ms
  unicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=2 dist=9 time=161.357 ms
multicast from 2001:800:40:2a0a:2c0:26ff:fe50:2115, seq=2 dist=4 time=161.898 ms
```

10. DNS IPv6

DNS IPv6: Introducción (1)

- Se **definieron** varios elementos para dar soporte IPv6 al DNS:
  - Para resolución directa RRs: **AAAA** y A6
  - Para resolución inversa: dominios IP6.INT e **IP6.ARPA**, DNAME y PTR RR, además de las notaciones **nibble** y bit-string

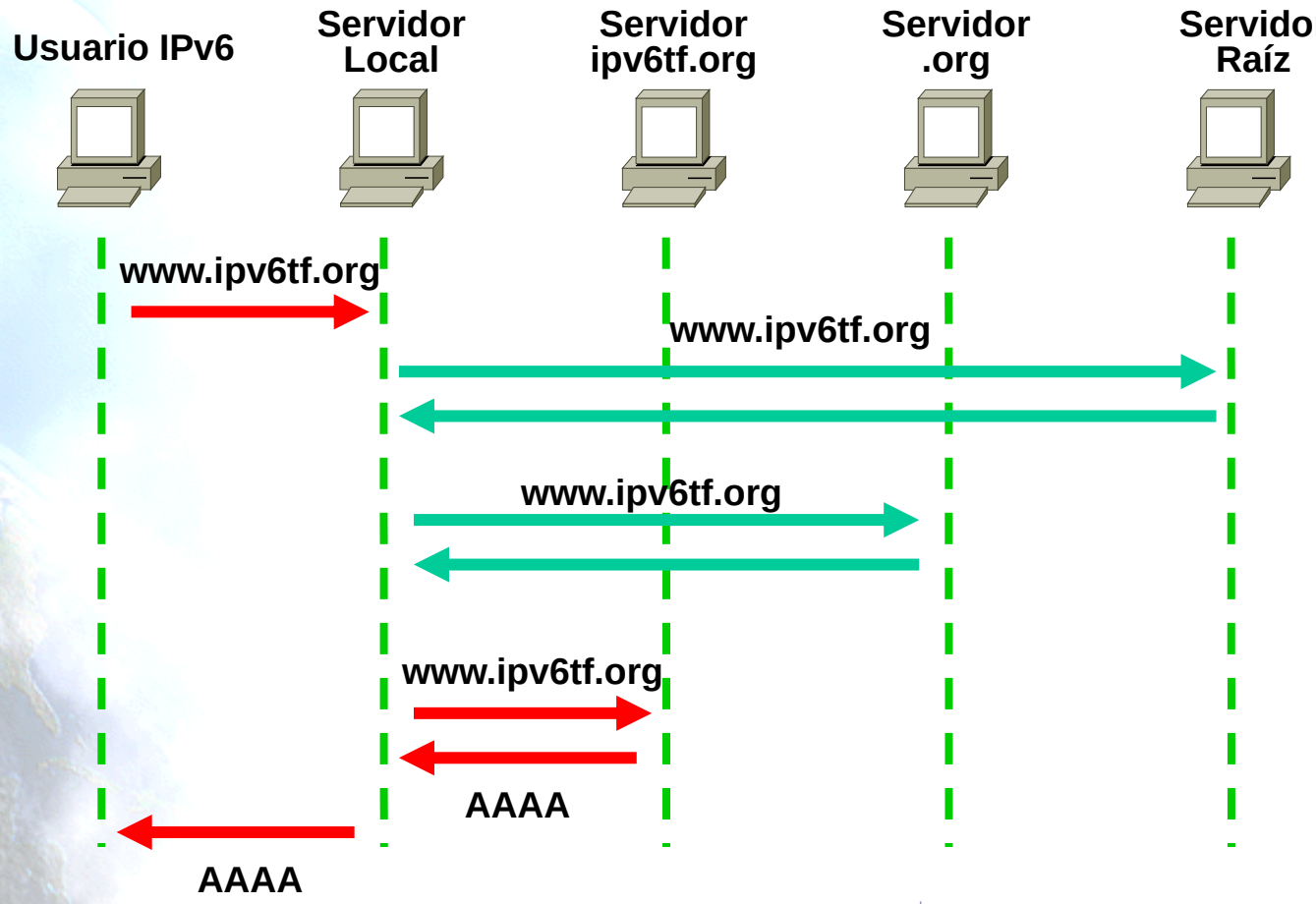
- 1995: AAAA, nibble e IP6.INT (RFC1886)
- 2000: A6, bit-string e IP6.ARPA (RFC2874)
- 2002: A6 y bit-string -> Experimental y DNAME -> Deprecado (RFC3363)

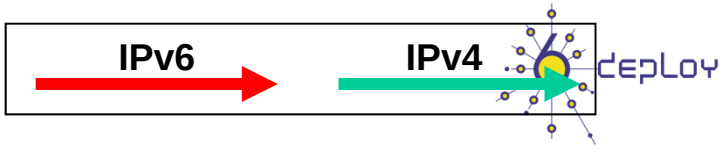
DNS IPv6: Introducción (2)

- Nos centraremos en los elementos usados hoy en día (RFC3596):
  - AAAA
  - IP6.ARPA
  - PTR
  - usando notación con nibbles (4 bits en hex)

DNS IPv6: Transporte vs. Contenido

- Diferencia entre transporte y contenido





DNS IPv6: Recomendaciones

- IPv4 e IPv6 coexistirán, 3 tipos de servidores:
  - Solo IPv4 -> alcanzable sólo por IPv4
  - Solo IPv6 -> alcanzable solo por IPv6
