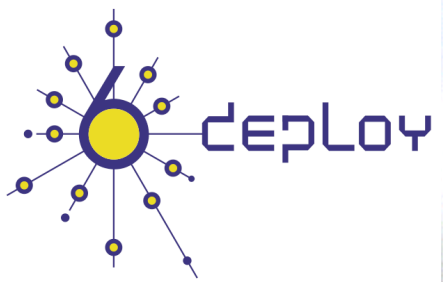
Tutorial Práctico de IPv6

ESNOG - GORE 2

Barcelona

Octubre 2008

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



Contenido

1. Introducción a IPv6
2. Auto configuración, DHCPv6 y Prefix Delegation
3. Introducción a mecanismos de transición
4. IPv6 en tecnologías de banda ancha

1. Introducción a IPv6

1.1 Historia de IPv6
1.2 Ventajas de IPv6
1.3 Formatos de cabeceras y tamaño de paquetes
1.4 Direccionamiento IPv6
1.5 ICMPv6 y Neighbor Discovery
1.6 Movilidad IPv6
1.7 Estado actual 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, PLC, etc.

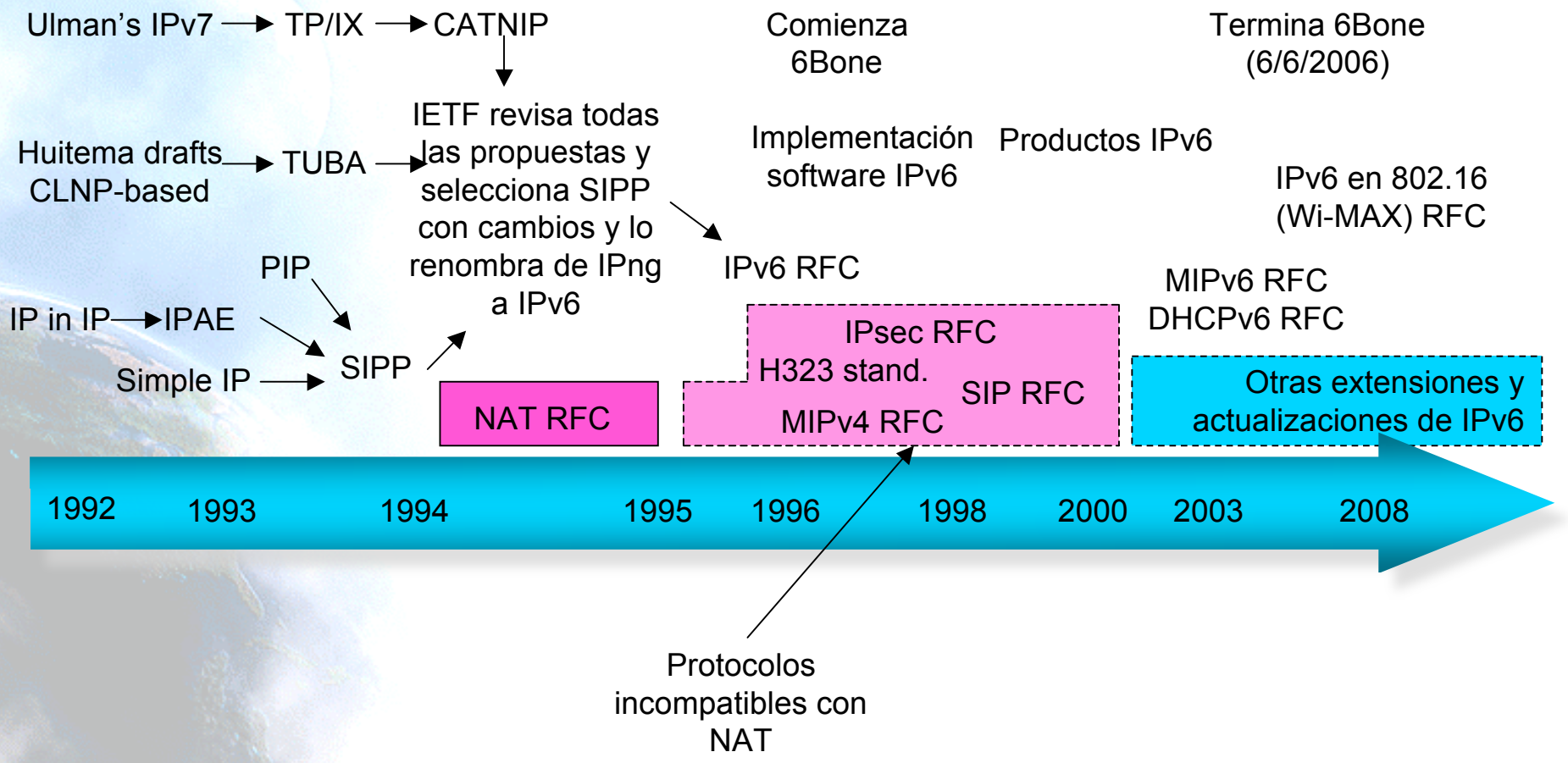
Requisitos de IPng

- 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

Evolución de IPng



Pero, ¿No es Verdad que aún quedan muchas Direcciones IPv4?

- ~ La mitad del espacio de direcciones IPv4 aún no ha sido utilizado
  - El tamaño de Internet se duplica cada año, ¿significa esto que sólo quedan unos pocos años?
- No, debido a que hoy negamos direcciones IPv4 públicas a la mayoría de los nuevos hosts
  - Empleamos mecanismos como NAT, PPP, etc. para compartir direcciones
- Pero nuevos tipos de aplicaciones y nuevos mecanismos de acceso, requieren direcciones únicas

¿Porqué NAT no es Adecuado?

- No funciona con gran número de “servidores”, es decir, dispositivos que son “llamados” por otros (ejemplo, Teléfonos IP)
- Inhiben el desarrollo de nuevos servicios y 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

1.3. Formatos de cabeceras y tamaño de paquetes

1.3.1 Terminología
1.3.2 Formato cabecera IPv6
1.3.3 Consideraciones sobre tamaño de paquete
1.3.4 Consideraciones sobre protocolos de capa superior
1.3.5 Jumbogramas

1.3.1Terminología

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

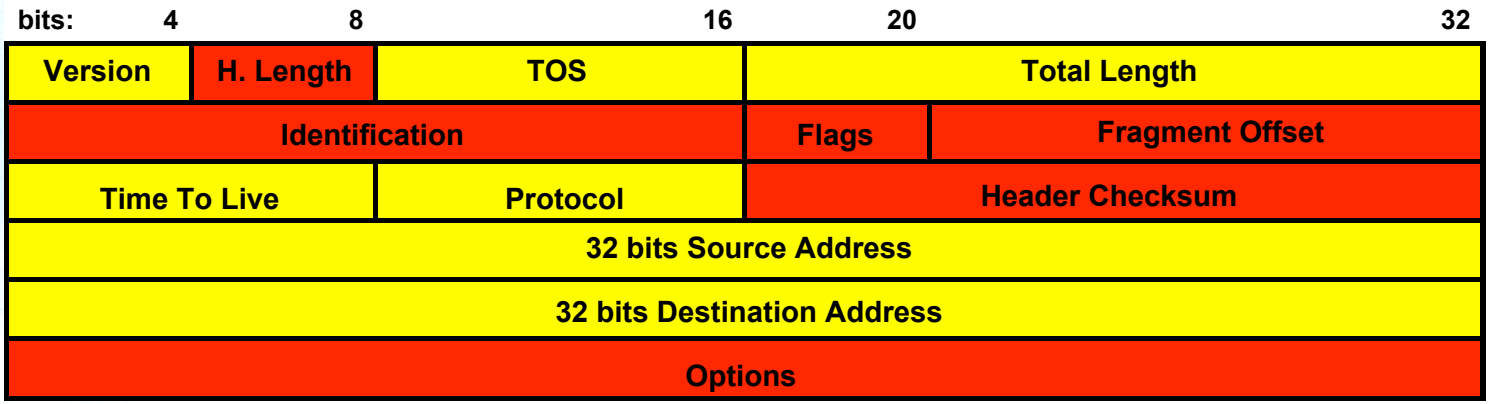
Terminología

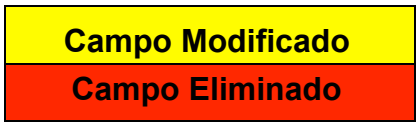
- **Node:** Dispositivo que implementa IPv6
- **Router:** Nodo que reenvía paquetes IPv6
- **Host:** Cualquier otro nodo que no es un router
- **Upper Layer:** Protocolo que está inmediatamente por encima de IPv6
- **Link:** Medio o entidad de comunicación sobre la que los nodos pueden comunicarse a 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

1.3.2 Formato cabecera IPv6

Formato de la Cabecera IPv4

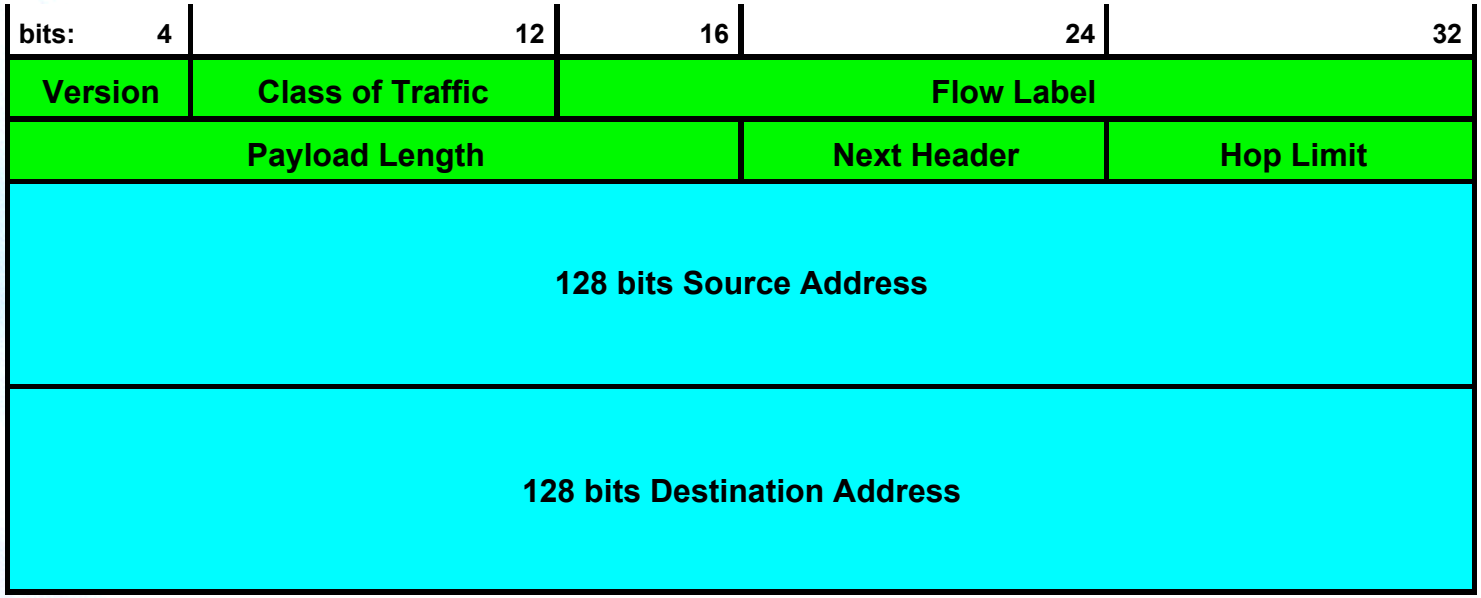
- 20 Bytes + Opciones (40 Bytes máximo)
  - Tamaño variable: 20 Bytes a 60 Bytes





Formato de la Cabecera IPv6

- Reducción de 12 a 8 campos (40 bytes)



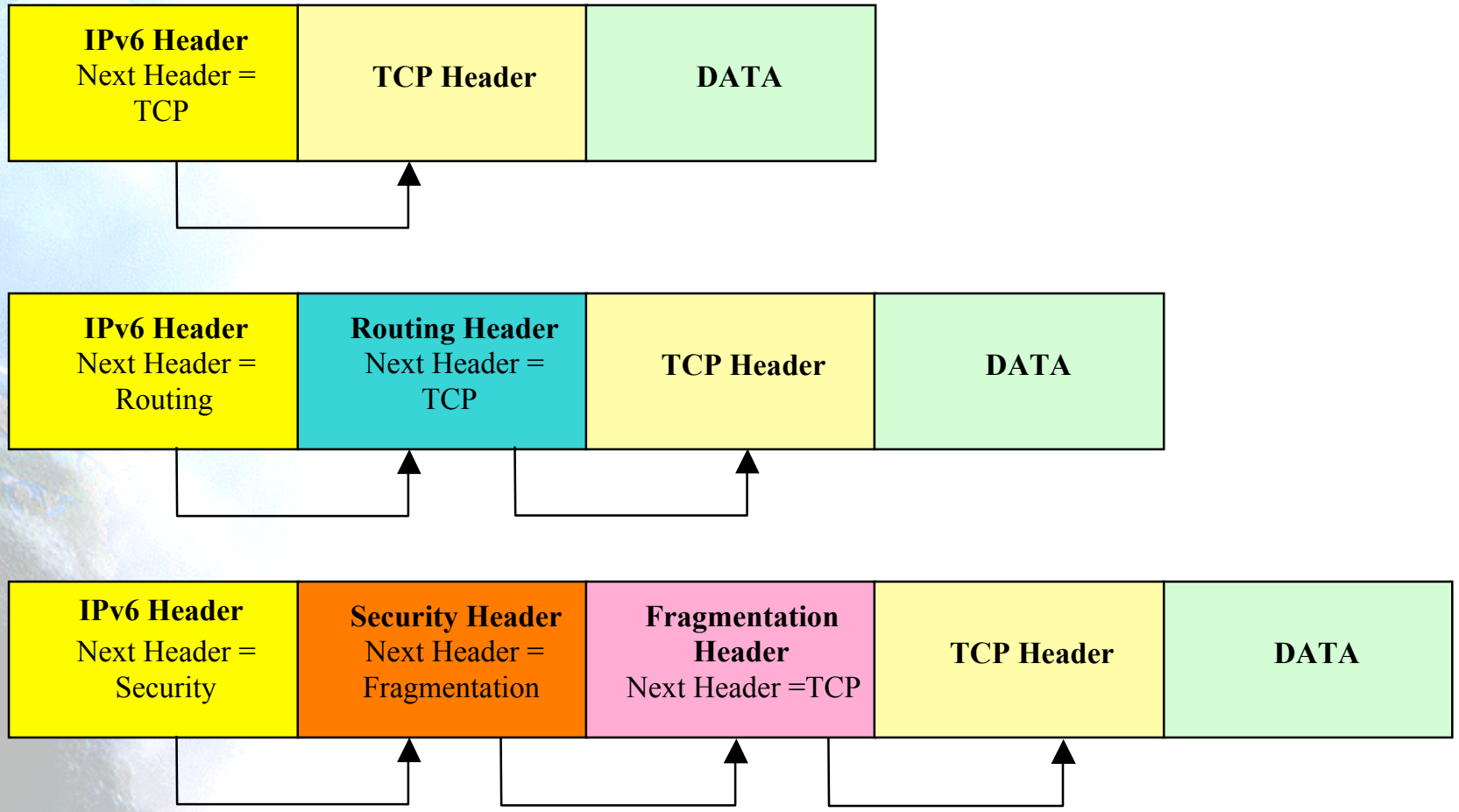
  - Evitamos la redundancia del checksum
  - Fragmentación extremo-a-extremo

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

Cabeceras de Extensión

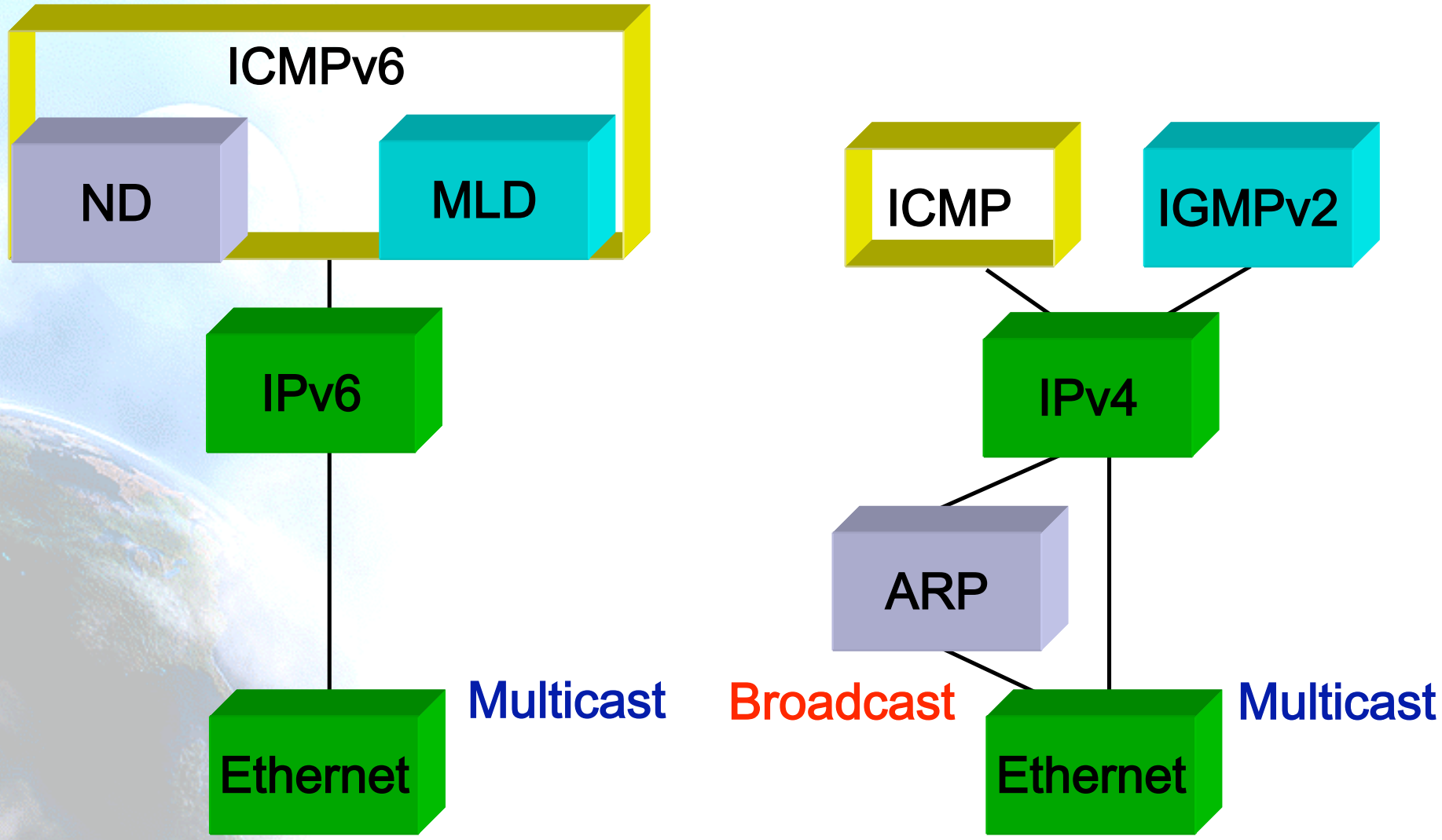
- Campo “Next Header”



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)
  - Detination 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)

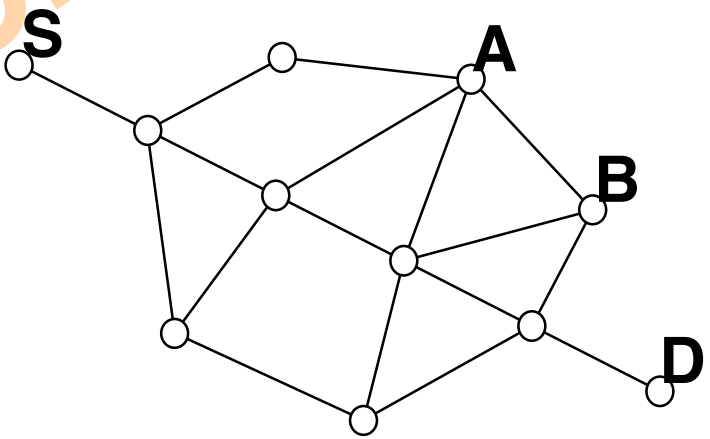
Plano de Control IPv4 vs. IPv6



Ejemplo: Uso de la cabecera de encaminamiento

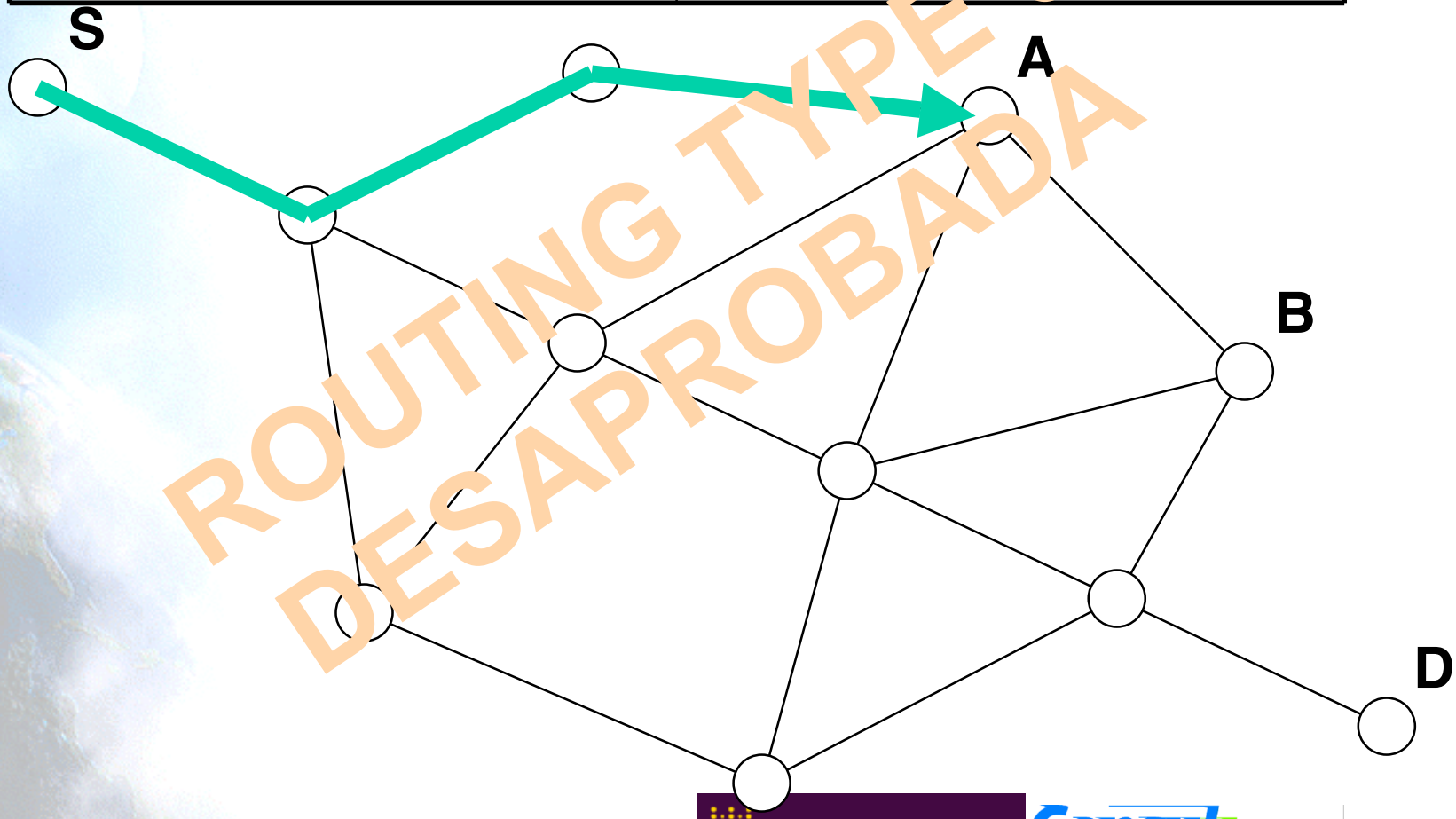
8 bits	8 bits unsigned	8 bits	8 bits unsigned
Next Header	**H. Ext. Length**	**Routing Type = 0**	**Segments Left**
Reserved = 0			
Address 1			
Address 2			
…			
Address n			

- Next Header = 43
- Routing Type = 0, donde:
  - Source Node: S
  - Destination Node: D
  - Intermediate Nodes: A & B



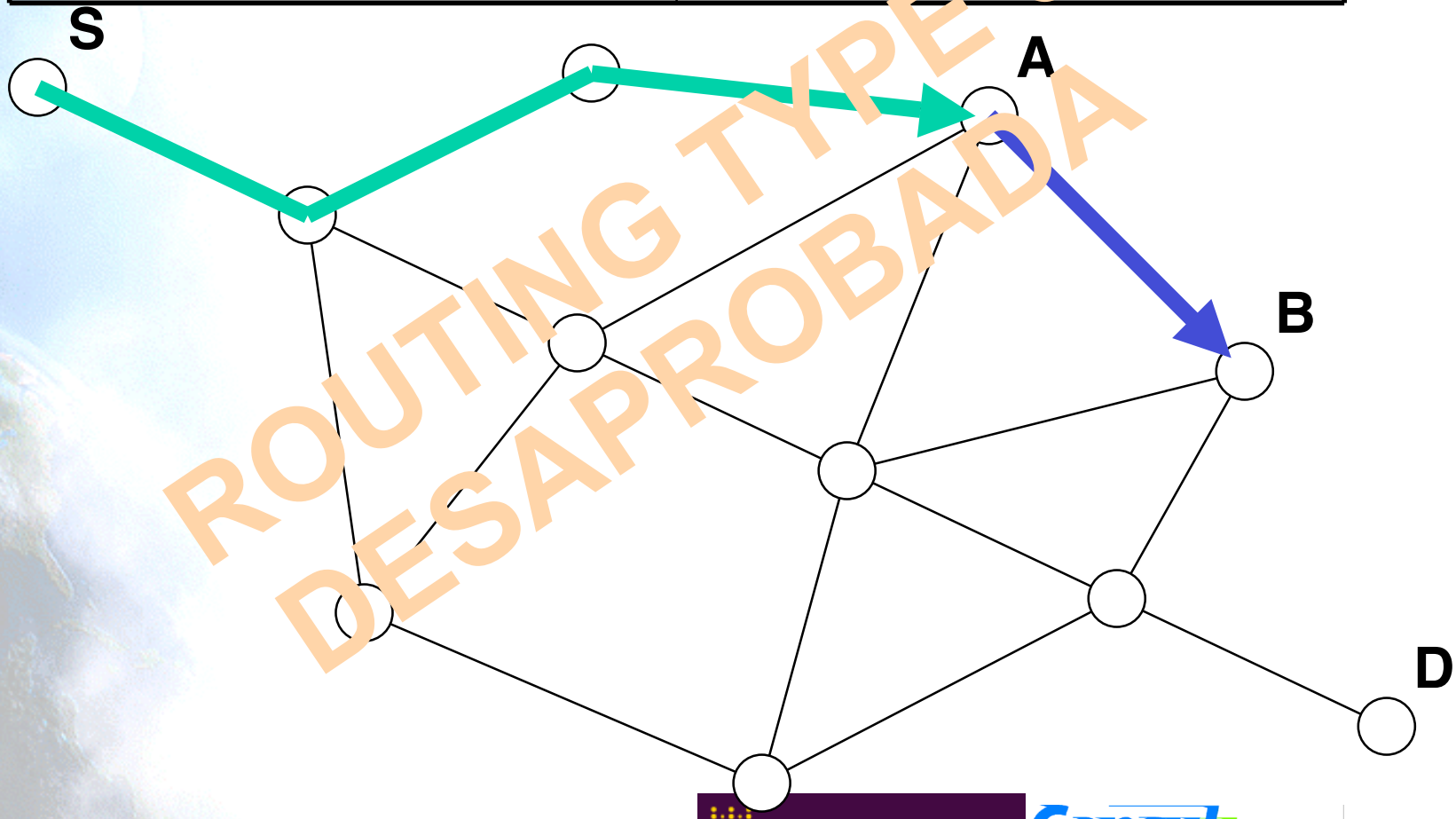
Ejemplo: Tramo S → A

IPv6 Base Header	Routing Header
Source Address = S Destination Address = A	H. Ext. Length = 4 Segments Left = 2 Address 1 = B Address 2 = D



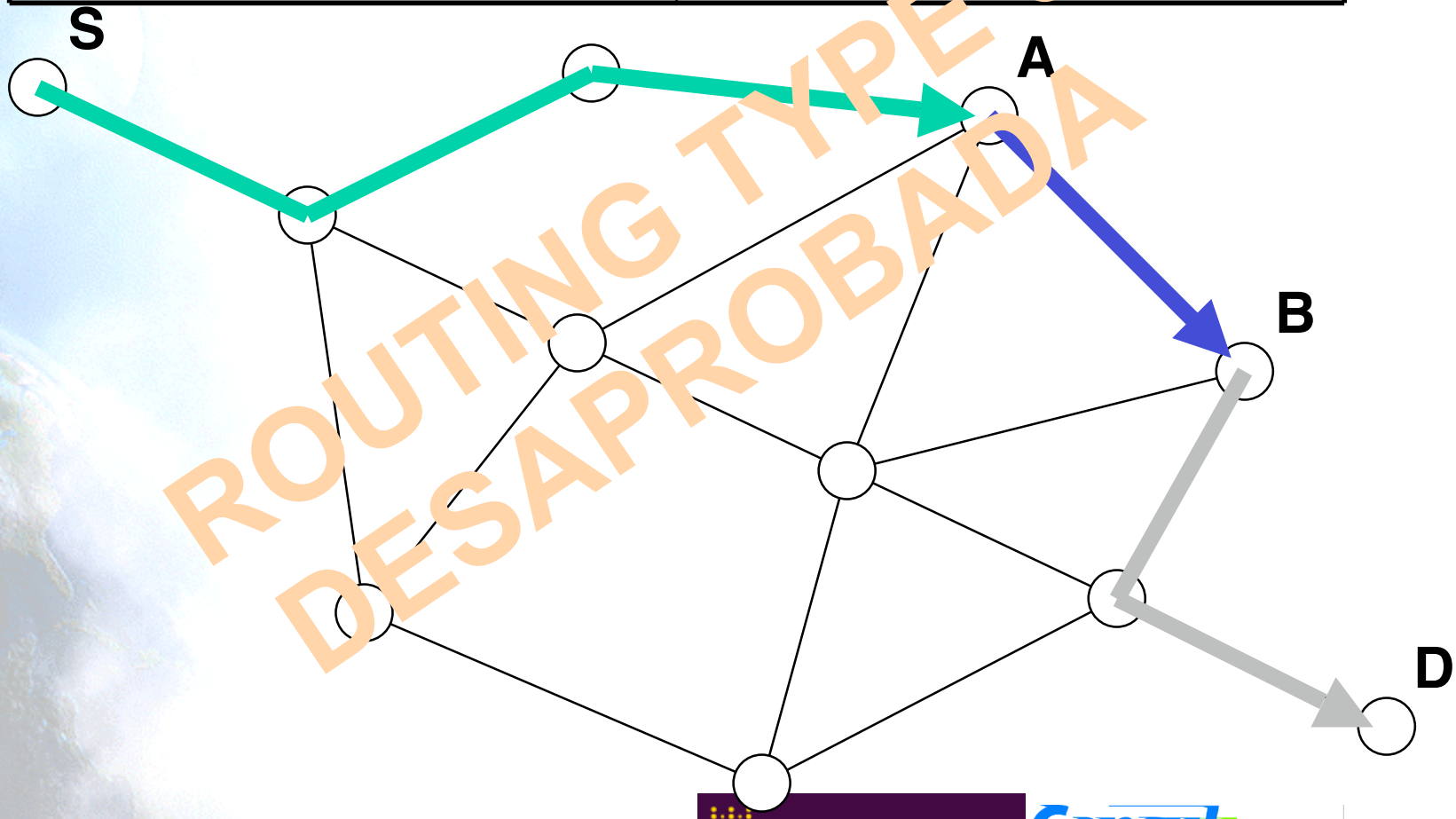
Ejemplo: Tramo A → B

IPv6 Base Header	Routing Header
Source Address = S Destination Address = B	H. Ext. Length = 4 Segments Left = 1 Address 1 = A Address 2 = D



Ejemplo: Tramo B → D

IPv6 Base Header	Routing Header
Source Address = S Destination Address = D	H. Ext. Length = 4 Segments Left = 0 Address 1 = A Address 2 = B

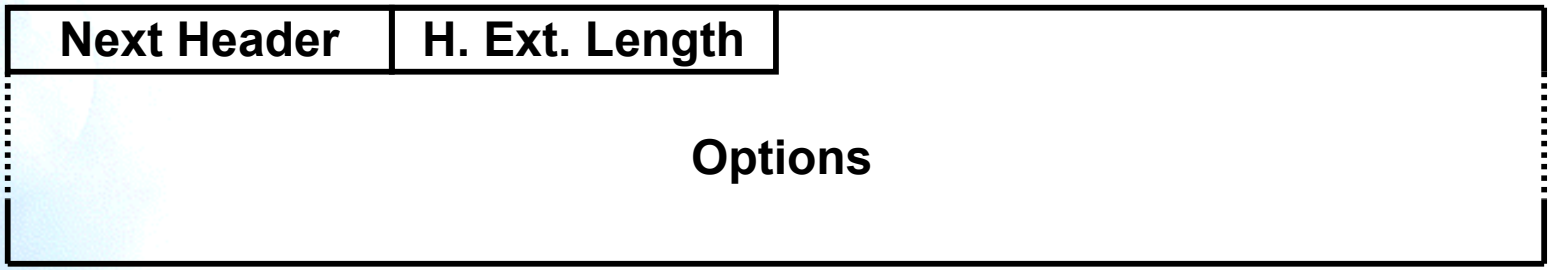


Cabecera Routing Type 0 (desaprobada)

- La cabecera de extensión “Routing Type 0” esta desaprobada en el RFC5095, debido a que puede ser utilizada de forma maligna para llevar a cabo ataques de tipo DoS
- Este posible ataque se fundamenta en lo siguiente:
  - Se obliga a los paquetes IPv6 a pasar por un determinado nodo
  - La dirección de uno de los nodos intermedios en el camino hasta el nodo destino puede aparecer mas de una vez
  - Como consecuencia se puede llevar a cabo un ataque de tipo DoS para obligar que gran cantidad de tráfico pase entre dos nodos, de manera repetida
  - Con un ataque a gran escala se consigue no solamente inhabilitar los dos nodos sino además todo el camino entre ambos
- El ataque es lo suficientemente serio como para inhabilitar este tipo de cabecera
  - Los nodos que reciban un paquete con esta cabecera procederán como se especifica en la sección 4.4 del RFC2460 acerca de cabeceras Routing con tipo no reconocido
- Como consecuencia el uso benigno de la cabecera tampoco se permite
  - Se podría especificar en el futuro otras extensiones para implementar esta funcionalidad
- 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

Cabeceras
Hop-by-Hop & Destination

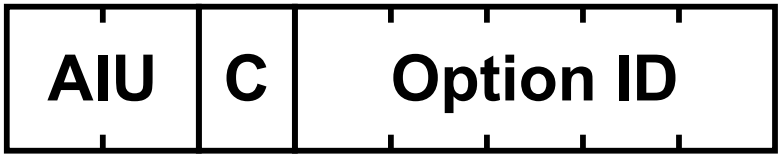
- Contenedores para opciones de longitud variable:



- Siendo Options =

- Valores para Next Header:
  - 0 para la cabecera Hop-by-Hop Option
  - 60 para la cabecera Destination Option

Opción “Type Encoding”



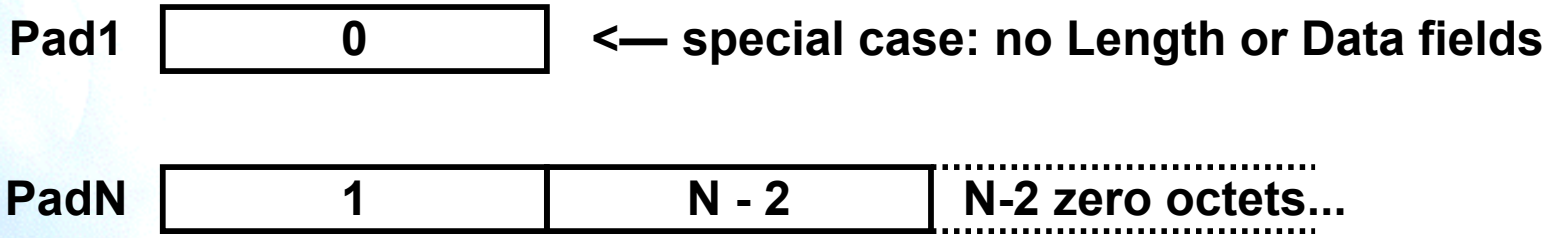
AIU — Action If Unrecognized: Acción si no se reconoce

00 — saltar la opción
01 — descartar el paquete
10 — descartar el paquete y
enviar un paquete ICMP Unrecognized Type a la fuente
11 — descartar el paquete y
enviar ICMP Unrecognized Type al origen
solo si el destino no es multicast

C — (1) si el campo Option Data cambia en ruta
(Hop-by-Hop Options solo)

Opción para alineamiento y relleno

Hay dos opciones para Padding:



- Se emplea para alinear posiciones de manera que los campos de datos multi-byte caen dentro de limites naturales
- Se usa para que el número de bytes de datos resultantes sea múltiplo de 8.

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				

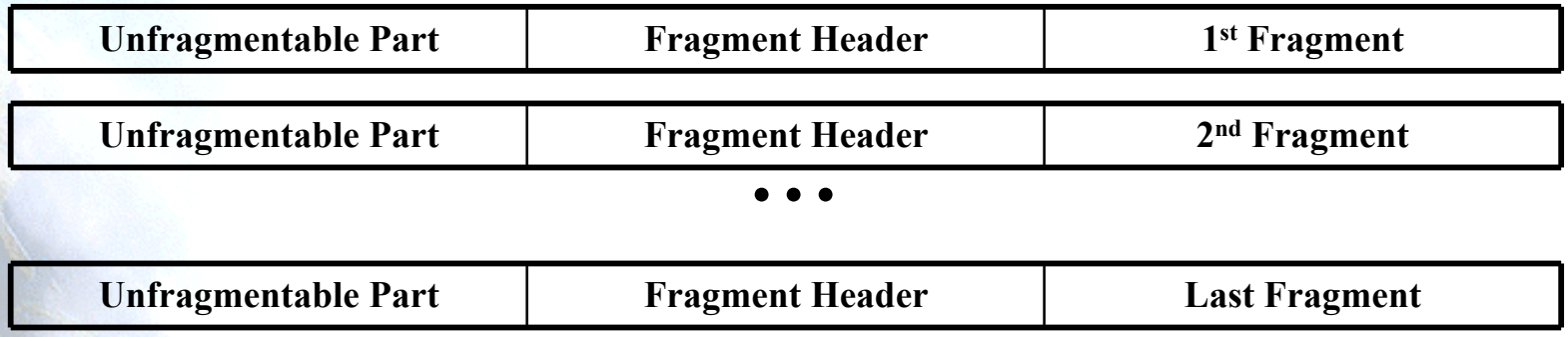
- Paquete Original (no fragmentado):

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

- Paquetes fragmentados:



1.3.3 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

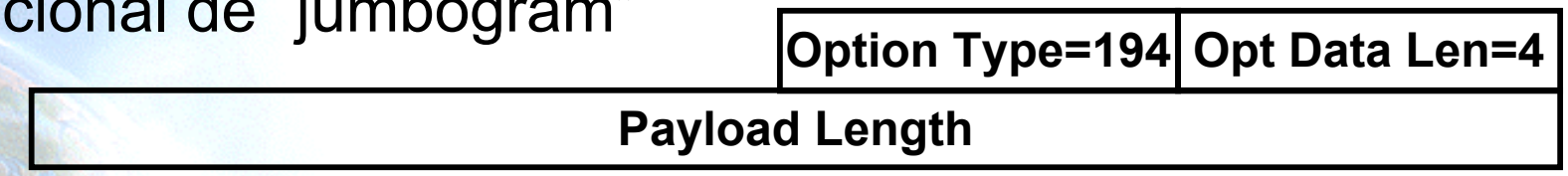
Next Header	Reserved	Fragment Offset	0 0 M
Original Packet Identifier			

- 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)

1.3.4 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.

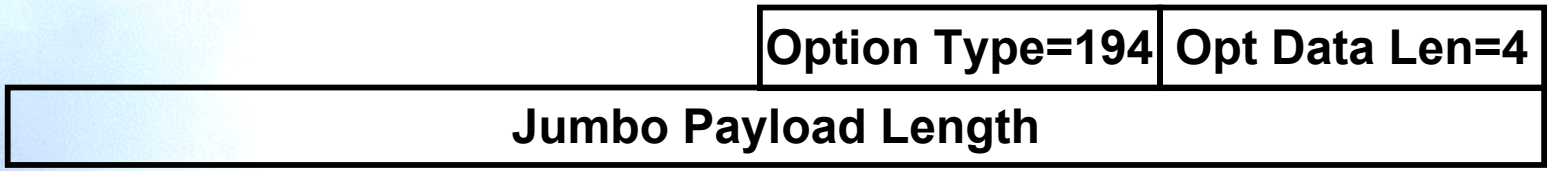
1.3.5 Jumbogramas

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

1.4. Direccionamiento IPv6

1.4.1 Tipos de Direcciones
1.4.2 Prefijo y representación
1.4.3 Direcciones IPv6 Unique Local
1.4.4 Identificadores de interfaz
1.4.5 Direcciones Multicast
1.4.6 Otras consideraciones

1.4.1 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 (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)

1.4.2 Prefijo y representación

Representación Textual de las Direcciones

Formato “preferido”:	2001:DB8:FF:0:8:811:200C:417A
Formato comprimido:	2001:DB8:0:0:0:0:0:43
	se comprime como 2001:DB8::43
IPv4-compatible:	::13.1.68.3 (desaprobada en RFC4291)
IPv4-mapped:	::FFFF:13.1.68.3
URL:	http://[2001:DB8::43]/index.html

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	(todo lo demás)	
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

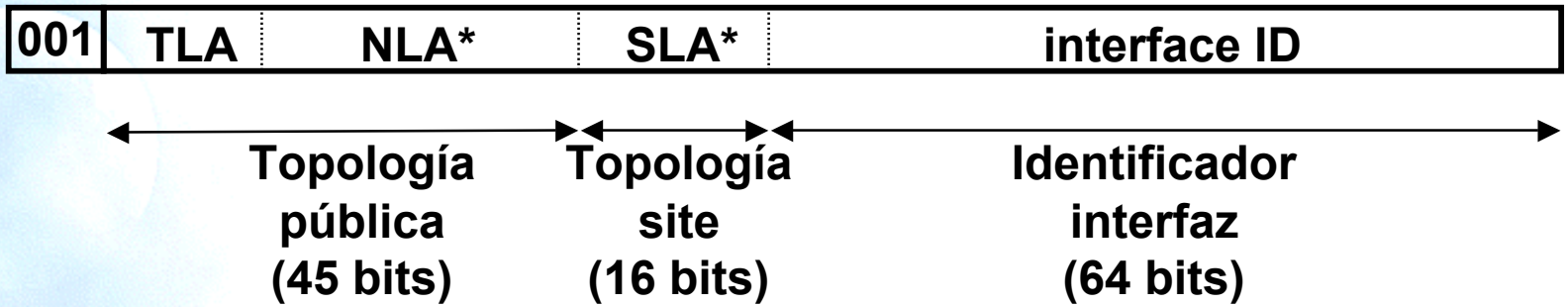
- Direcciones **Anycast** se asignan de los prefijos Unicast

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).