  - Doble-pila -> alcanzable por ambos
- Se debe evitar la fragmentación del espacio de nombres, esto ocurre cuando el proceso de resolución recursiva se rompe (e.g. cuando solo un NS IPv6 es autoritativo para un dominio, resultando que un servidor DNS solo IPv4 no podrá seguir la cadena de resolución).
- IDEA: compatibilidad hacia atrás.
- Políticas administrativas (RFC3901)
  - Todo servidor recursivo debe ser solo IPv4 o doble-pila.
  - Toda zona DNS debe ser servida al menos por un servidor autoritativo alcanzable sobre IPv4.

DNS IPv6: Estado actual (1)

- **Clientes**: Buen soporte DNS IPv6
- **Servidores**: Muy buen soporte: BIND, nsd, newbie, maradns and djbdns [8][9]
- Implantanción extendida a nivel **TLD** (.fr, .uk, .jp, etc.)
- Actualmente en curso: Ha comenzado la implantación en los **Servidores Raíz** (7/13)

DNS IPv6: Estado actual (2)

- Desde Julio 2004 con el anuncio de ICANN [1] sobre el soporte de direcciones IPv6 en los servidores raíz, muchos TLDs lo han añadido [2].
- ICANN realizó un trabajo previo sobre el tema de IPv6 en los servidores raíz por medio de RSSAC [7] y SSAC [6]. Resultado:
  - Informe sobre 'glue' AAAA en servidores raíz[5]: zonas raíz y 'root hints'.
  - Se está llevando a cabo un estudio sobre tráfico real en algunos servidores raíz.
  - Estado Transporte: B, F, H, I, J, L y M eran capaces de IPv6 pero no con una conectividad con calidad para producción.
- Actualmente (root zone 2008121200) [3] 7 Servidores Raíz tienen direcciones IPv6 de forma oficial. Se hizo el anuncio [4] y desde el 4 de Febrero de 2008 son alcanzables por IPv6.

DNS IPv6: Referencias

[1] Next-generation IPv6 Address Added to the Internet's Root DNS Zone: http://www.icann.org/announcements/announcement-20jul04.htm

[2] IANA Administrative Procedure for Root Zone Name Server Delegation and Glue Data: http://www.iana.org/procedures/delegation-data.html

[3] Root Zone Hints File in IANA Popular Links: http://www.iana.org/popular.htm

[4] IPv6 Address Added for Root Servers in the Root Zone: http://www.icann.org/announcements/announcement-04feb08.htm

[5] "Accommodating IP Version 6 Address Resource Records for the Root of the Domain Name System", ICANN, March 2007. http://www.icann.org/committees/security/sac018.pdf

[6] ICANN Security and Stability Advisory Committee (SSAC). http://www.icann.org/committees/security/

[7] ICANN DNS Root Server System Advisory Committee (RSSAC). http://www.icann.org/committees/dns-root/

[8] Internet Systems Consortium http://www.isc.org

[9] DeepSpace6 - Current Status of IPv6 Support for Networking Applications http://www.deepspace6.net/docs/ipv6_status_page_apps.html

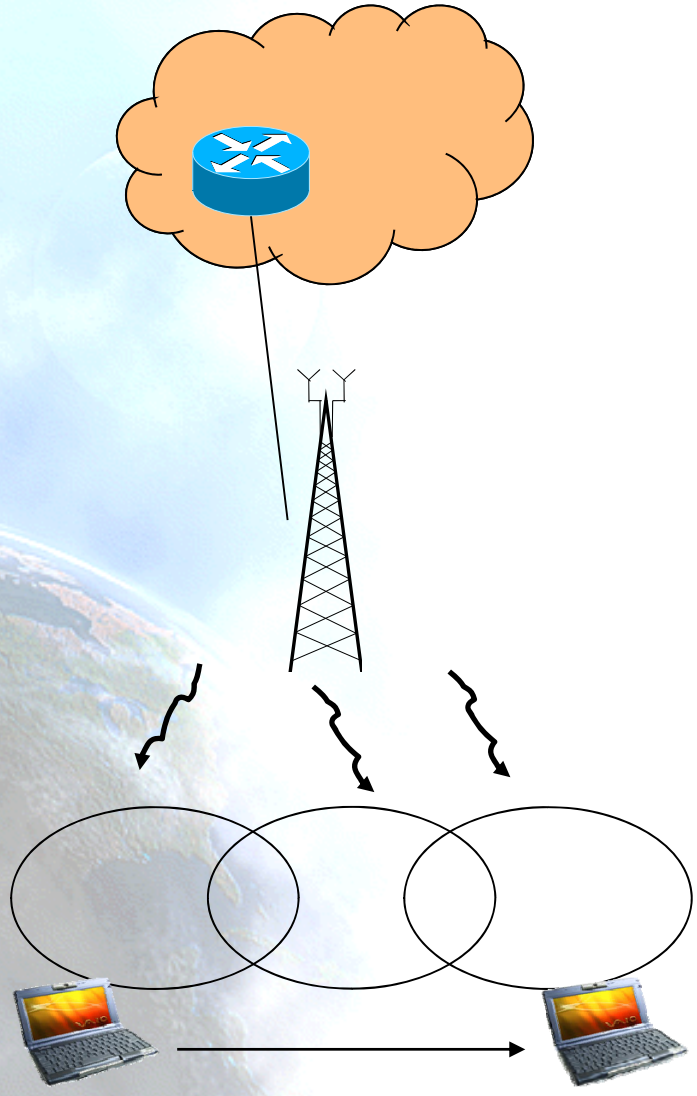
11. Movilidad IPv6

11.1 Conceptos de movilidad

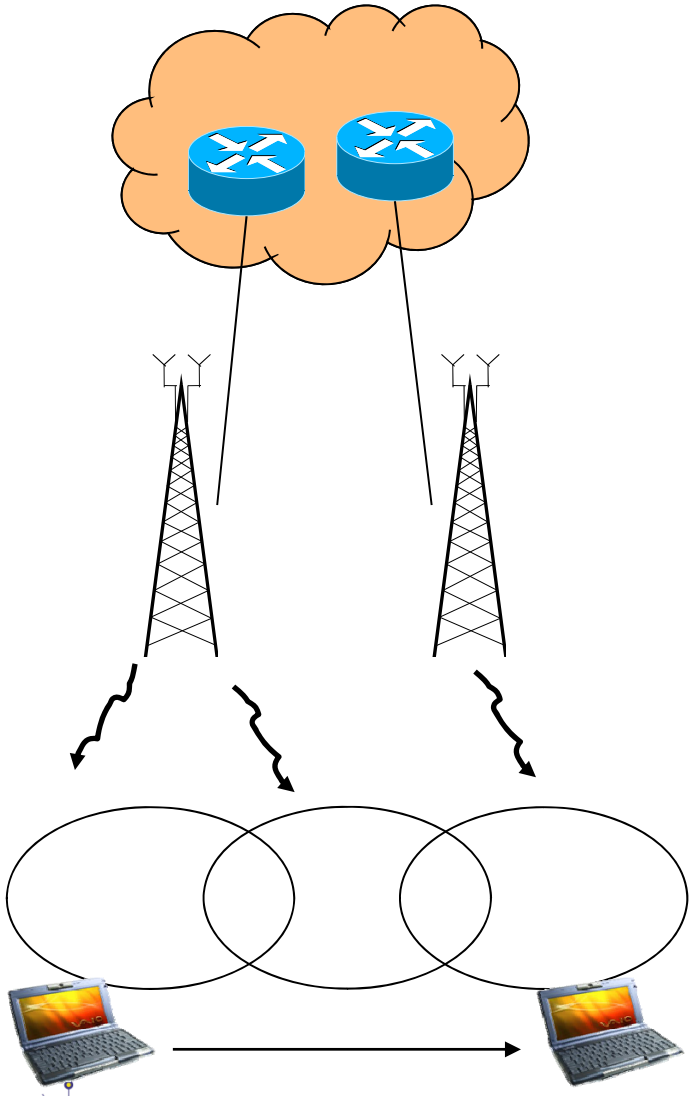
11.2 Movilidad IPv6

11.1 Conceptos de movilidad

Diferentes Visiones Movilidad



Movilidad nivel II



Movilidad nivel III

Movilidad en la capa IP

- Implicaciones
  - Comunicación = f(IP_fuente, Pto_fuente, IP_dest., Pto_dest)
  - Si cambia la dirección IP la comunicación no es posible
- Requisitos
  - Compatibilidad con aplicaciones y sistemas actuales
  - No modificación de encaminadores
  - Transparente a las aplicaciones
  - ……

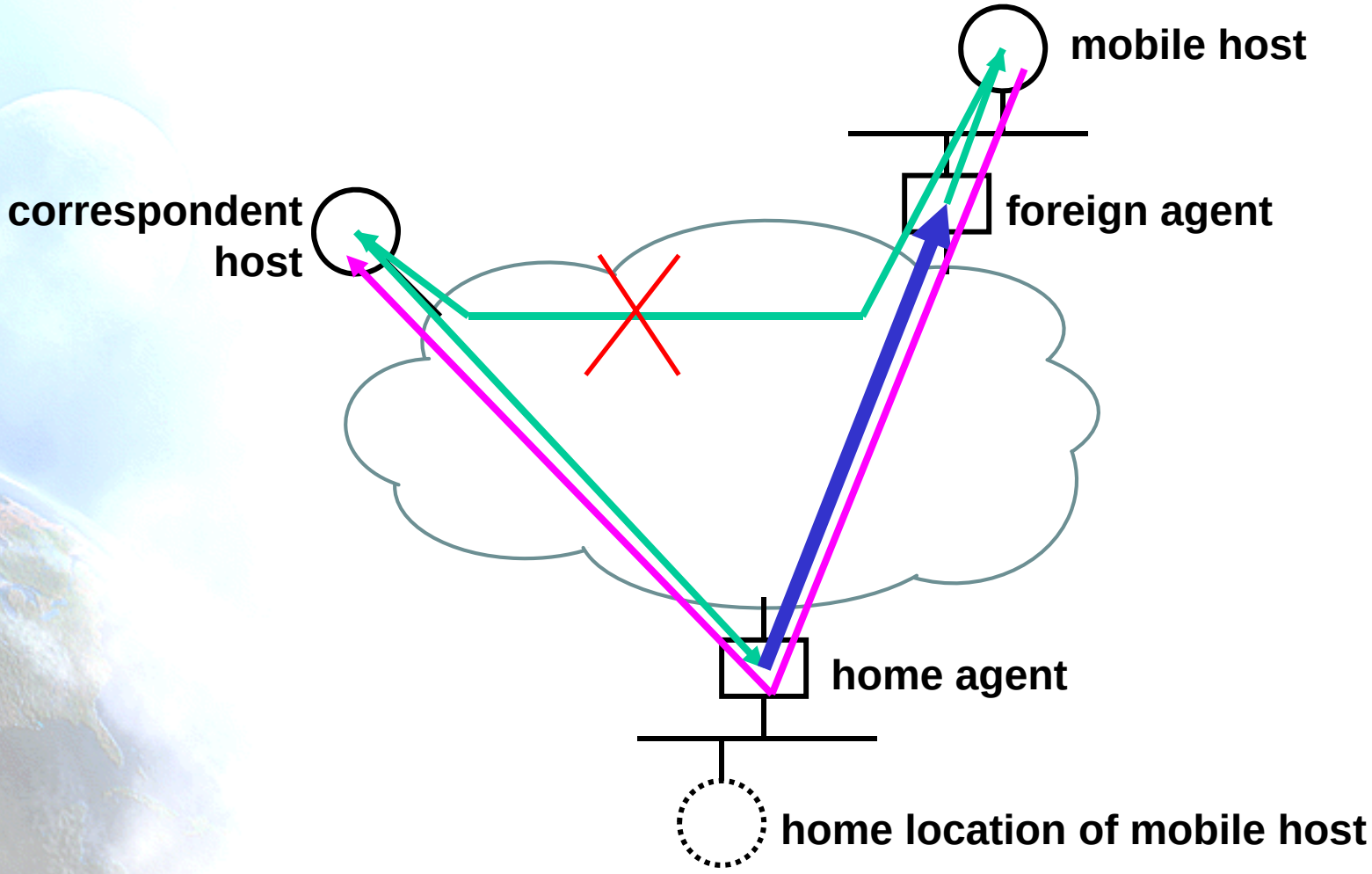
Movilidad IPv4 (1)

- Conceptos
  - **Home Agent**: Servidor en la “Home Network” (HN).