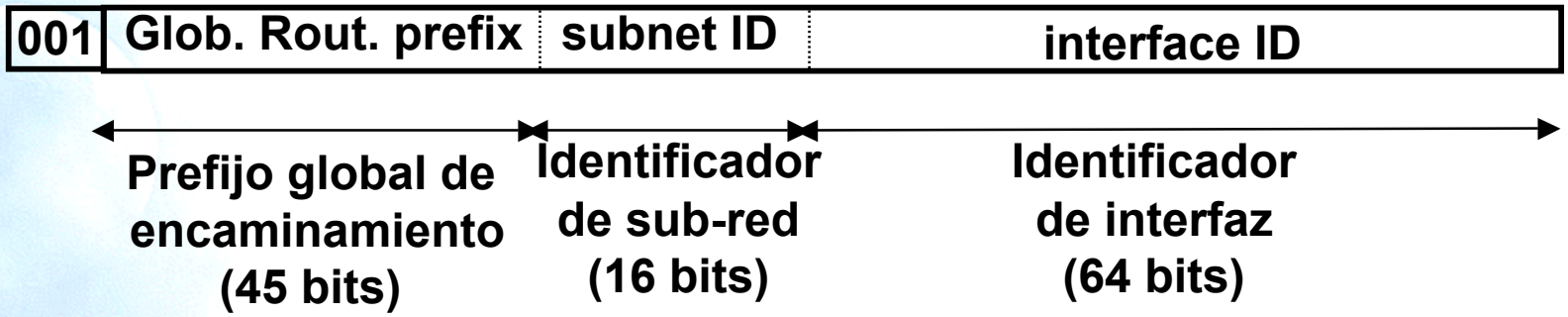
Aggregatable Global Unicast Addresses (RFC2374) (obsoleto)



- 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

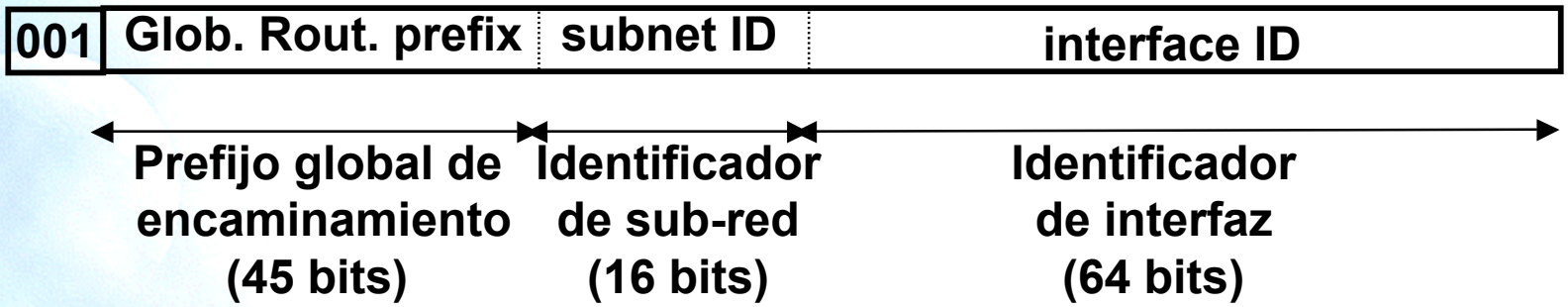
Dirección Global Unicast (RFC3587)



- 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

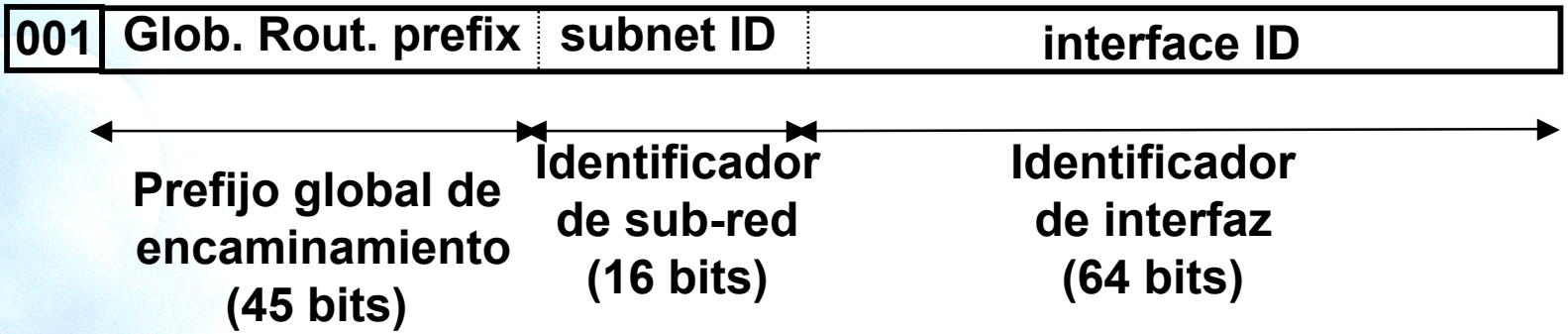
Dirección Global Unicast para 6Bone

(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

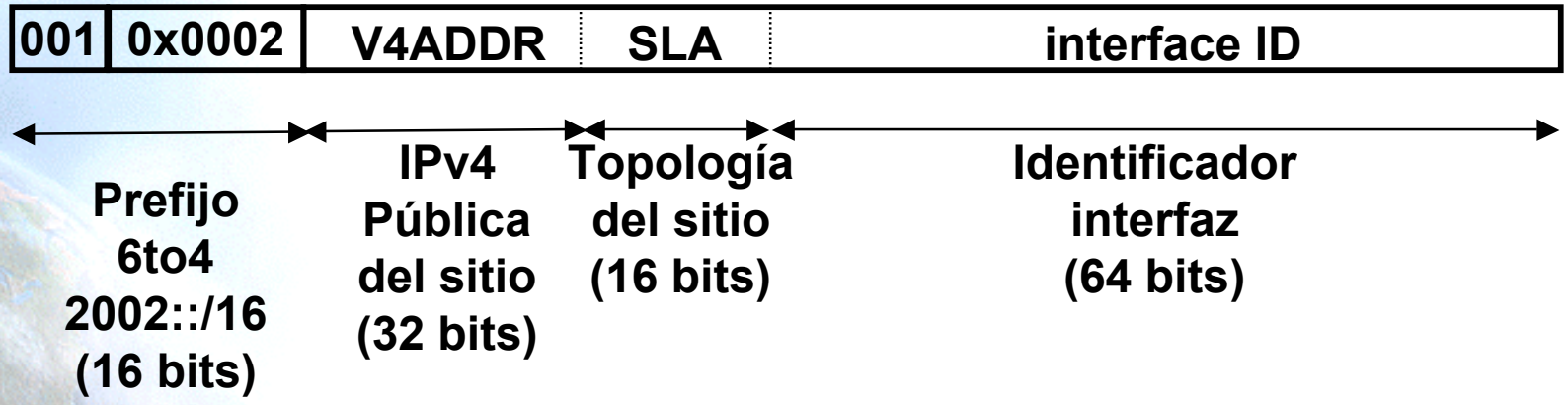
Dirección Global Unicast para Servicios de Producción



- 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)

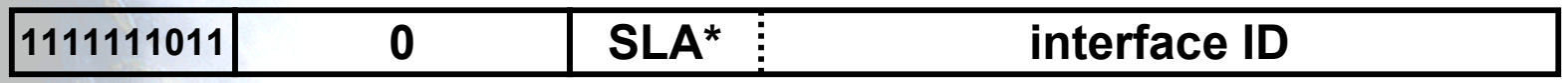
- RFC3056: Connection of IPv6 Domains via IPv4 Clouds
- Prefijo asignado **2002::/16**
- Para asignado a los sitios **2002:V4ADDR::/48**



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**)

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)**



Direcciones para documentación (RFC3849)

- **2001:DB8::/32**

- RFC3849: IPv6 Address Prefix Reserved for Documentation
- Prefijo IPv6 unicast reservado para ejemplos en
  - –RFCs
  - –Libros,
  - –Documentos
  - –etc.

1.4.3 Direcciones IPv6 Unique Local

Unique Local IPv6 Unicast Addresses - IPv6 ULA (RFC4193)

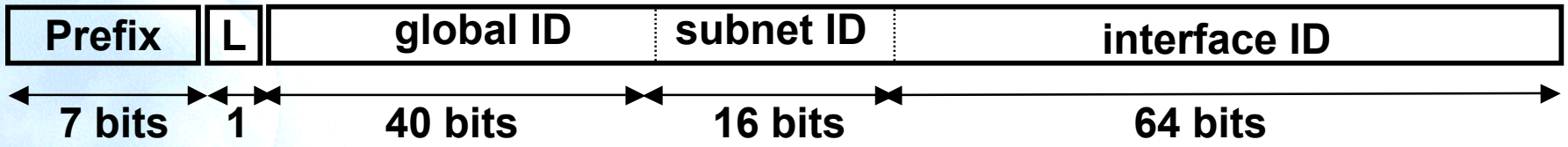
- Prefijo global con alta probabilidad de ser único
- Para comunicaciones locales, normalmente dentro de un "site"
- No son prefijos que vayan a ser encaminados en la Internet Global
- Son prefijos encaminables dentro de un área más limitada, como un determinado "site"
- Incluso podrían ser encaminados 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

Direcciones unicast IPv6 ULA asignadas centralmente (1)

- Direcciones locales asignadas centralmente
  - vs direcciones locales asignadas localmente
- Último Draft:
  - draft-ietf-ipv6-ula-central-02
  - Junio 2007
  - Define las características y requisitos para las direcciones locales IPv6 asignadas centralmente en el marco definido en IPv6 ULA – RFC4193

Direcciones unicast IPv6 ULA asignadas centralmente (2)

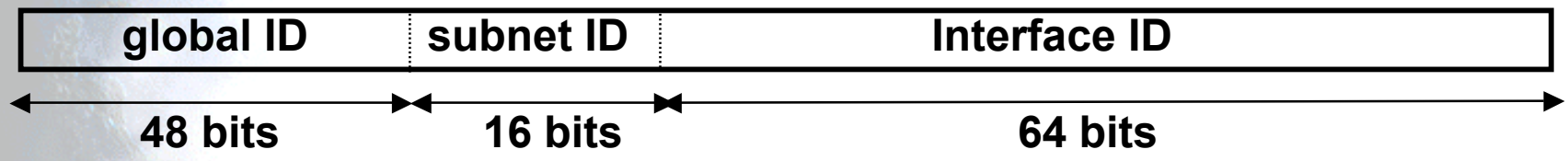
- La principal diferencia entre ambas asignaciones:
  - Las asignadas centralmente son direcciones únicas y la asignación puede ser revocada para resolver cualquier disputa en relación a asignaciones duplicadas
- Se recomienda que los “sites” que planeen hacer uso de ULA, usen prefijos asignados centralmente ya que se evita cualquier posibilidad de conflicto, aunque no existe ninguna obligación de hacerlo, solo 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

1.4.4 Identificadores de interfaz

Identificadores de Interfaz

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

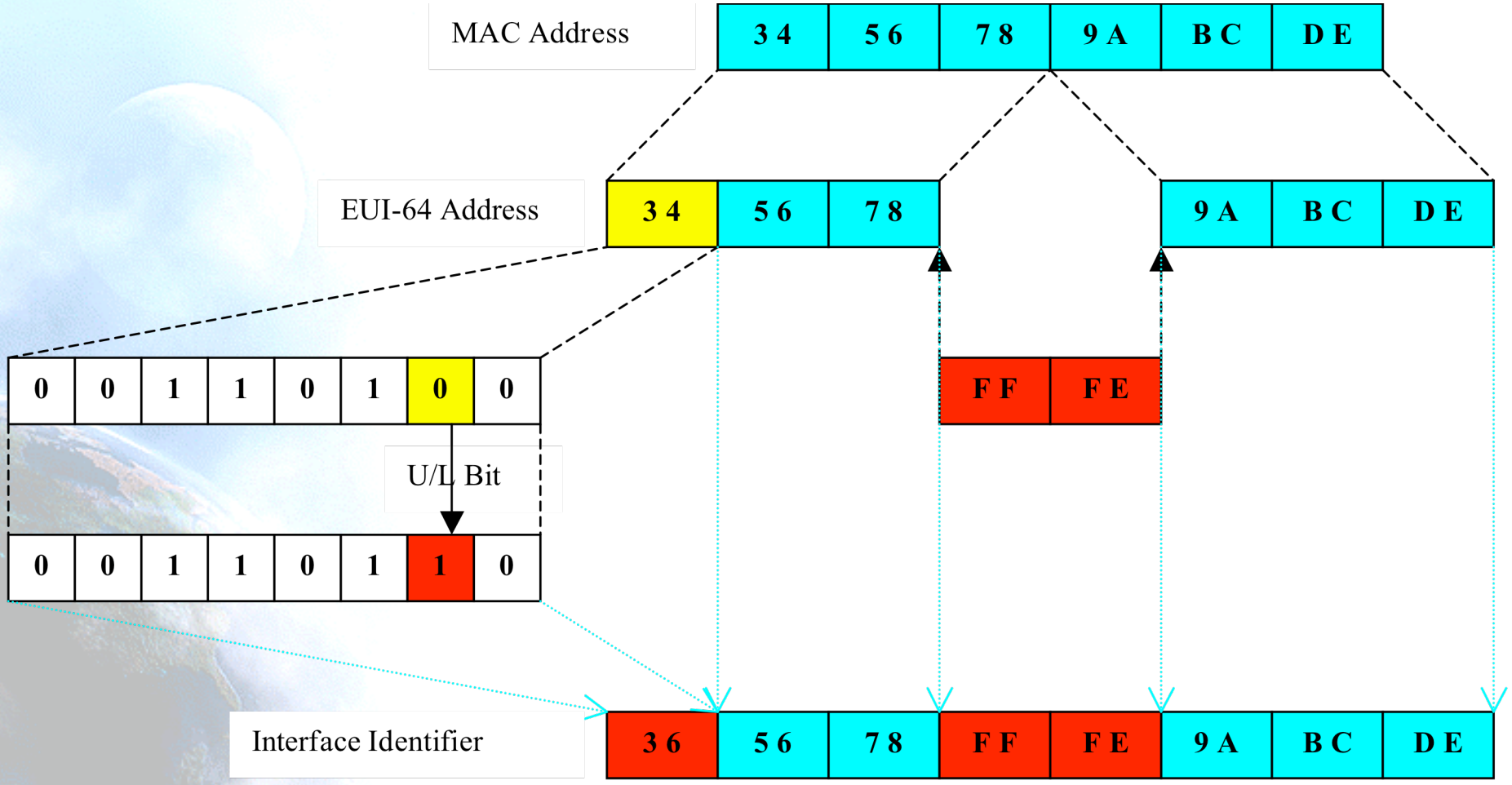
- auto-configuradas a partir de una dirección MAC de 48-bit (ejemplo, direcciones Ethernet), y expandida aun EUI-64 de 64-bits
- asignadas mediante DHCP
- configuradas manualmente
- auto-generadas pseudo-aleatoriamente (protección de la privacidad)
- posibilidad de otros métodos en el futuro



IPv6 en Ethernet

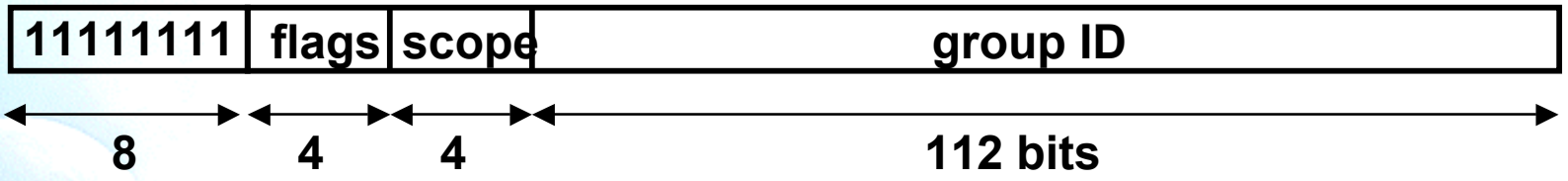
48 bits	48 bits	16 bits	
Ethernet Destination Address	Ethernet Source Address	1000011011011101 (86DD)	IPv6 Header and Data

EUI-64


MAC Address
3 4
5 6
7 8
9 A
B C
D E
EUI-64 Address
3 4
5 6
7 8
9 A
B C
D E
F F
F E
0 0 1 1 0 1 0 0
U/L Bit
0 0 1 1 0 1 1 0
Interface Identifier
3 6
5 6
7 8
F F
F E
9 A
B C
D E

1.4.5 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)

1.4.6 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.

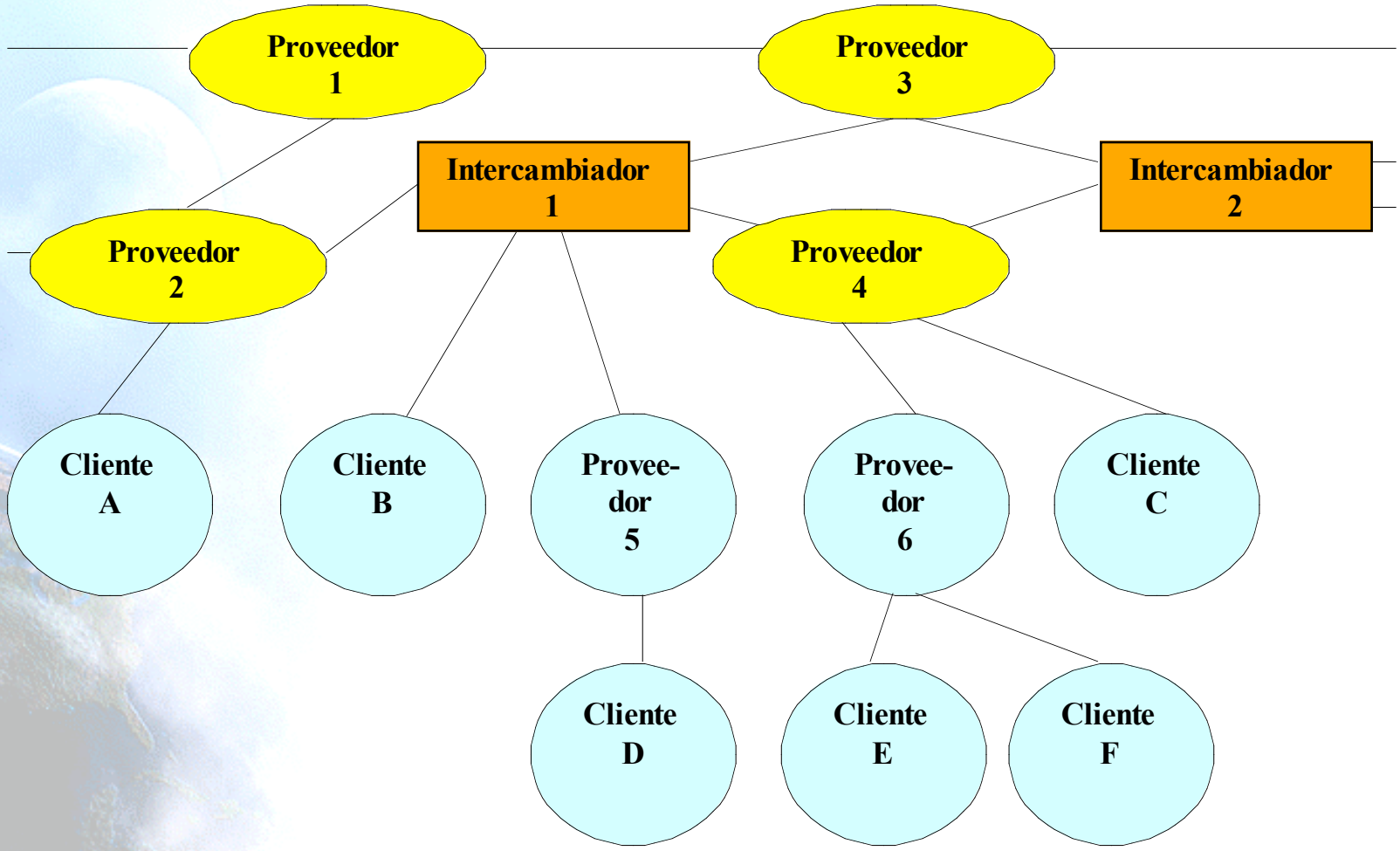
- Direcciones obligatorias en un Router IPv6: Host +:

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

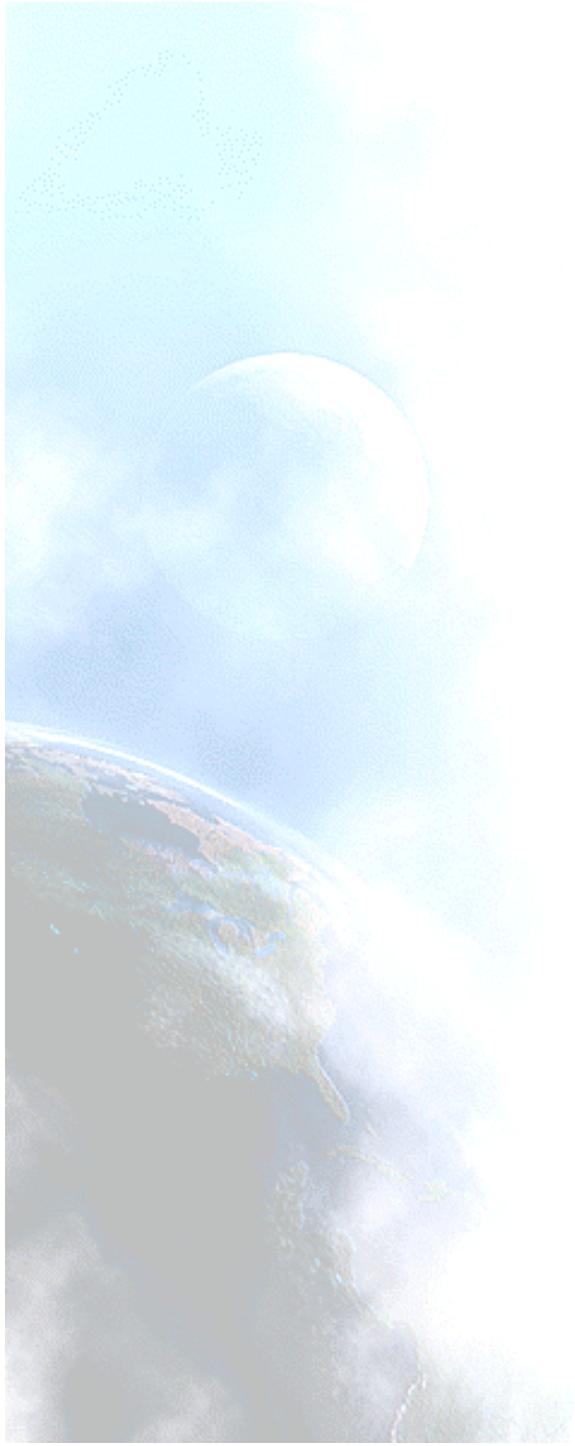
Esquema de Agregación



1.5. ICMPv6 y Neighbor Discovery

1.5.1 ICMPv6

1.5.2 Neighbor Discovery



1.5.1 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:

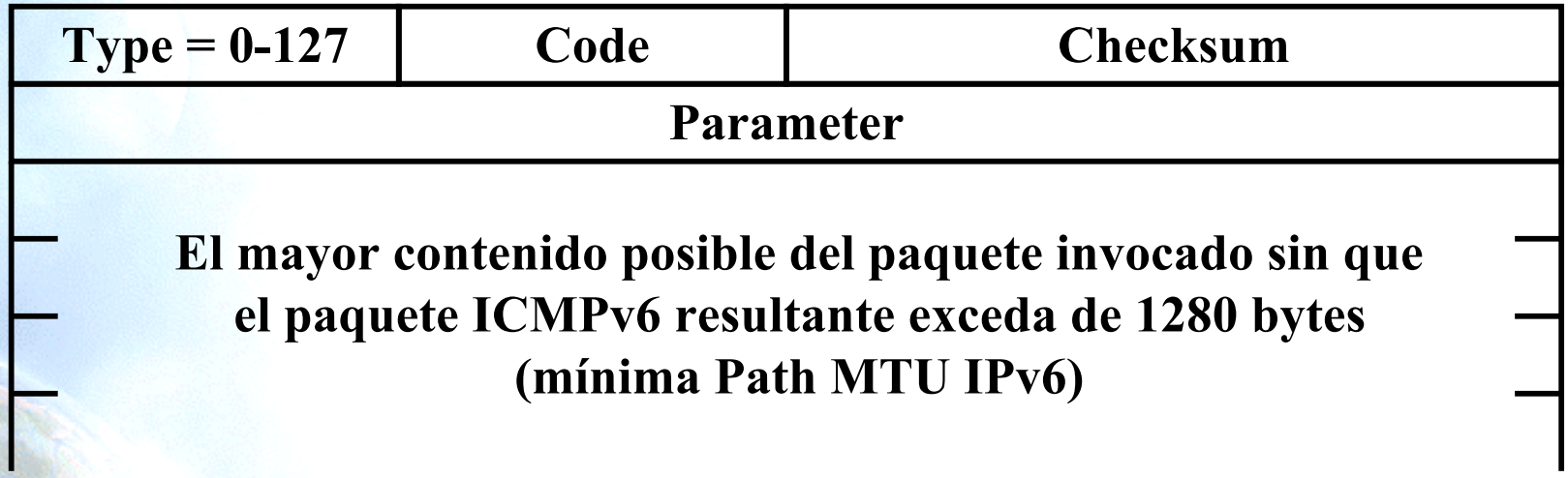
a) Si el mensaje es como respuesta a un mensaje enviado a una de las direcciones unicast del nodo, entonces Dirección Fuente Respuesta = Misma Dirección

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



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):

1.5.2 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.

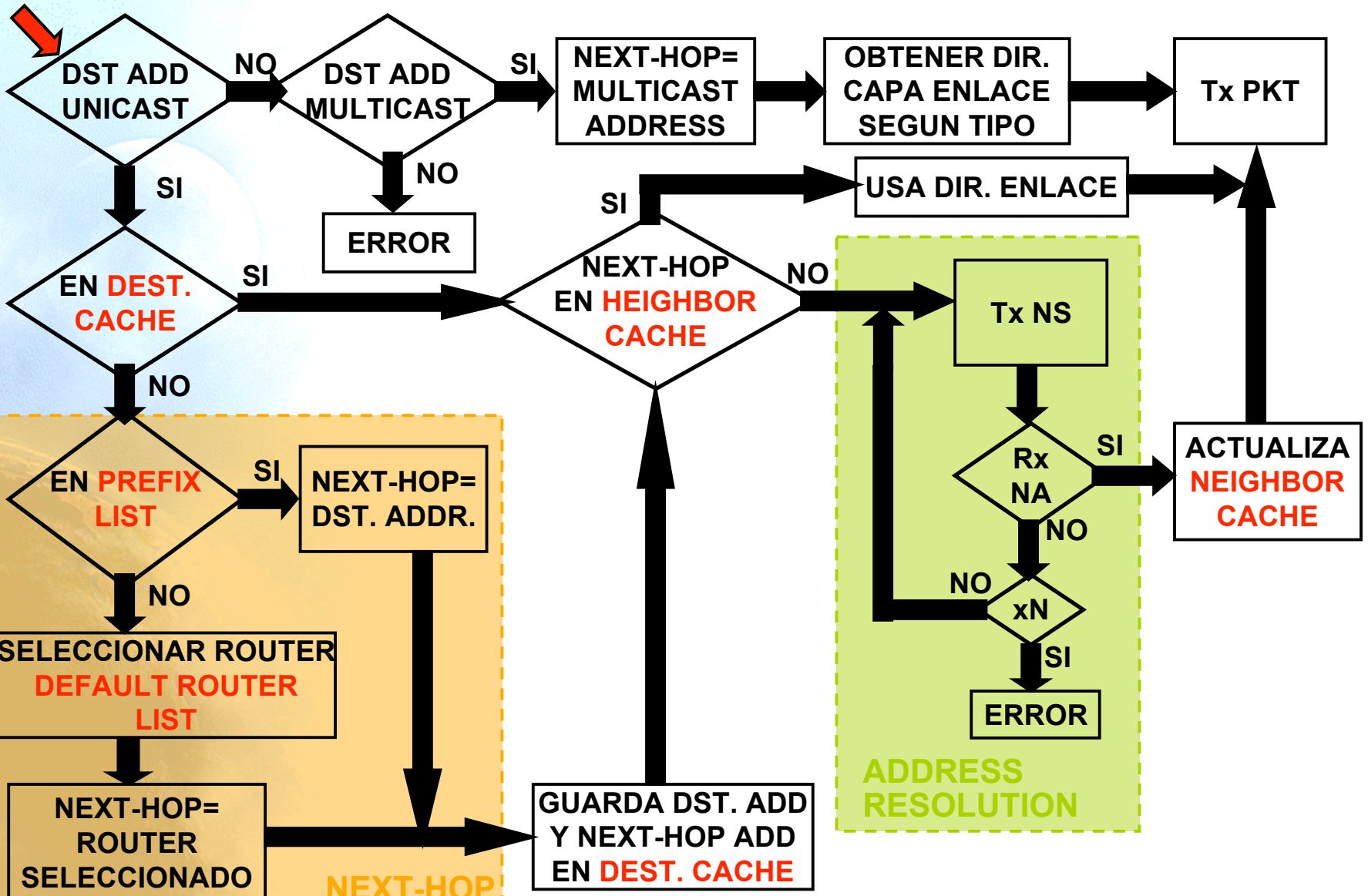
Bits 8	16	32
Type = 137	**Code = 0**	**Checksum**
Reserved = 0		
Target Address		
Destination Address		
Options …		

- 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 …				

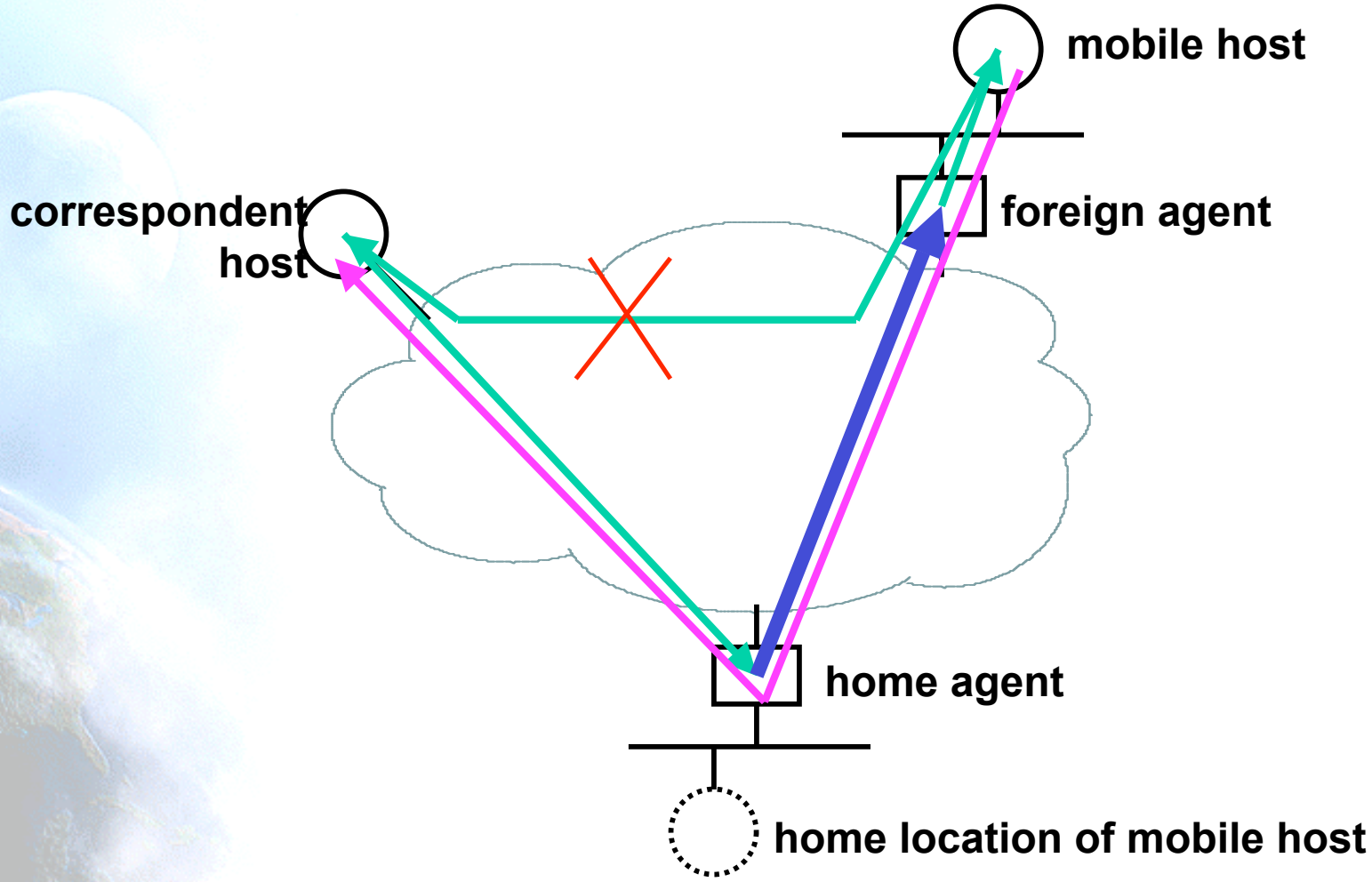
- RFC4191 describe una extensión opcional para los RAs para que los encaminadores comuniquen a los hosts preferencias para los encaminadores por defecto y rutas más específicas.
- PRF (Default Router Preference) = 01 Alta
  = 00 Meda (Por defecto)
  = 11 Baja
  = 10 Reservada (NO SE DEBE usar)
- También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

1.6 Movilidad IPv6

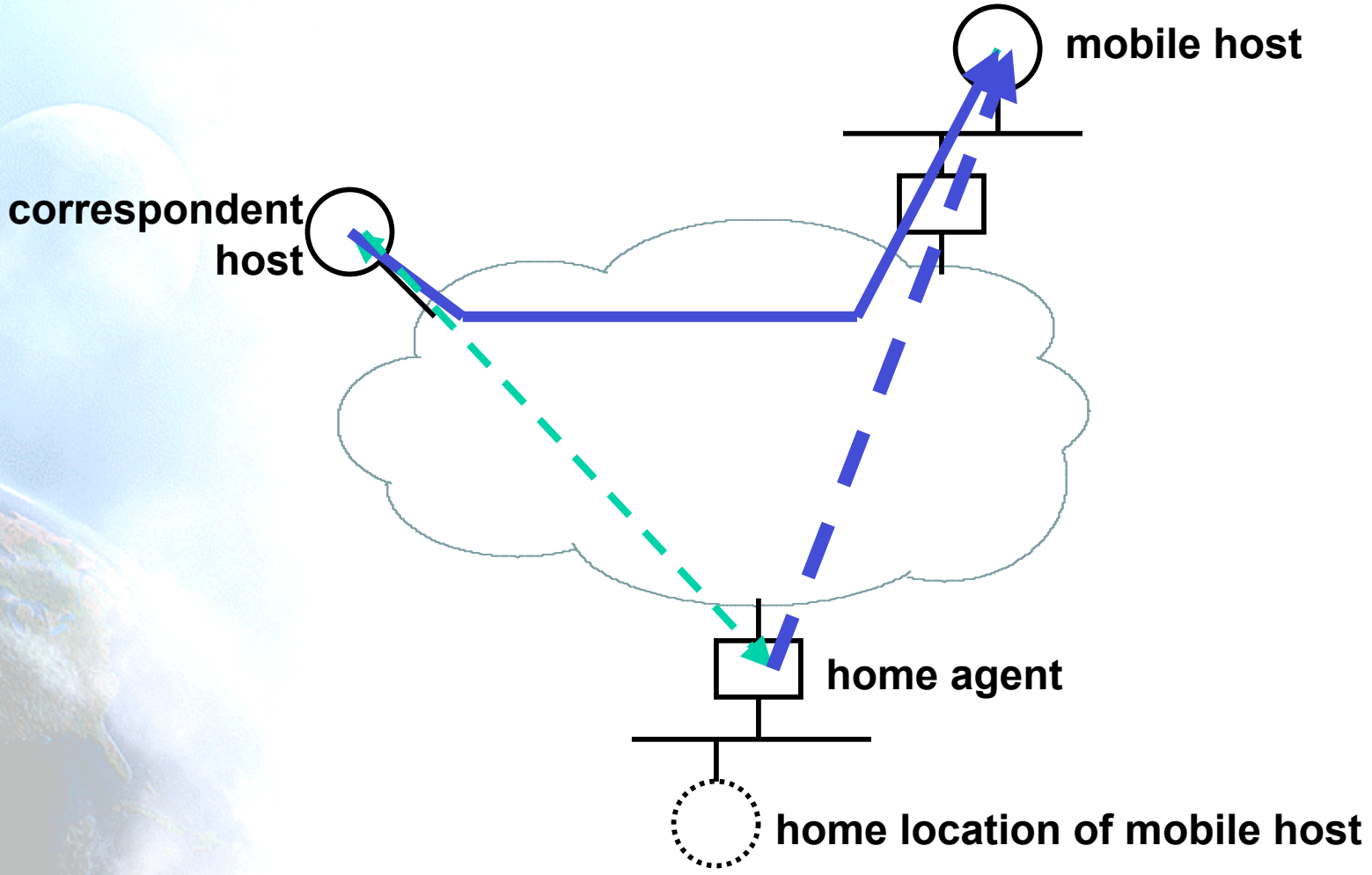
Movilidad IPv6

- Un host móvil 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 “extranjera” (foreign)
  - utiliza auto-configuración para obtener la dirección
  - registra la “foreign address” con un agente doméstico (“home agent”), por ejemplo, un router en su subred de origen
- Los paquetes enviados a la dirección de origen del host móvil, son interceptados por el home agent y reenviados a la foreign address, utilizando encapsulación

Movilidad IPv4



Movilidad IPv6



1.7 Estado actual de IPv6

Estándares (1)

- Las especificaciones del Núcleo de IPv6 son IETF Draft Standards => muy probadas y estables
  - Especificaciones base IPv6, Direccionamiento, ICMPv6, Neighbor Discovery, PMTU Discovery, IPv6-over-Ethernet, IPv6-over-PPP...
- Las especificaciones de Encaminamiento, Movilidad, Seguridad y Transición son IETF Proposed Standards => probadas y +- estables
  - BGP4+, OSPF, Movilidad IPv6, Seguridad (AH, ESP), ...
- Otras especificaciones avanzan a buen ritmo
  - Header compresion, Multihoming, QoS, etc.
- El estándar de la R5 de 3G/UMTS obliga a incorporar IPv6

Estándares (2)

- Más de 850 RFCs sobre IPv6 (de un total de 5100)
  - Core IPv6
  - Movilidad
  - Transición
  - Seguridad
  - Routing
  - Multicast

- Más detalles en

  http://www.ipv6tf.org/index.php?page=using/standardization/rfcs

Implementaciones

- La mayoría de los fabricantes y desarrolladores tienen ya implementaciones de IPv6
  - 3Com, *BSD(KAME), Cisco, Epilogue, Ericsson Telebit, IBM, Hitachi, NEC, Nortel, Sun, Trumpet, Linux, Microsoft, HP, Juniper, Apple
  - La totalidad de fabricantes importantes tienen soporte de IPv6 en sus productos
- Información del estado actual de implementaciones y productos con soporte IPv6 (mas de 1700 entradas)

  http://www.ipv6-to-standard.org

Despliegue (1)

- Infraestructura Experimental: 6bone (obsoleta desde 6/6/2006)
- Proyectos Europeos IST
  - 6NET, Euro6IX, ….
- Infraestructuras de Producción en redes de Educación e Investigación: 6ren
  - CAIRN, Canarie, CERNET, Dante, ESnet, Internet 2, IPFNET, NTT, RedIRIS, Renater, Singren, Sprint, SURFnet, vBNS, WIDE
- Infraestructura Comercial
  - La mayoría de grandes ISPs (Cable & Wireless, China Telecom, Deutsche Telekom, Global Crossing, NTT, Telefónica,…) dan servicio IPv6 comercial o algún tipo de trial
- Más detalles en
  - **http://www.ipv6-to-standard.org**

Despliegue (2)

- Obtención de direcciones IPv6 de producción
  - RIRs (Regional Internet Registries)
    - AfriNIC
    - APNIC
    - ARIN
    - LACNIC
    - RIPE-NCC
- Seguimiento del despliegue de IPv6
  - The IPv6 Portal: **http://www.ipv6tf.org**

Aún queda por hacer

Aunque IPv6 hoy en día tiene toda la capacidad funcional de IPv4,

- Las implementaciones no están tan avanzadas respecto al rendimiento, suporte multicast, compacticidad, instrumentación, etc.
- El despliegue masivo está empezando ahora
- Hay mucho trabajo por hacer para portar las aplicaciones, el middleware, el software de gestión, etc. a IPv6
- También mucho trabajo en formación (desarrolladores de aplicaciones, administradores de red, personal de venta, …)
- Muchas de las características avanzadas de IPv6 aún necesitan un especificación, implementación y despliegue.

Características Avanzadas de IPv6

- Plug-and-play
  - Ya tenemos la mayor parte de los elementos para las capas IP y para DNS. Sin embargo aún es necesario seguir trabajando en la auto-configuración de aplicaciones y servicios.
- Movilidad
  - Es necesario desplegar la infraestructura necesaria para la distribución de claves con el fin de obtener un encaminamiento eficiente en todos los casos.
- Seguridad
  - Aunque IPv6 permite le uso de IPSec en comunicaciones de extremo-a-extremo, (se elimina el uso de NATs), también depende de la infraestructura de distribución de claves
- Calidad de Servicio
  - Las características de QoS de IPv6 son las mismas que las de IPv4 pero no están tan implementadas aún

“Asuntos Calientes” IPv6 Recientes en IETF

- selección dirección/multihoming
- Espacio de direccionamiento
- Descubrimiento de DNS
- Direccionamiento anycast
- Semántica del flow-label
- API
  - (flow label, traffic class, PMTU discovery, scoping,…)
- Info. Mejorada router-to-host
- Procedimientos de renumeración
- Direcciones temp. privacidad
- Encaminamiento multicast inter-dominio
- Propagación de direcciones y AAA en diferentes escenarios de acceso
  - (always-on, dial-up, mobile,…)

Y por supuesto, transición / co-existencia / interoperabilidad con IPv4

Nota: Esto indica vitalidad, no que IPv6 este incompleto

2. Autoconfiguración, DHCPv6 y Prefix Delegation

2.1 Autoconfiguración

2.2 DHCPv6

2.3 DHCPv6 Prefix Delegation

2.1 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

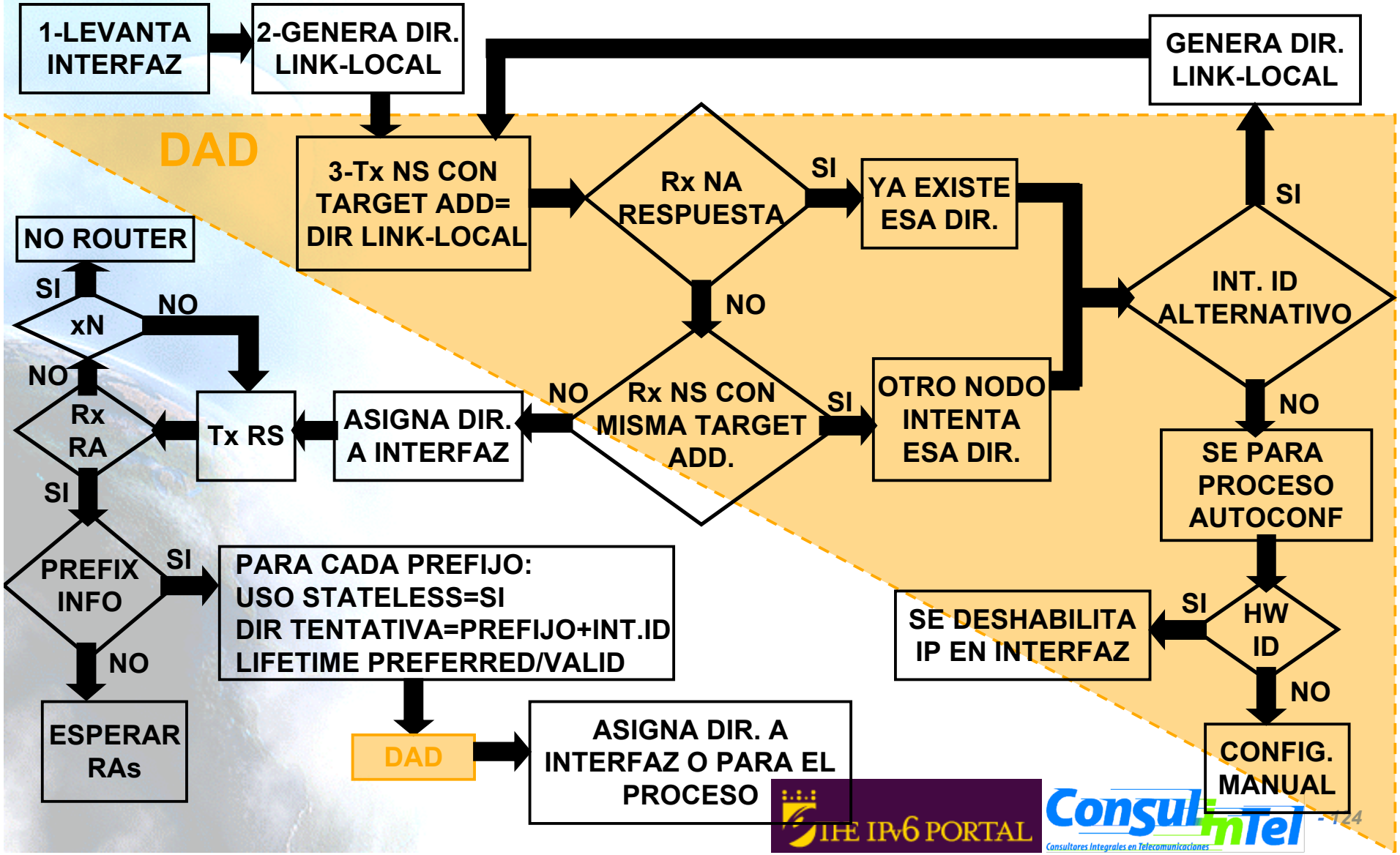
Autoconfiguración Stateless o Serverless (RFC4862)