  - **Foreing Agent**: Servidor en la red visitada.
  - **Mobile Node**: Nodo en movimiento.
  - **Correspondent Node**: Nodo con el que comunica el MN.
  - **Home Address**: Dirección obtenida en la HN.
  - **Care of Address**: Dirección obtenida en la red visitada y que representa al MN. Es una dirección que está dentro del FA, en una interfaz virtual (CoA).

Movilidad IPv4 (2)

- Un MN tiene una o más direcciones de origen
  - relativamente estables; asociadas con el nombre del host a través de DNS
- Cuando descubre que se encuentra en una subred diferente (cuando no esta en su subred de origen), adquiere una dirección diferente
- Registra la “care-of-address” obtenida con su HA
- Los paquetes enviados a la “home address” del MN , son interceptados por el HA y reenviados al FA, utilizando encapsulación.
- Los paquetes enviados por el MN se entregan de dos maneras alternativas:
  - Los envía al FA y este los renvía con la “home address”
    - Problemas si se implementa “ingress-filtering” en el ISP
  - Crea un túnel con el HA y se los reenvía

Movilidad IPv4 (3)



Movilidad IPv4 (4)

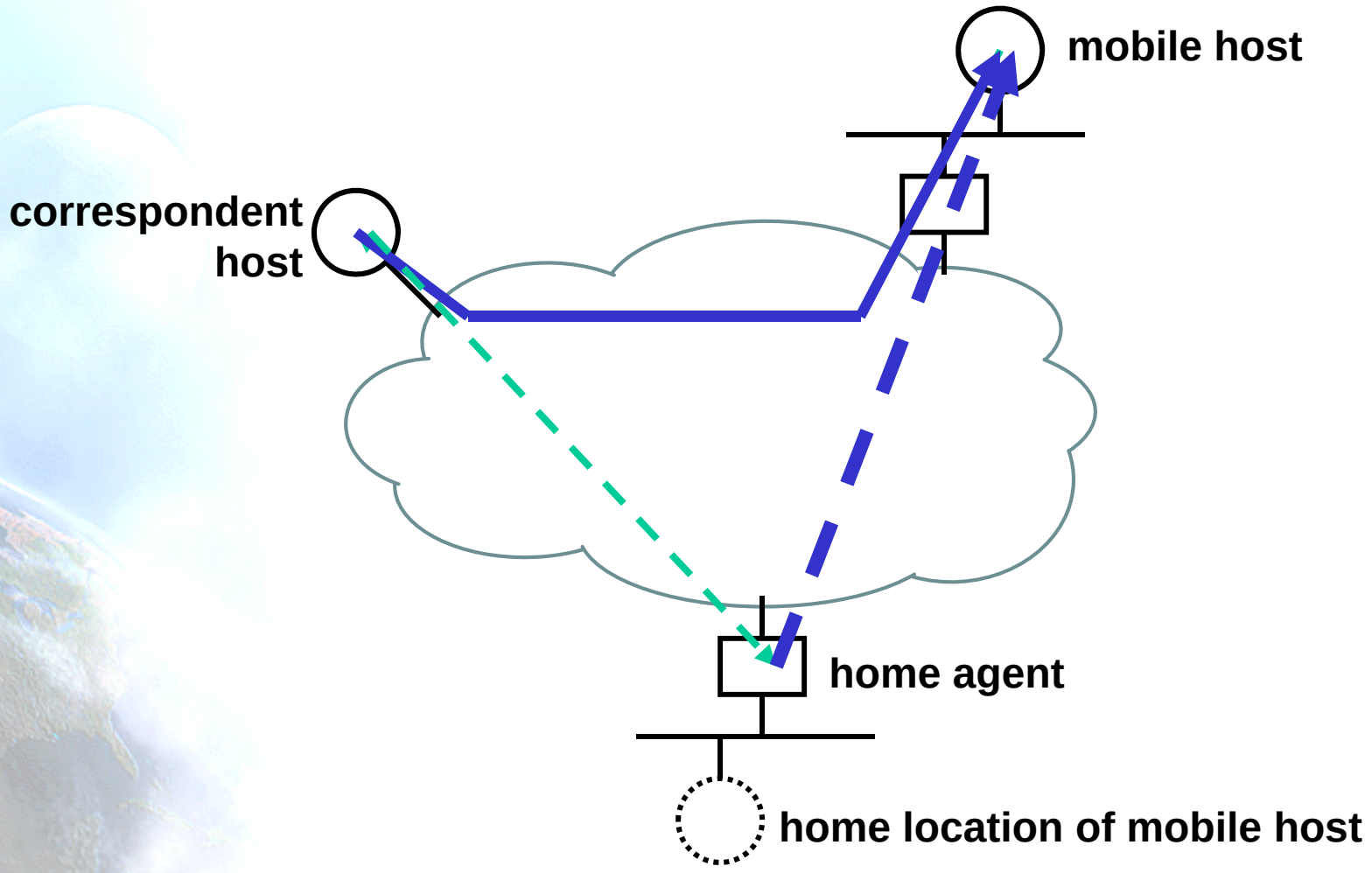
- Seguridad
  - Necesario autenticación
    - FA → HA
    - MN→ FA
  - Se suele usar infraestructaras de AAA
- Problemas con IPv4
  - Escasez de direcciones IPv4 públicas
    - Los FA suelen ser estar detrás de encaminadores que implementan NAT y modifican los paquetes
  - Escasez y complejidad en el despligue de AAA
- Consecuencia
  - MIPv4 inoperativa

11.2 Movilidad IPv6

Movilidad IPv6 (1)

- IPv6 posee dos características importantes que ayudan enormemente en el diseño de una solución de movilidad
  - Descubrimiento de Vecinos (ND)
  - Auto-configuración
  - Se emplean para
    - Mobile Prefix Discovery: Similar a los RS y RA
    - Dynamic HA Address Discovery. Puede haber más de un HA
- Existen numerosas diferencias con MIPv4, las más reseñables:
  - La CoA se configura en el propio MN, no en un FA
  - No existe FA
  - Las relaciones de autenticación son diferentes
    - MN → HA
    - MN → CN