- 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

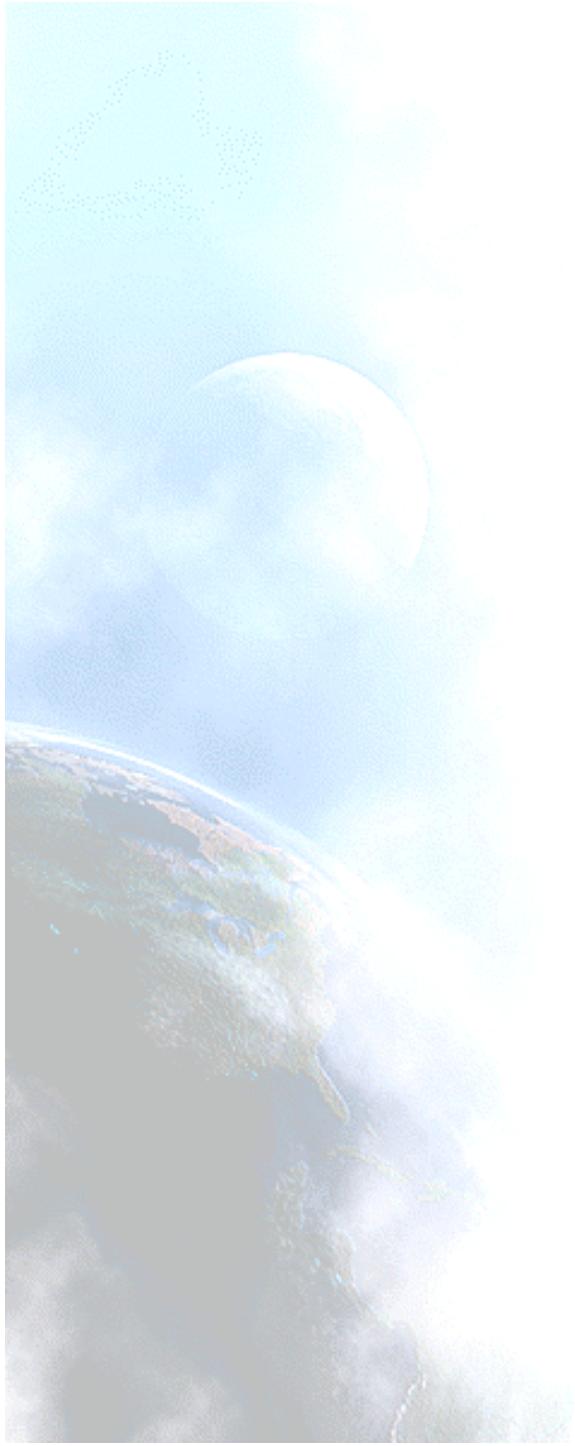
- Para asegurarse de que todas las direcciones configuradas son únicas en un determinado segmento de red los nodos ejecutan el algoritmo DAD (Duplicate Address Detection) antes de que la asignación de las direcciones a una interfaz de red sea definitiva
- El algoritmo DAD se realiza para todas las direcciones, 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)



2.2 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

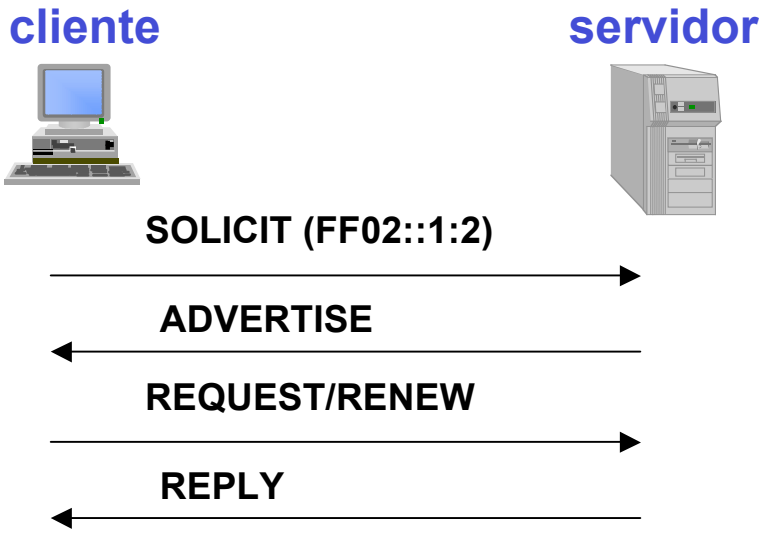
Objetivos de DHCPv6

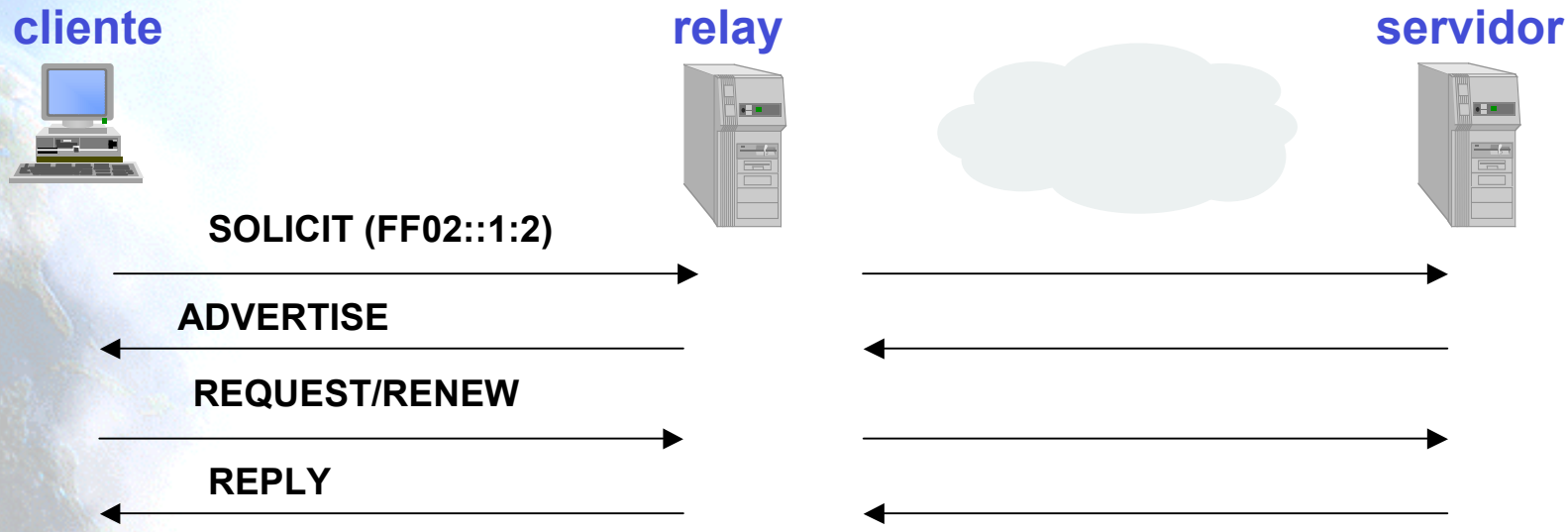
- Es un mecanismo, no una política de asignación
- Es compatible con la auto-configuración IPv6 “stateless”
- No requiere configuración manual de parámetros de red en los clientes DHCP
- No requiere un servidor en cada segmento de red
- Coexiste con nodos configurados estáticamente, nodos no participantes 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





2.3 DHCPv6 Prefix Delegation

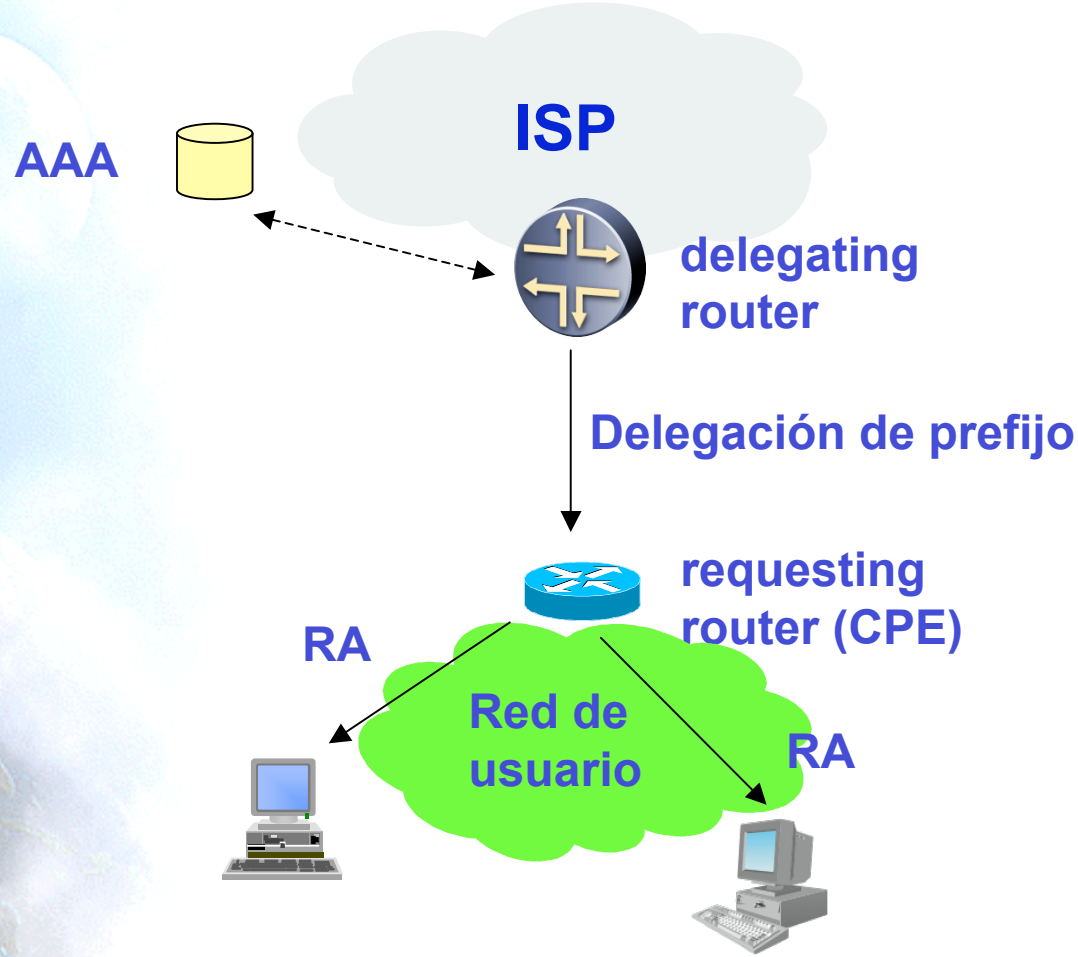
DHCPv6-PD (RFC3633)

- 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

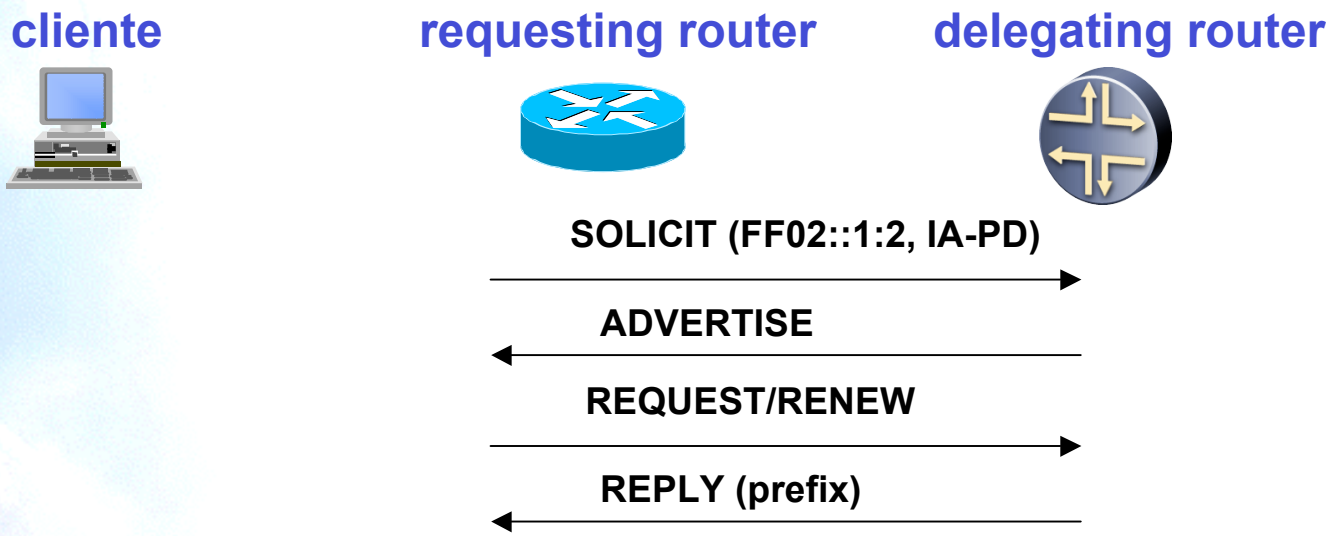
Detalles de DHCPv6-PD

- 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

3. Introducción a mecanismos de transición

- 3.1 Conceptos de Transición
- 3.2 Doble Pila
- 3.3 Túneles
- 3.4 Tunnel Broker
- 3.5 6to4
- 3.6 Teredo
- 3.7 Softwires
- 3.8 Traducción
- 3.9 Seguridad

3.1 Conceptos de Transición

Técnicas de Transición / Coexistencia

- IPv6 se ha diseñado para facilitar la transición y la coexistencia con IPv4.

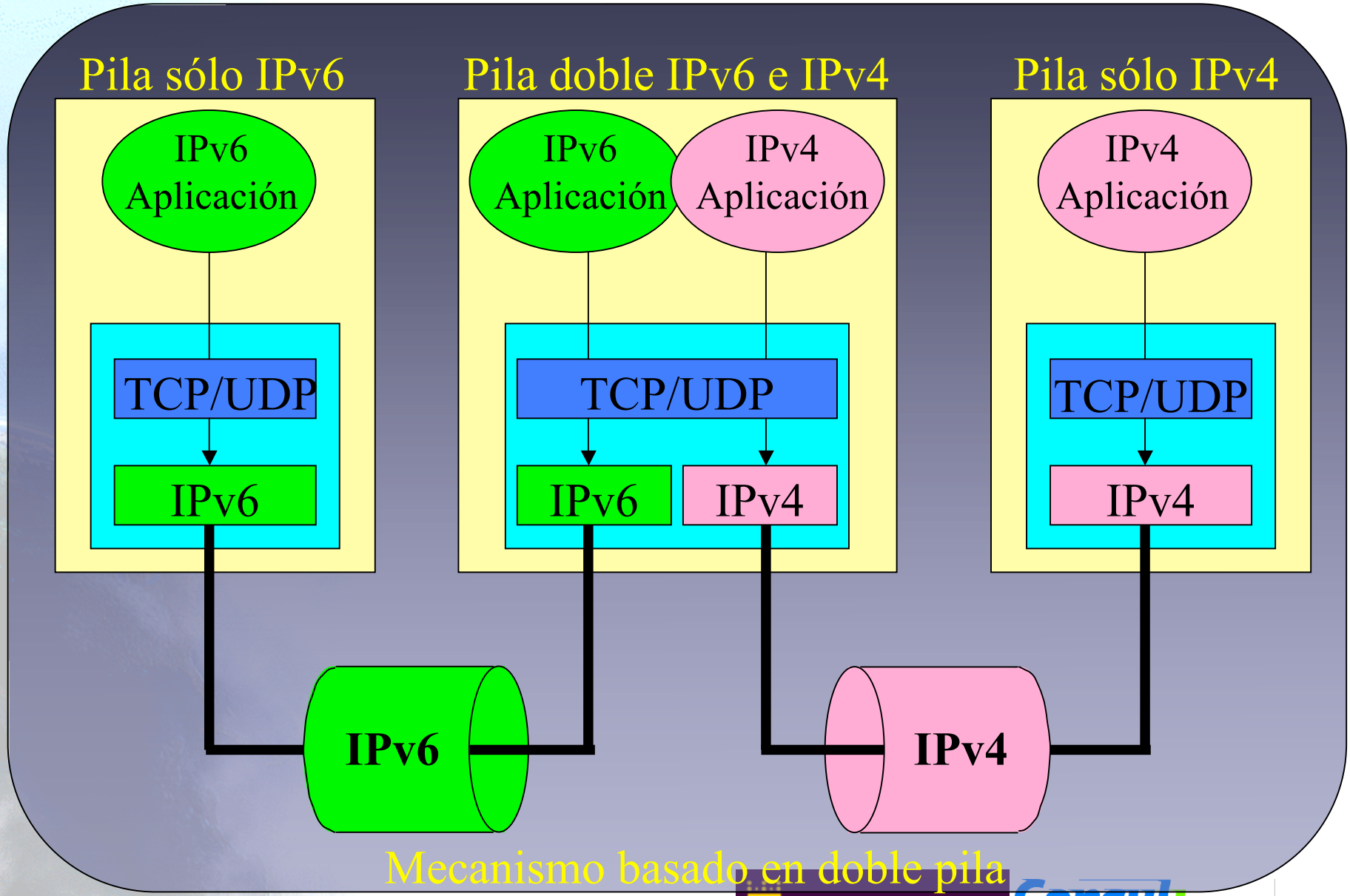
- Se han identificado e implementado un amplio abanico de técnicas, agrupadas básicamente dentro de tres categorías:
  1) Doble-pila, para permitir la coexistencia de IPv4 e IPv6 en el mismo dispositivo y redes.
  2) Técnicas de túneles, encapsulando los paquetes IPv6 dentro de paquetes IPv4. Es la más 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.

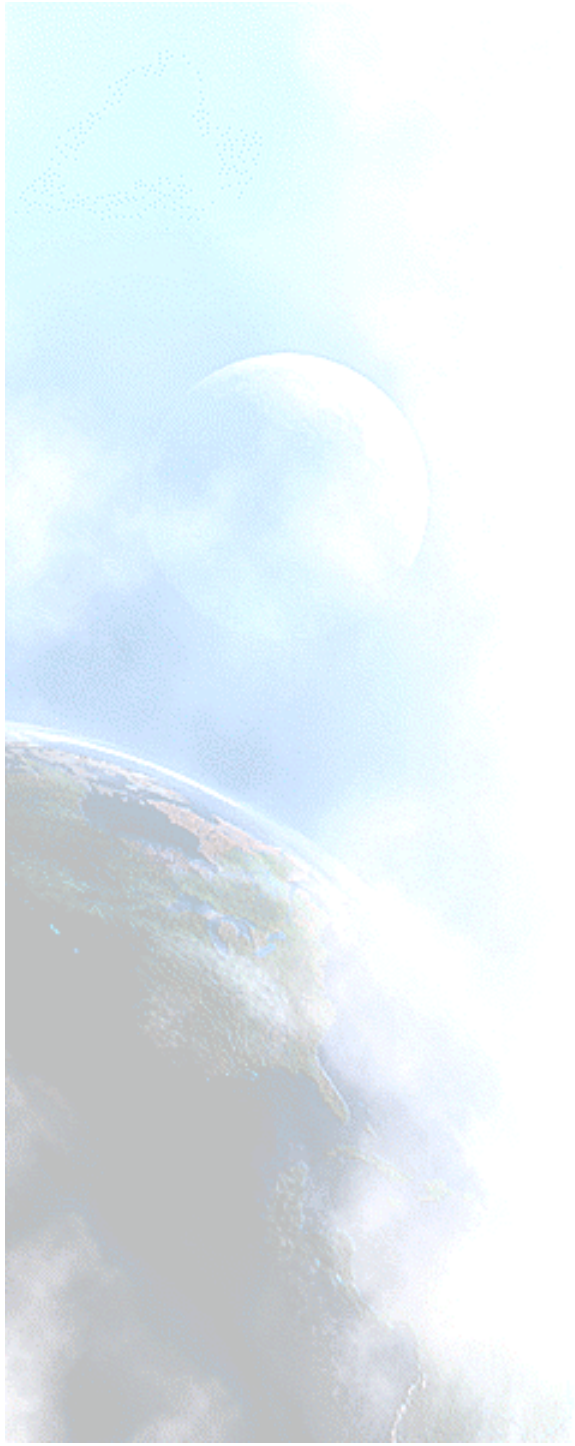
3.2 Doble Pila

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)


Pila sólo IPv6
IPv6 Aplicación
TCP/UDP
IPv6
Pila doble IPv6 e IPv4
IPv6 Aplicación
IPv4 Aplicación
TCP/UDP
IPv6
IPv4
Pila sólo IPv4
IPv4 Aplicación
TCP/UDP
IPv4
IPv6
IPv4
Mecanismo basado en doble pila

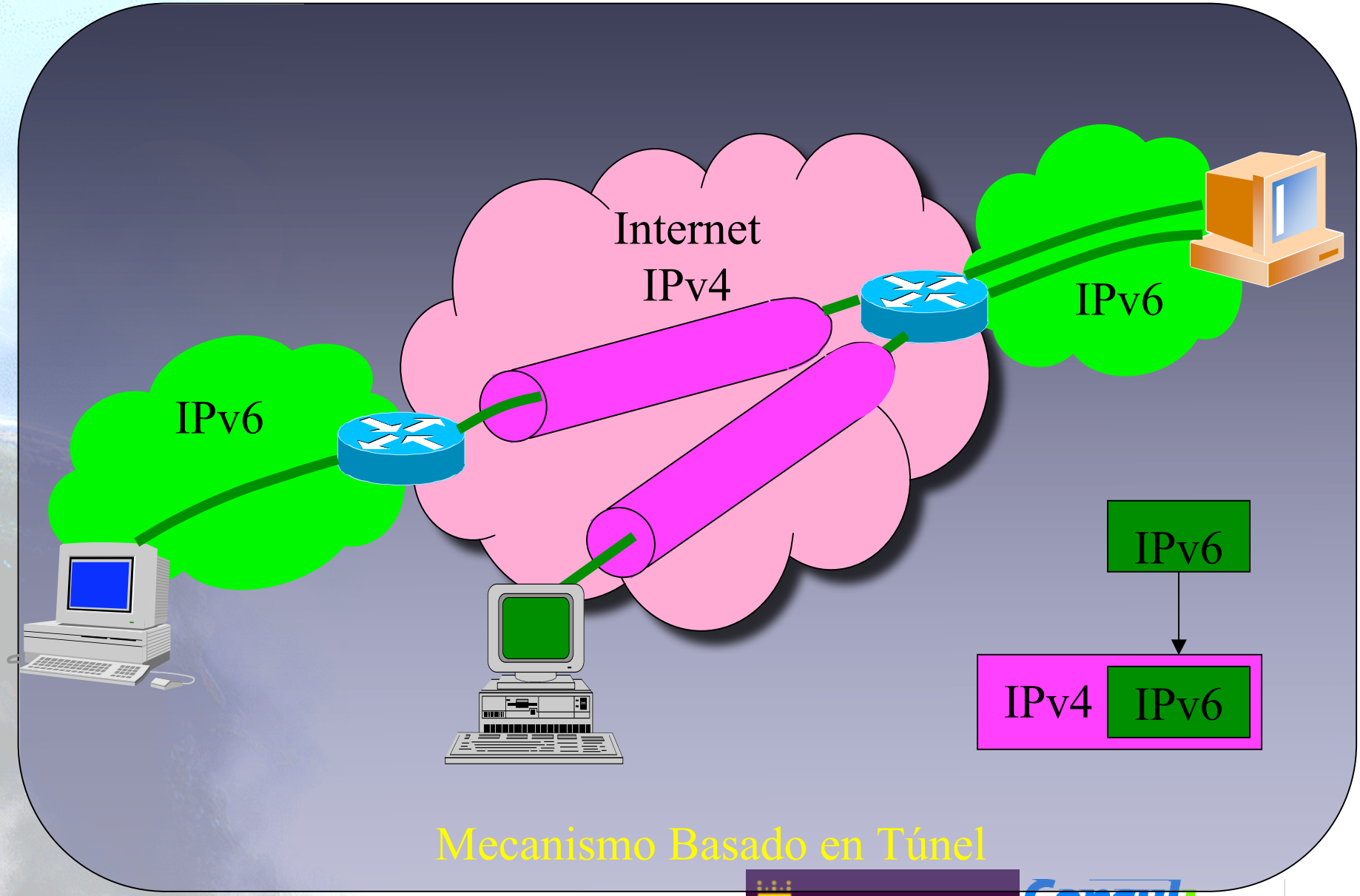


3.3 Túneles

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
  - "tunnel brokers" (tipicamente con interfaces web)
  - "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

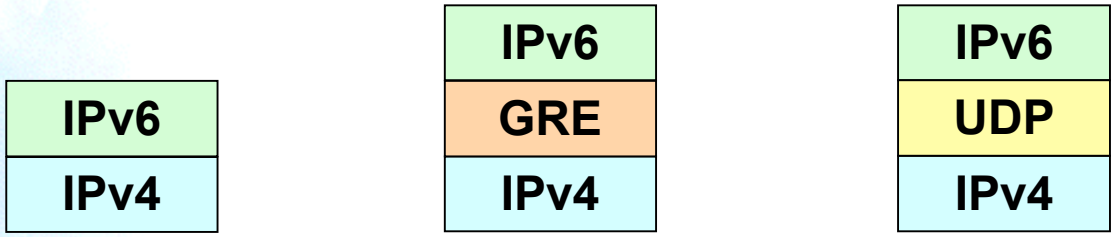
Túneles 6in4 (1)



Mecanismo Basado en Túnel

Túneles 6in4 (2)

- Existen diversas formas de encapsular los paquetes IPv6:



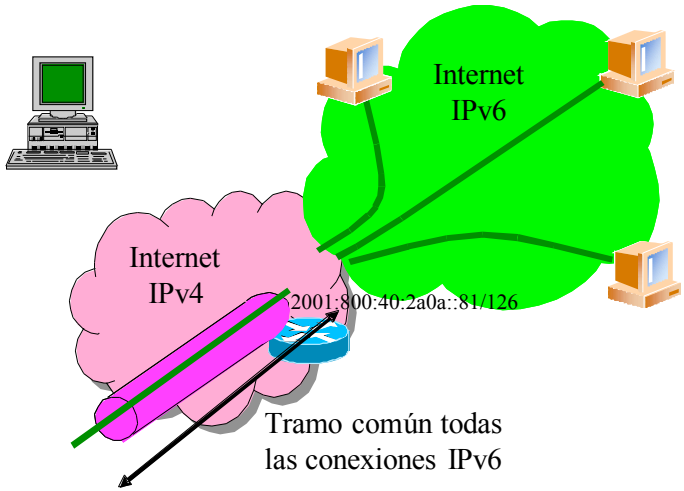
- Lo mismo se aplica para IPv4 usado en redes solo IPv6.

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

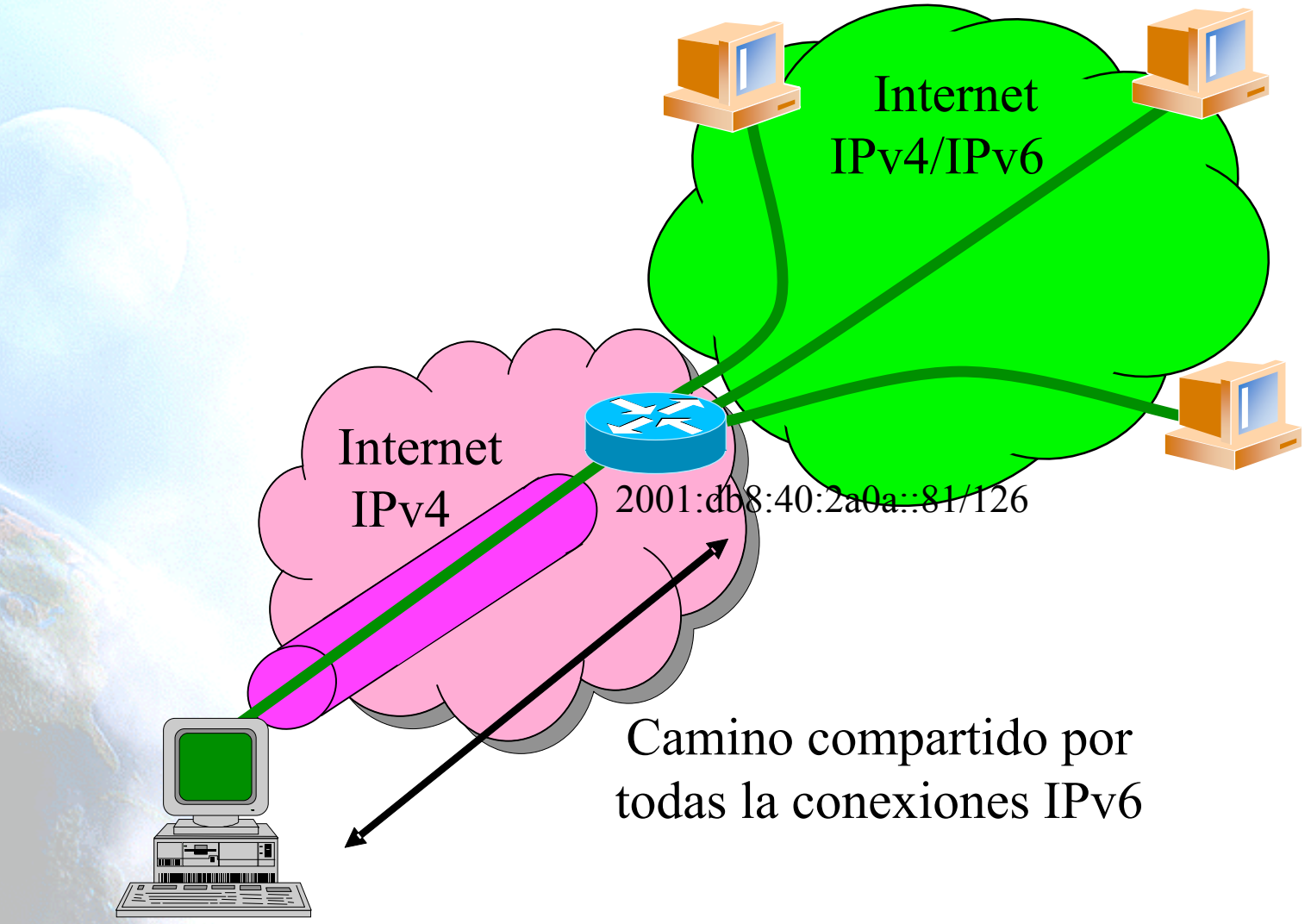
Detalles Túneles 6in4 (RFC4213)



- 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
  - Imprescindible que la implementación de NAT soporte “proto-41 forwarding” [PROTO41] para permitir que los paquetes IPv6 encapsulados atraviesen el NAT.

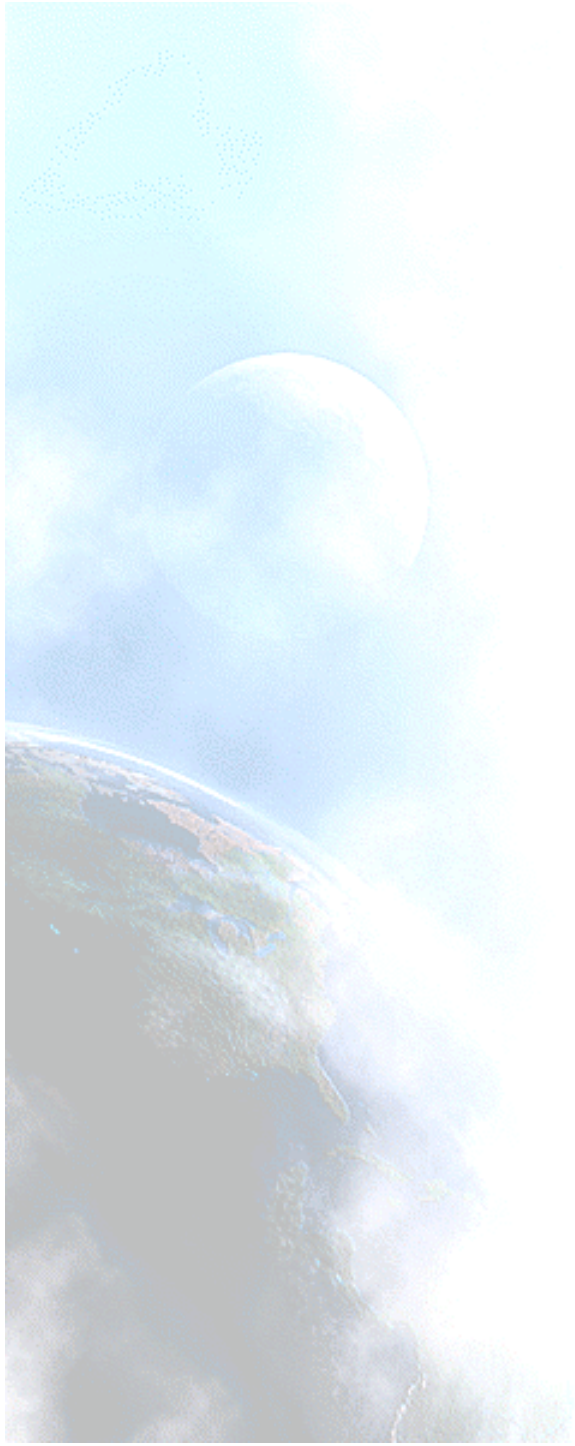
3.4 Tunnel Broker

Tunnel Broker (RFC3053)



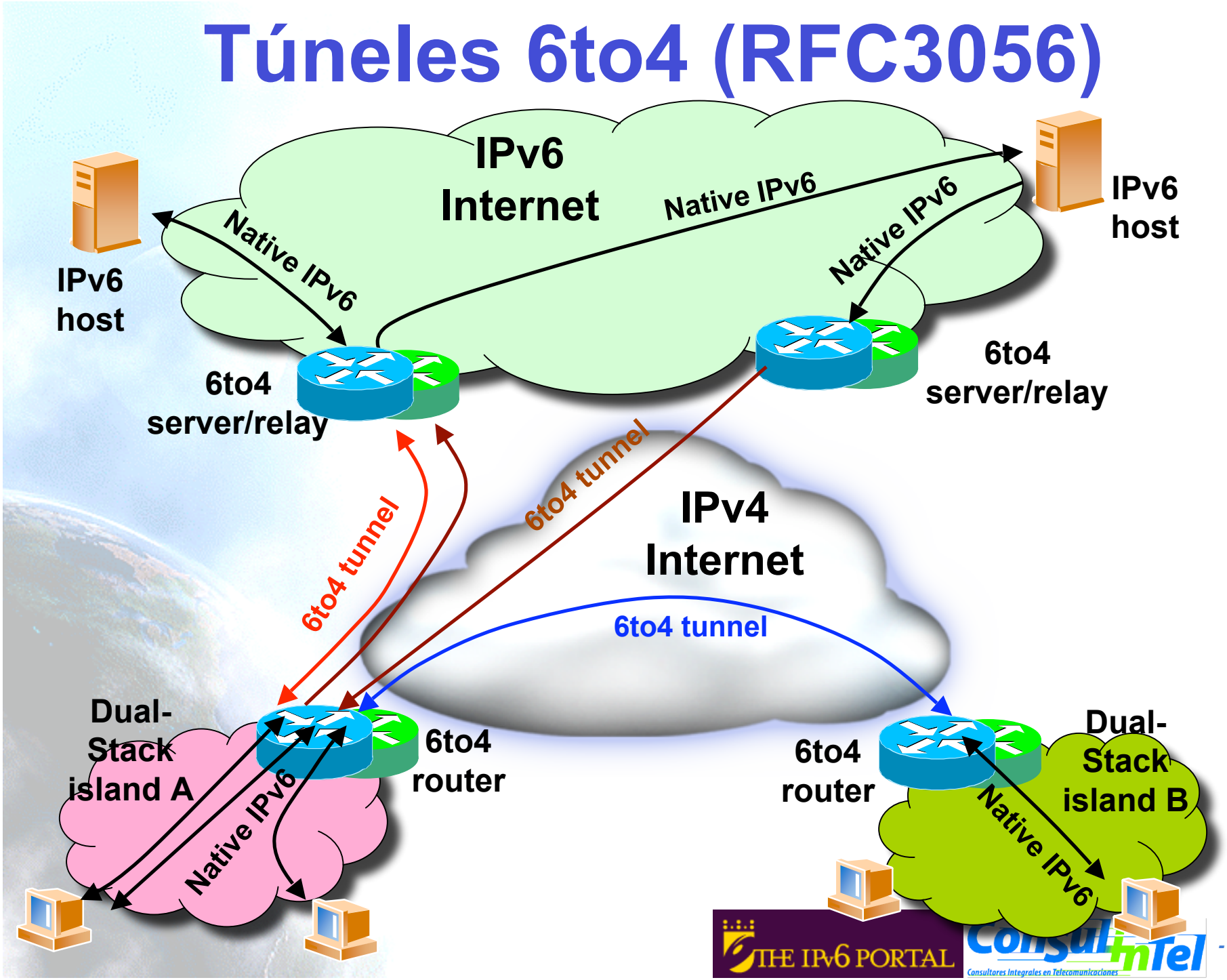
Tunnel Broker (RFC3053)

- 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.



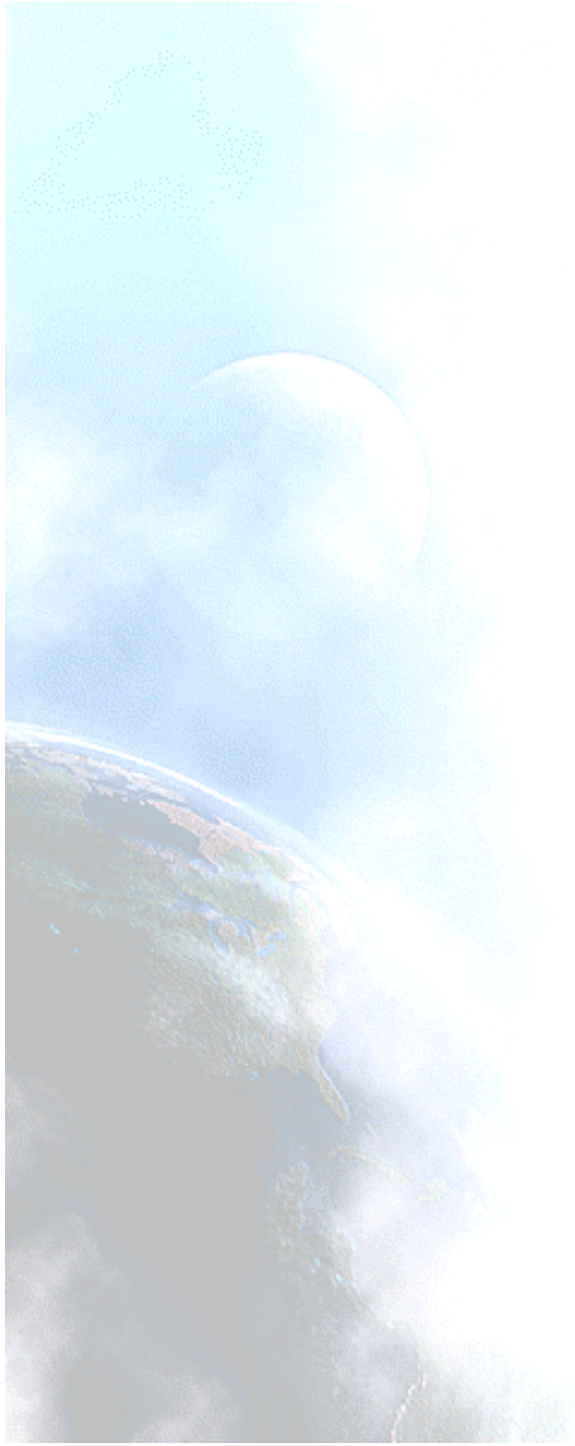
3.5 6to4

Túneles 6to4 (RFC3056)



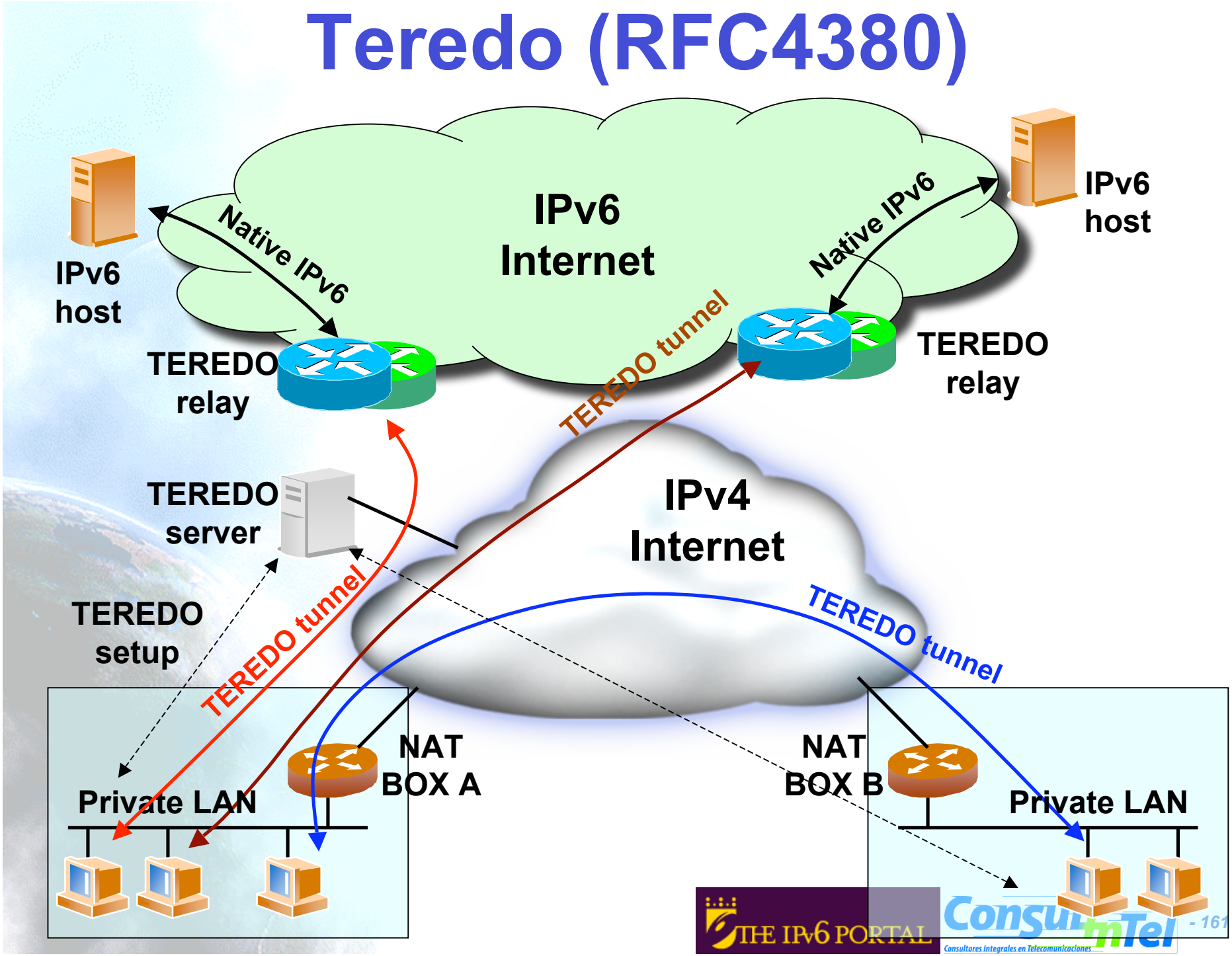
Túneles 6to4 (RFC3056)

- Definido en RFC3056.
- Se trata de un encapsulado de paquetes IPv6 en paquetes IPv4, similar a 6in4.
- Diferencias:
  - La dirección IPv6 del cliente no depende del router al que se conecta sino de la dirección IPv4 pública
    - Prefijo 2002::/16
  - Los paquetes IPv6 de salida del cliente siempre son enviados al mismo “6to4 relay”, sin embargo los paquetes IPv6 de entrada al cliente pueden provenir de otros “6to4 relay” diferentes.
- Prefijo Anycast IPv4: 192.88.99.1 (RFC3068)



3.6 Teredo

Teredo (RFC4380)



Teredo (RFC4380)