  - Se emplea ESP, luego no se requiere AAA
  - Optimización de Rutas

Movilidad IPv6 (2)



Movilidad IPv6 (3)

- La optimización de rutas es una de las características más reseñables:
  - Inicialmente CN → HA → MN
  - MN → CN (incluyendo una Header Option con su “home address”
    - Alternativamente MN → HA → CN mediante un túnel
  - Cuando se establece comunicación entre el CN y el MN: CN → MN
- Esto elimina la posibilidad de que el HA sea un “single point-of-failure”
- También se eliminan retardos innecesarios cuando la distancia CN → MN es menor que CN → HA → MN
- Se requiere una autenticación previa entre CN → MN

Despliegue de Movilidad IPv6

- MIPv6 ha sido estandarizada en 2004
  - Funciona con configuraciones manuales No escalable
- El despliegue de MIPv6 como un servicio de red tiene varias implicaciones
  - Definir un mecanismo escalable que proporcione los parámetros para que MIPv6 funcione sin la intervención manual del usuario
    - “Bootstrapping”: proporciona HoA, los credenciales de cifrado del usuario y la dirección del HA
  - Resolver algunos problemas de red que impiden que MIPv6 funcione en cualquier red:
    - Balanceo de carga de los HA
    - Funcionamiento de MIPv6 en redes de acceso IPv4
    - Atravesamiento de Firewalls
- La mayoría de estos temas se han evaluado en el seno del IETF, en los WG:
  - http://www.ietf.org/html.charters/mip6-charter.html (cerrado)
  - http://www.ietf.org/html.charters/mext-charter.html
- También existen proyectos de I+D que abordan esa problemática:
  - http://www.ist-enable.eu
  - http://www.nautilus6.org

Estándares

- Mobility Support in IPv6
  - RFC3775 – Junio 2004
- Uso de IPsec para proteger la señalización de Mobile IPv6 entre Nodos Móviles y Home Agents
  - RFC3776 – Junio 2004
  - RFC4877 – Abril 2007 (actualiza RFC 3776)
- Otros: RFC4823, RFC4225, RFC4285, RFC4295, RFC4887, RFC4449, RFC4584, RFC4640, RFC4882

Gracias !!

Contacto:

- Cesar Olvera (Consulintel): cesar.olvera@consulintel.es

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

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