- 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

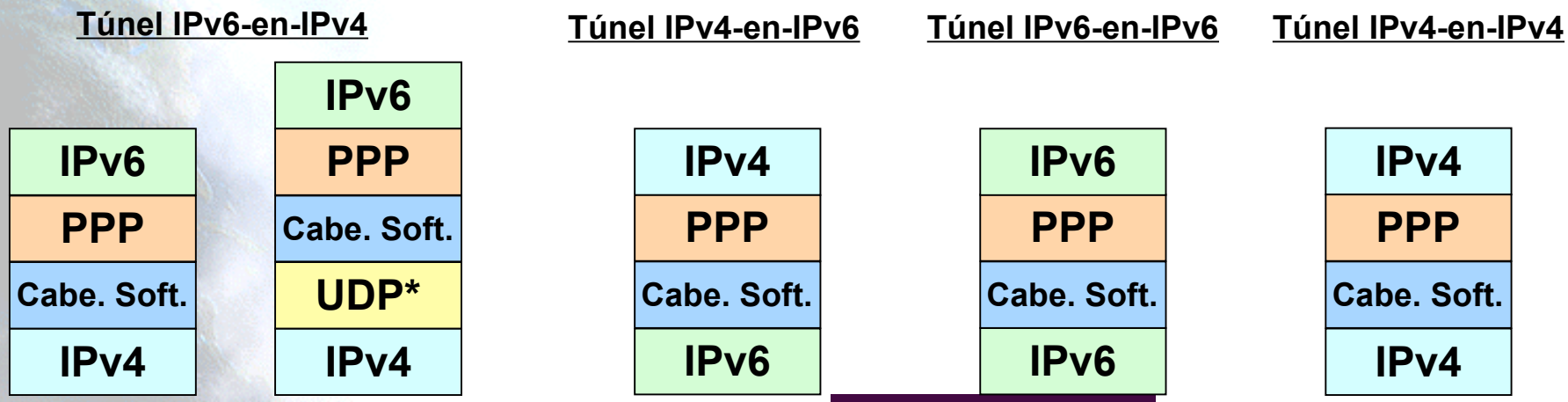
3.7 Softwires

Softwires

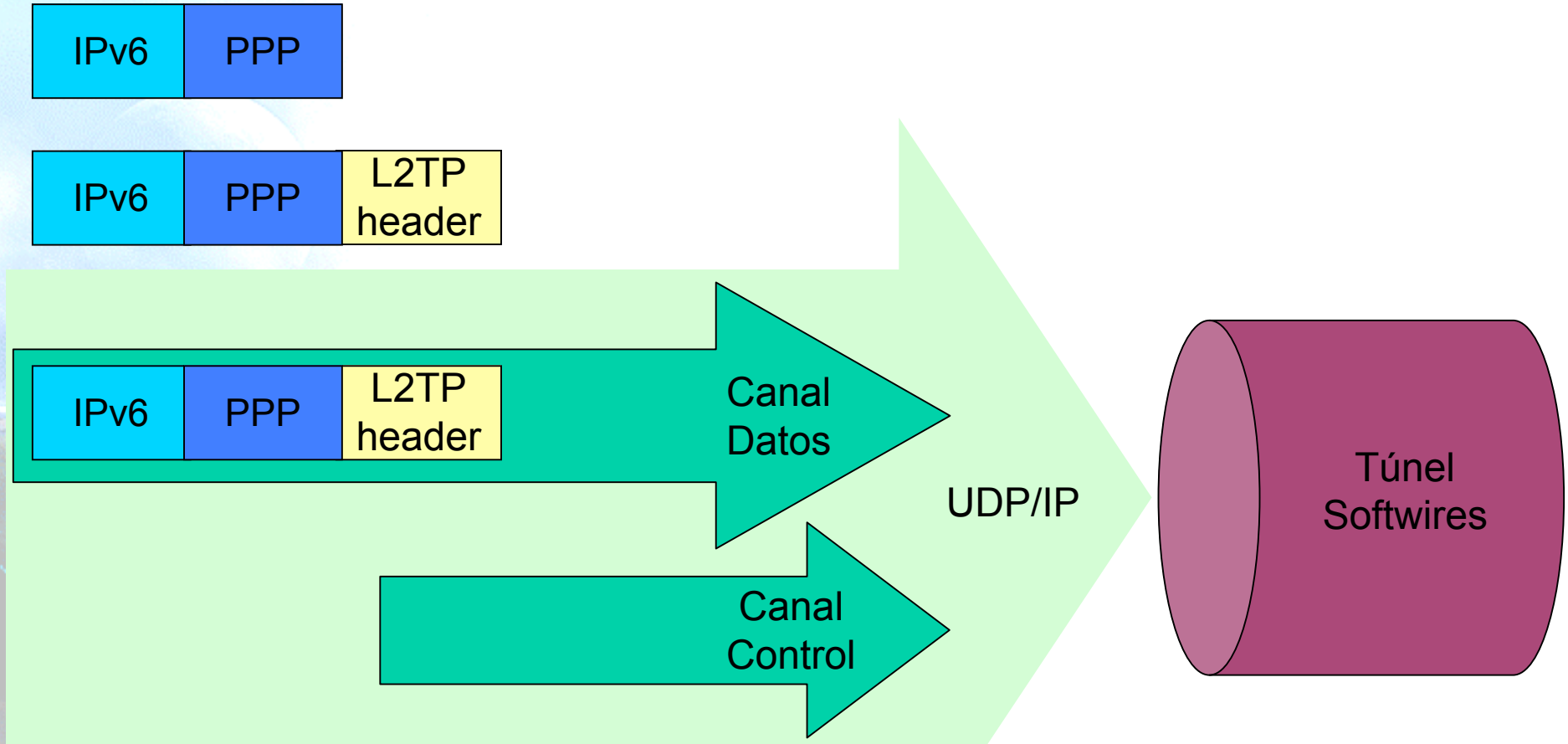
- Protocolo que esta siendo discutido en el grupo de trabajo Softwire del IETF. Presenta las siguientes características:
  - Mecanismo de transición “universal” basado en la creación de túneles
    - IPv6-en-IPv4, IPv6-en-IPv6, IPv4-en-IPv6, IPv4-en-IPv4
    - Permite atravesar NATs en las redes de acceso
    - 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)
  - 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



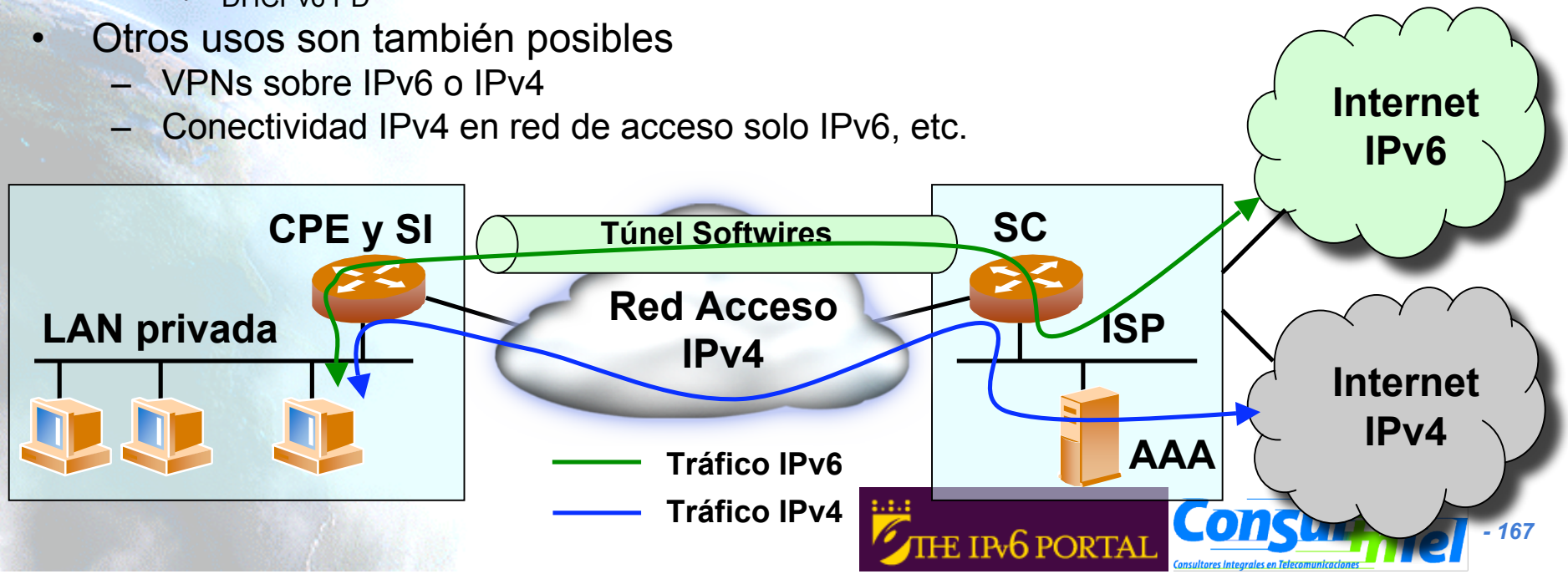
Softwires basado en L2TPv2



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

Ejemplo de uso de Softwires

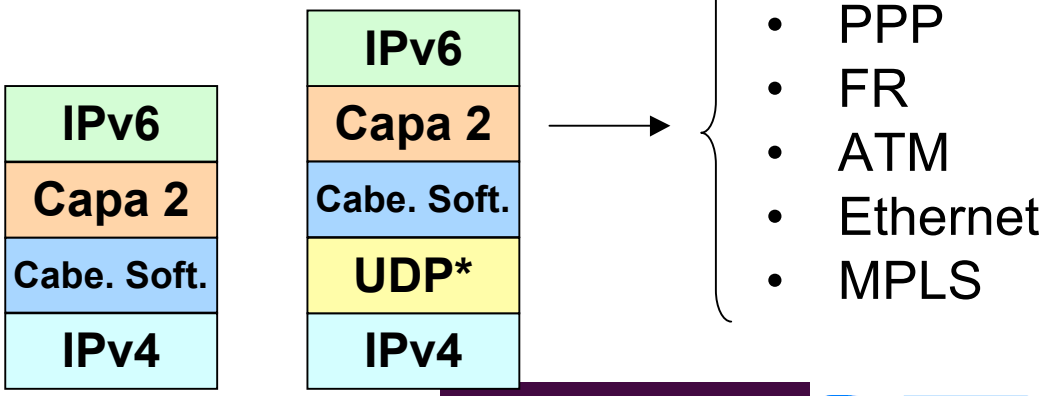
- Un uso típico previsible de Softwires es la provisión de conectividad IPv6 a usuarios domésticos a través de una red de acceso solo-IPv4
  - El SC está instalado en la red del ISP
    - DSLAM, Router de agregación u otro dispositivo
  - El SI está instalado en la red del usuario
    - CPE típicamente. 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**

3.8 Traducción

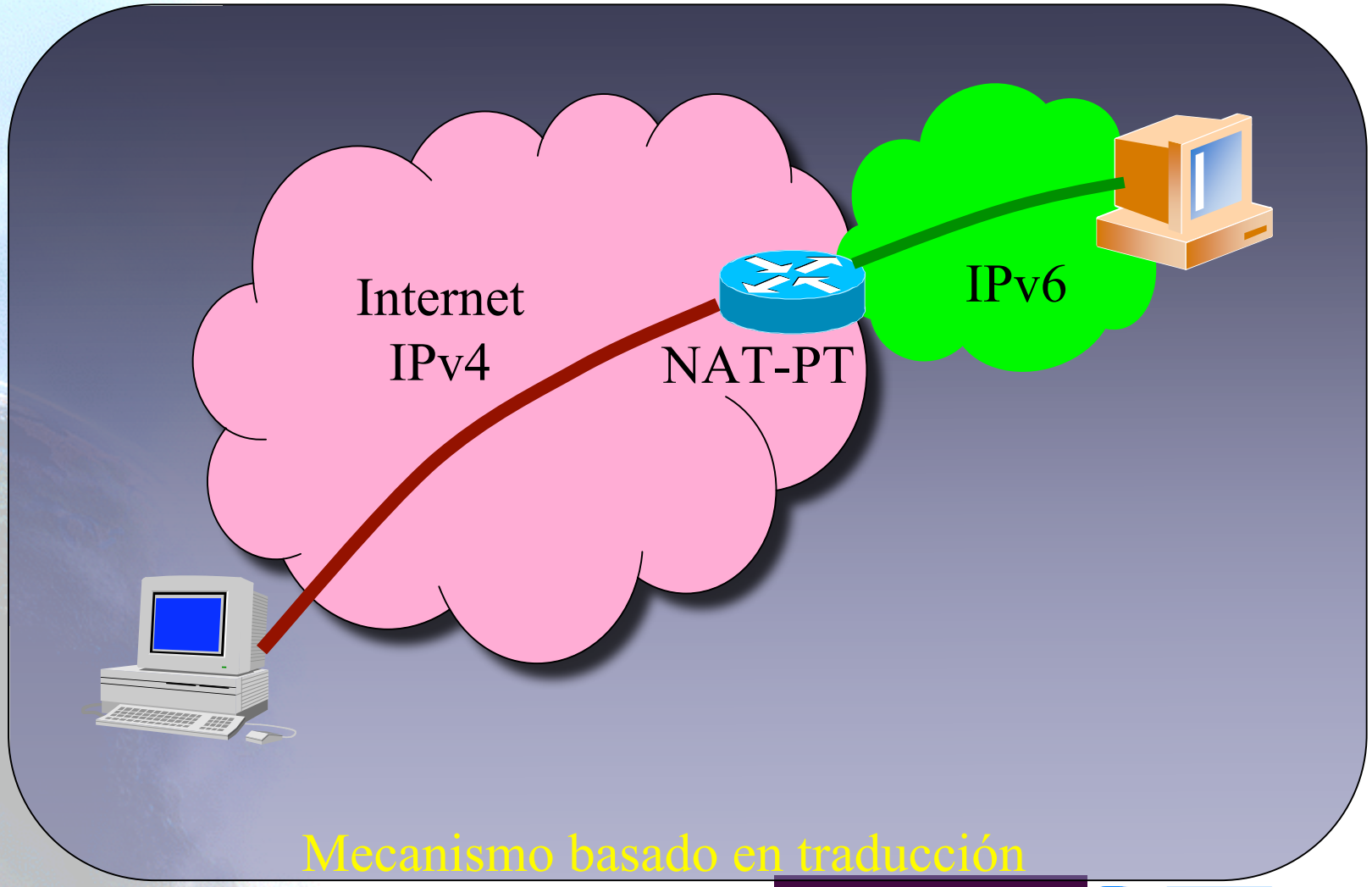
Traducción

- 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) (1)

- 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.

Traducción IPv4/IPv6 (obsoleto) (2)



Mecanismo basado en traducción

3.9 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)

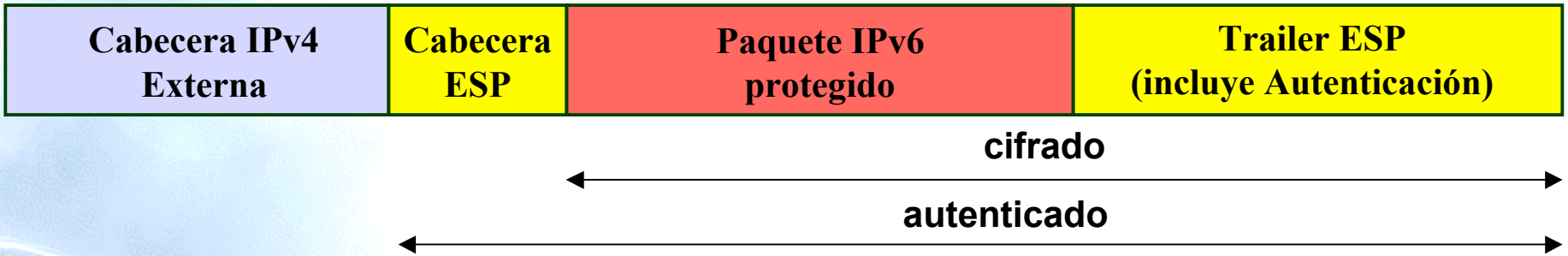
- Existen básicamente dos tipos de amenazas para los túneles de tipo 6in4
  - La dirección IPv4 del paquete (cabecera externa) se puede suplantar (“spoofing”)
    - Esta amenaza se pude minimizar mediante dos mecanismos:
      - Filtrado de ingreso en todos los ISP ➔ No se cumple en el 100% de los casos
      - 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
  - 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

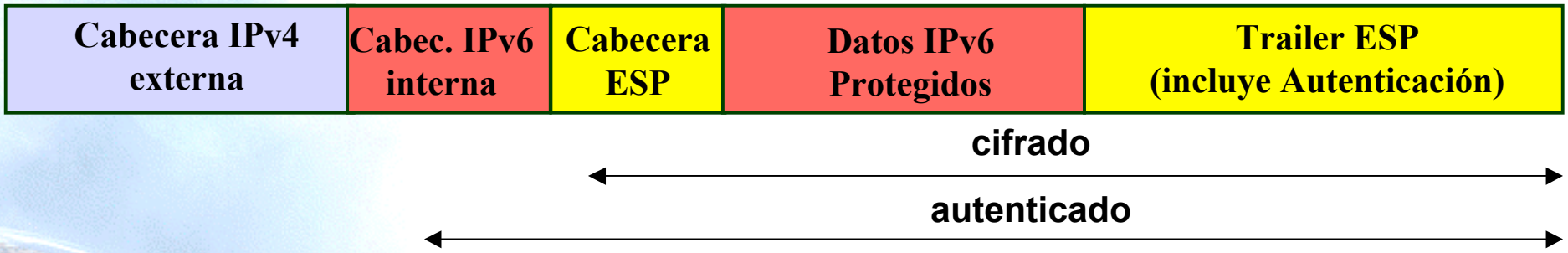
Ejemplo del Modo Transporte con ESP



- 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] draft-ietf-ngtrans-isatap-24
- [NATPT] RFC2767
- [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] draft-ietf-softwire-hs-framework-l2tpv2
- [STATELESS] RFC2462
- [STATEFUL] RFC3315
- [STUN] RFC3489
- [TB] RFC3053
- [TEREDO] RFC4380
- [TEREDOC] http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/teredo.mspx
- [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

4. IPv6 en tecnologías de banda ancha

4.1 La banda ancha

4.2 IPv6 y banda ancha

4.2.1 IPv6 en redes de cable DOCSIS

4.2.2 IPv6 en redes ADSL

4.2.3 IPv6 en redes Ethernet

4.2.4 IPv6 en redes PLC

4.2.5 IPv6 en redes Inalámbricas

4.1 La banda ancha

Beneficios de la banda ancha

- Juega un papel muy importante en la modernización de las economías
- Es un habilitador de tecnología
  - Permite el desarrollo de tecnologías de la información y de comunicación
  - Tecnologías que son un factor clave de productividad y crecimiento
- Fomenta la expansión de la sociedad de la información
- Habilita el intercambio de contenidos avanzados nuevos y mejora el de los ya existentes
- Fomenta el desarrollo de servicios nuevos
- Permite la re-estructuración del trabajo y de los procesos productivos
- En definitiva, posibilita beneficios significativos a los negocios, la administración y los consumidores

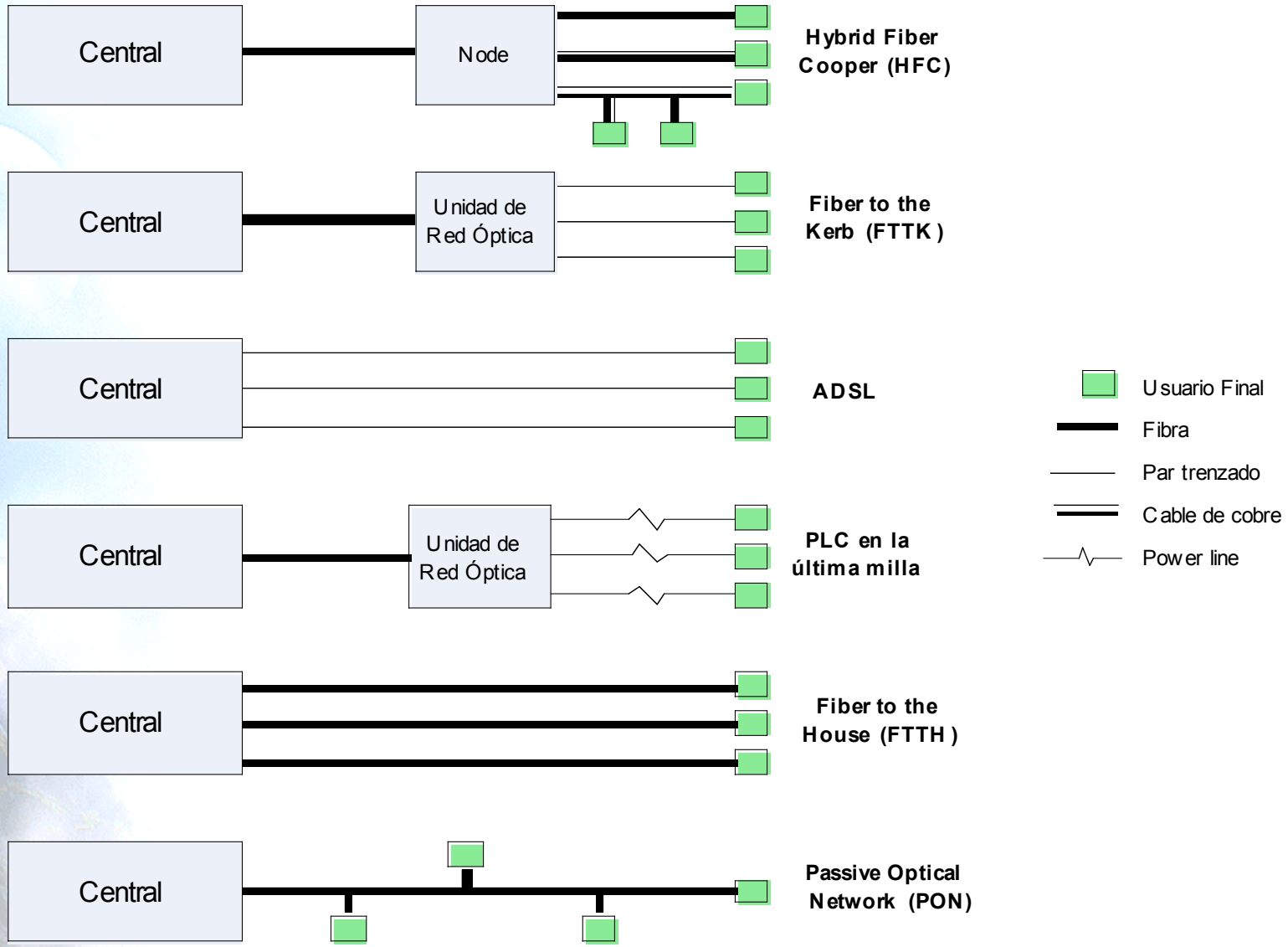
Definición de banda ancha

- Término definido en "Broadband Manifesto" de EICTA (March 2002) como:
  - Una herramienta básica que permite a las personas acceder e intercambiar contenidos multimedia de video, audio, música, servicios grupales, aplicaciones de negocio y muchas otras, a alta velocidad sobre una gran variedad de redes de acceso alámbricas e inalámbricas
- Banda ancha se refiere a conexiones digitales de alta velocidad
  - FCC de EEUU considera alta velocidad a las conexiones de 0,2 Mbps o superiores
    - 0,2 Mbps permite que una pagina Web con texto y gráficos aparezcan en pantalla con el mismo tiempo que se tarda en pasar una pagina de un libro
    - 5 Mbps permiten la transmisión en tiempo real de video con calidad de DVD
    - 10 Mbps permiten la transmisión de HDTV
    - 200 Mbps permiten la transmisión del cine digital

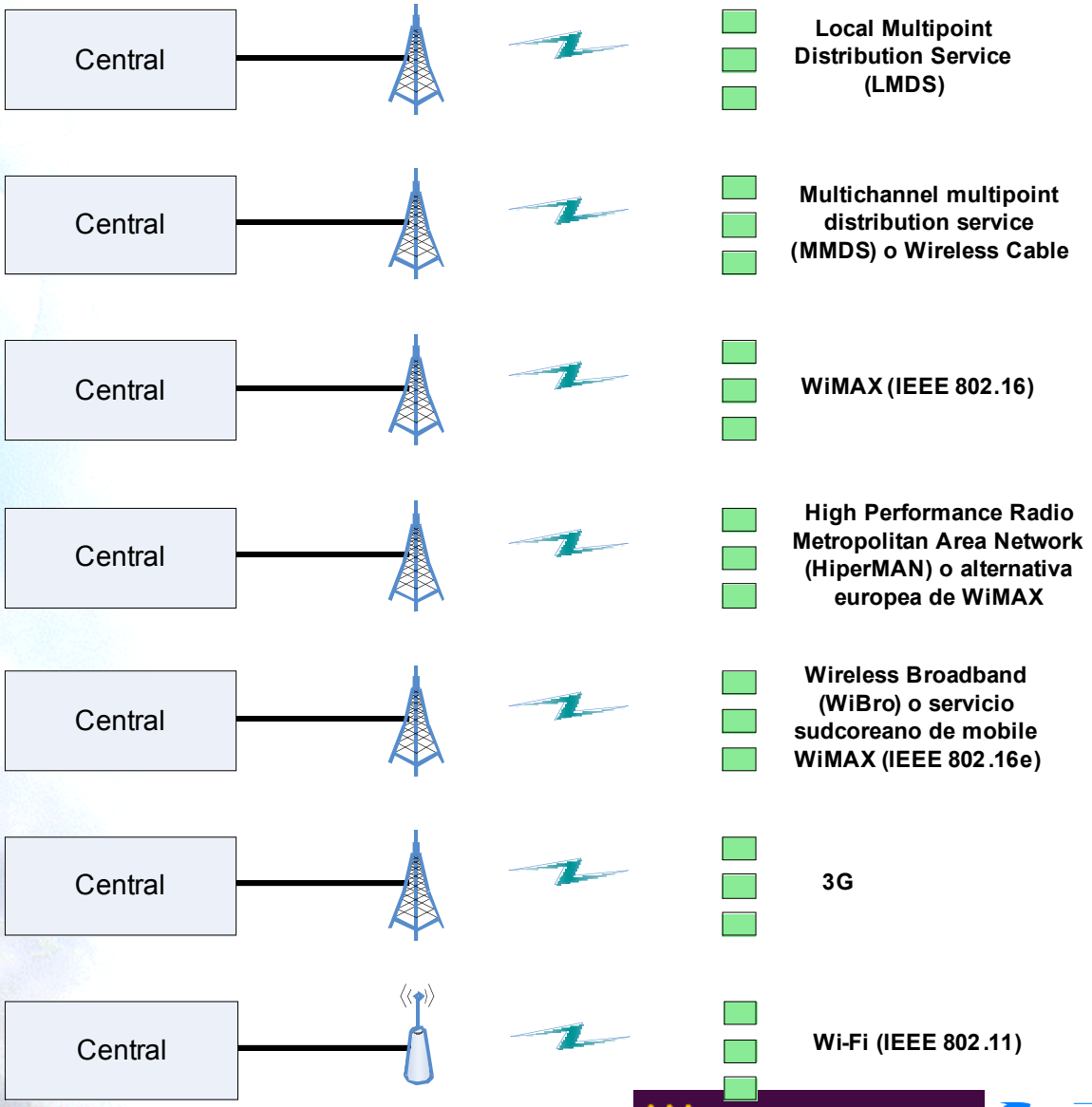
Acceso de banda ancha

- El poder brindar banda ancha depende principalmente de las infraestructuras
  - Acceso de ancho de banda (Broadband access)
- Acceso de ancho de banda (Broadband access)
  - Es la conexión física entre el equipo terminal en las instalaciones del usuario y la red de comunicaciones
- No existe una tecnología de banda ancha universal
  - Existen tecnologías apropiadas para cada entorno
  - El uso de una tecnología especifica depende de factores económicos, culturales, políticos, geográficos, entre otros
    - Puede depender de redes legadas, marcos regulatorios, soporte de instituciones, etc.
- Categorías de acceso de ancho de banda
  - **Alámbrico (líneas fijas)**
  - **Inalámbrico**

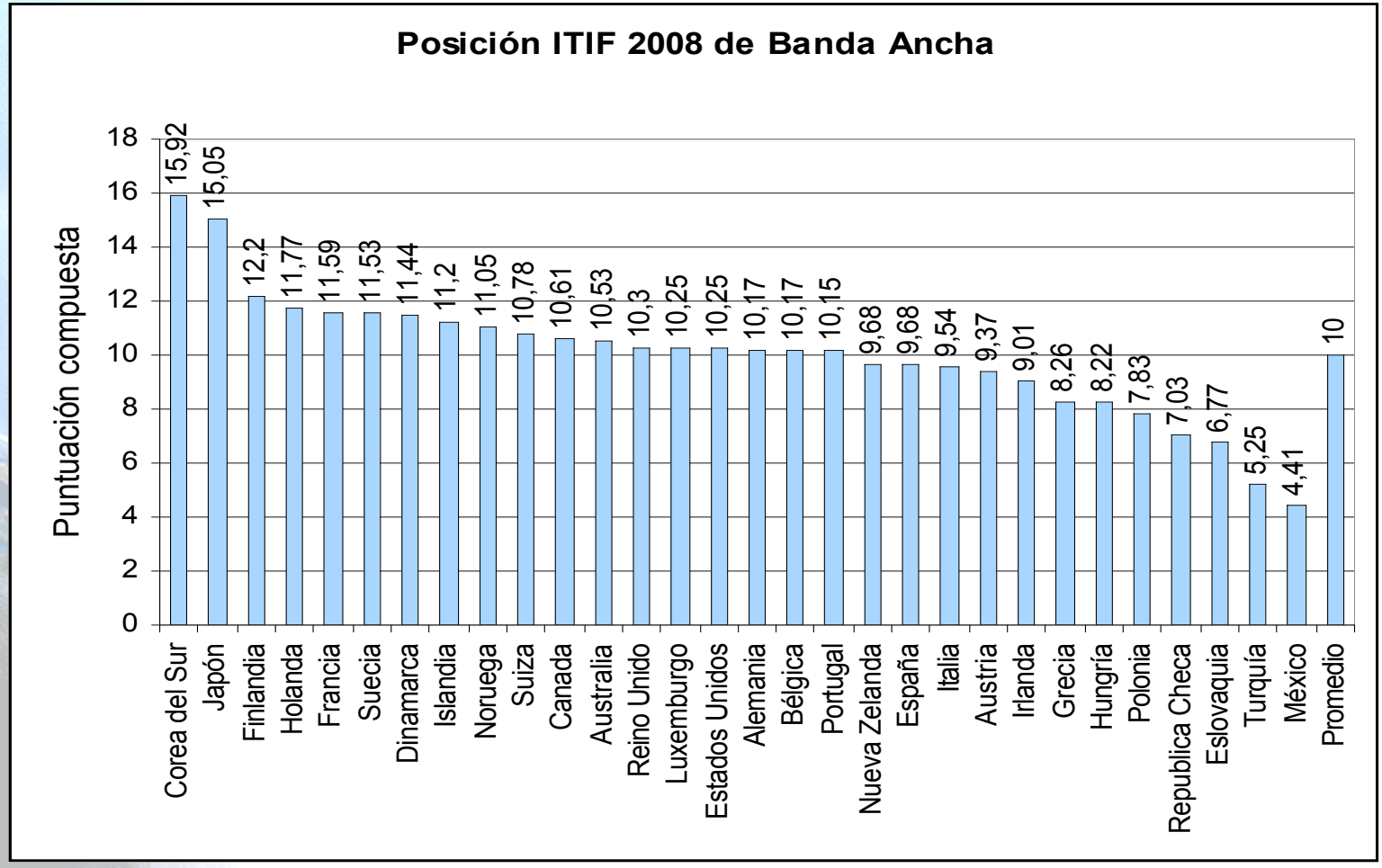
Acceso alámbrico



Acceso inalámbrico

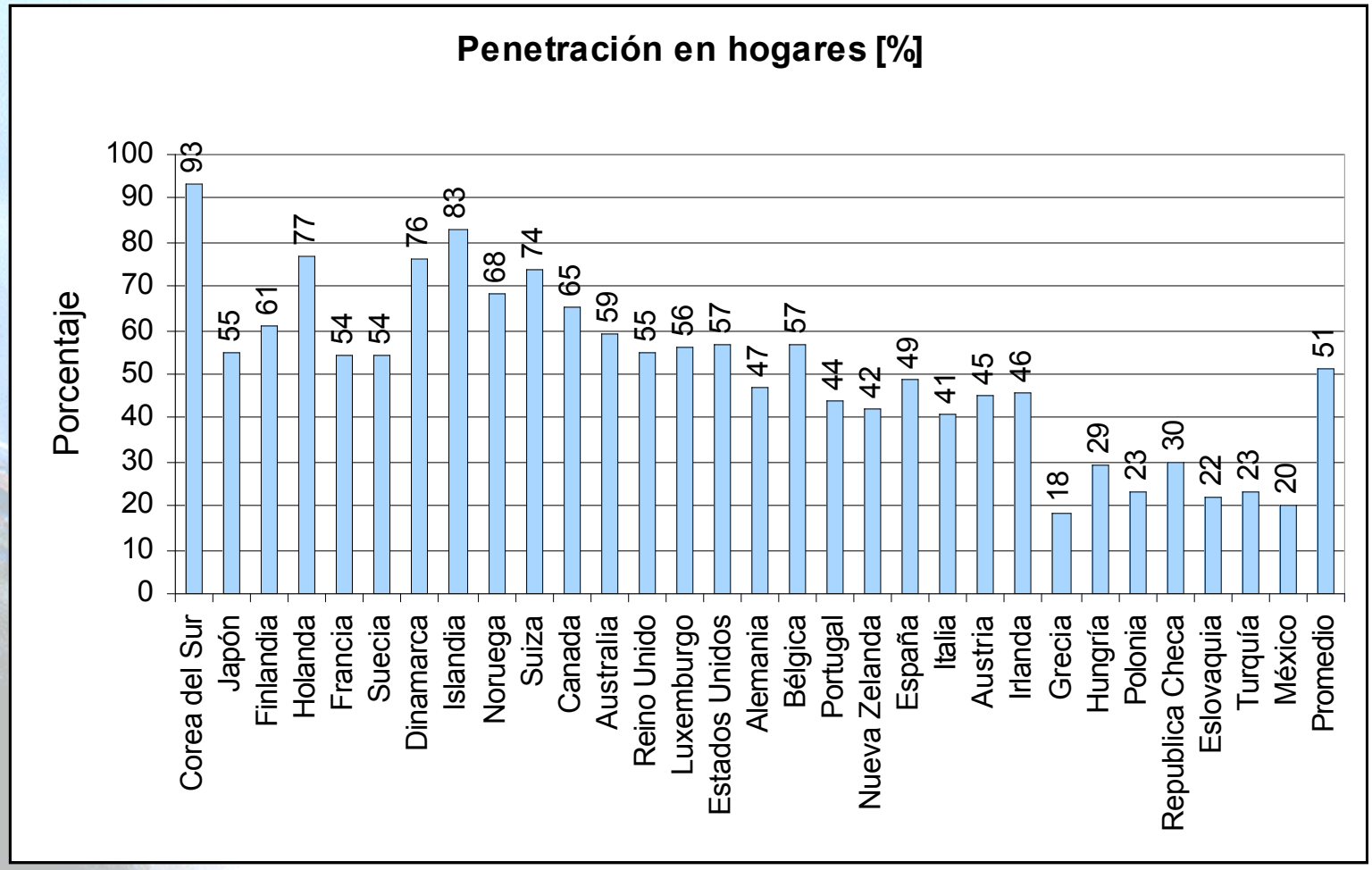


Calificación ITIF 2008 sobre Banda Ancha (1)



- Estudio del ITIF (The Information Technology & Innovation Foundation) sobre países de la OECD (Organization for Economic Cooperation and Development)
- La Puntuación compuesta incluye la suma de puntajes individuales de Penetración en hogares [%], Velocidad promedio de bajada [Mbps] y Precio (mas bajo mensual por Mbps) [US $]

Calificación ITIF 2008 sobre Banda Ancha (2)



- Estudio del ITIF (The Information Technology & Innovation Foundation) sobre países de la OECD (Organization for Economic Cooperation and Development)
- La Puntuación compuesta incluye la suma de puntajes individuales de Penetración en hogares [%], Velocidad promedio de bajada [Mbps] y Precio (mas bajo mensual por Mbps) [US $]

4.2 IPv6 y banda ancha

IPv6 y banda ancha (1)

- El despliegue de servicios de banda ancha extiende la infraestructura de red a muchos lugares
  - Conectividad xDSL “always on” en casa
    - Extiende la red hasta las residencias
    - Permite conectar equipos que podrían no estar conectados con otra tecnología (nevera, horno de microondas, etc.)
  - “Hotspots” inalámbricos
    - Extiende la red hasta lugares públicos
    - Permite conectar equipos personales para acceso a servicios
  - Teléfonos móviles 3G
    - Extiende la red hasta los usuarios de teléfonos móviles
  - Tecnología GRID y middleware
    - Permite conectar y controlar una gran cantidad de dispositivos que actualmente no están conectados
- Esto hace que los servicios de banda ancha incrementen exponencialmente la demanda de direcciones IP > IPv6

IPv6 y banda ancha (2)

- La gran cantidad de direcciones disponibles en IPv6 minimiza la necesidad de NAT
  - NAT imponen limitaciones significativas a servicios
    - p2p
    - VoIP
    - Videoconferencia
    - Ambientes colaborativos
- Cada dispositivos IPv6 conectado a la red es potencialmente un dispositivo p2p

IPv6 y la banda ancha (3)

- La banda ancha es la mejor solución a la demanda de formas eficientes de comunicación que permitan la trasferencia de mayores volúmenes de datos
- Esto permite ofrecer una serie de nuevos servicios
  - E-salud
  - E-gobierno
  - E-trabajo
  - E-educación
  - etc.
- IPv6 proporciona las herramientas adecuadas para ofrecer estos servicios
  - Autoconfiguración
  - MIPv6
  - IPsec
  - QoS
  - Multicast

Opciones de despliegue de IPv6 en banda ancha

Modo de despliegue	Pros	Contras
IPv6 nativo con infraestructura dedicada	Sin impacto en los servicios IPv4, más escalable	Si la red es grande posibles costes altos
Pila doble con transporte IPv6 nativo	Solo es necesario la actualización de una parte de la red	Mas recursos necesarios en los dispositivos de doble pila
Túneles de IPv6 sobre IPv4	Costes mínimos, solo es necesario actualizar los extremos de los túneles	No escalable, mas sobrecarga en los dispositivos extremos

¡ Seleccionar IPv6 nativo !

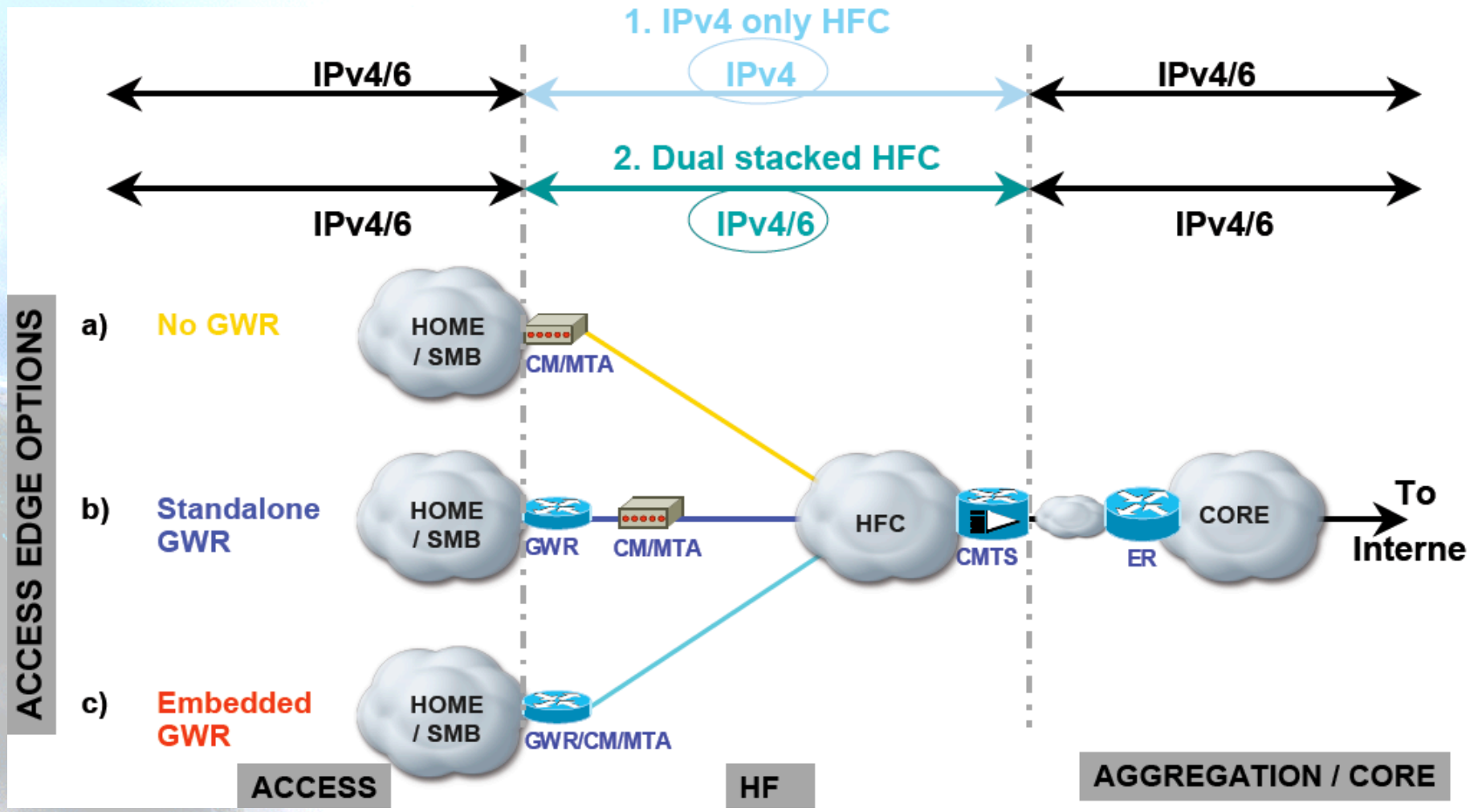
- Usar IPv6 nativo, mejores resultados a medio-largo plazo
- Doble pila es una buena forma para la transición de IPv4 a IPv6
- Los túneles solo deben de usarse cuando no sea posible el IPv6 nativo

4.2.1 IPv6 en redes de cable DOCSIS

Componentes de red de cable DOCSIS

- Cable (HFC) Plant
  - Hybrid Fiber Coaxial plant, usada como el transporte para llevar el tráfico del subscriptor
- Cable Modem Termination System (CMTS)
  - Localizado en la cabecera o el hub de distribución, provee la conectividad de datos entre el Host/Cable Modem y otros dispositivos de la red IP
- Cable Modem (CM)
  - Modulador/Demodulador en el emplazamiento del subscriptor para transportar los datos de trafico hacia/desde el cable plant
- Multimedia Terminal Adapter (MTA)
  - Trasporta el tráfico VoIP hacia/desde los subscriptores
- Residential Gateway Router (GWR)
  - Provee servicios de nivel 3 a los hosts
- Host
  - PC, notebook, dispositivo, etc. conectado al CM o al GWR
- Edge router (ER)
  - Router de frontera que conecta el CMTS a la red troncal. Un ER puede agregar varios CMTSs

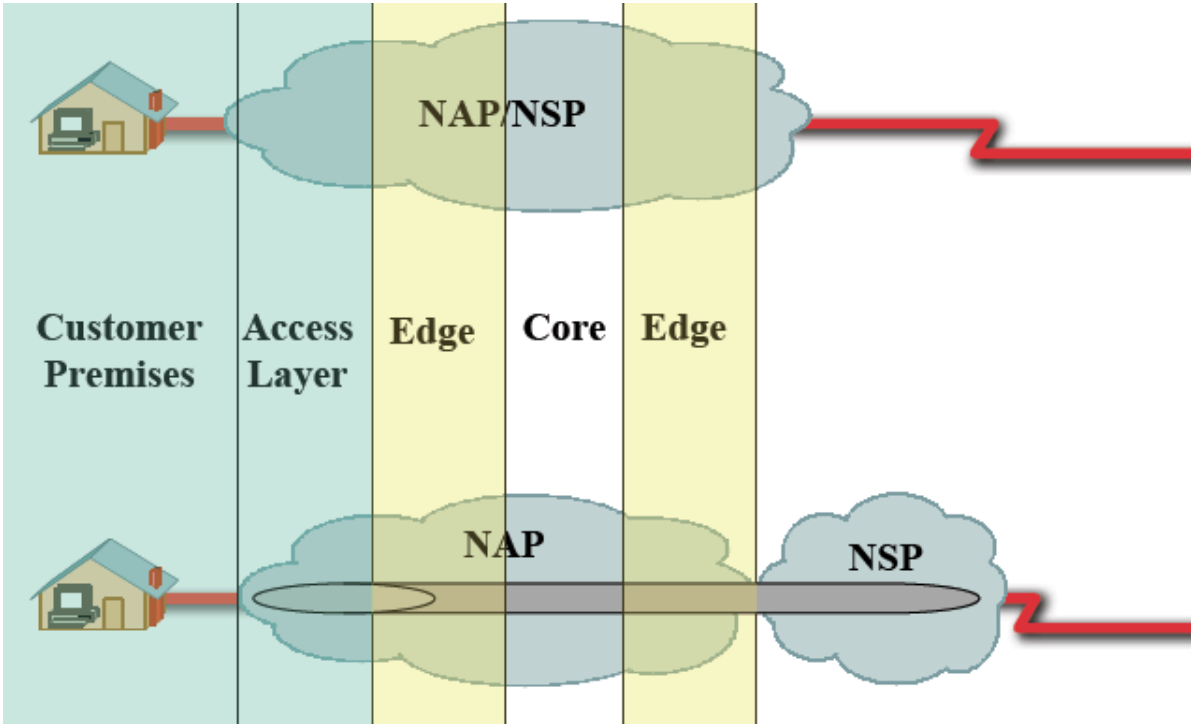
IPv6 en red de cable DOCSIS



4.2.2 IPv6 en redes ADSL

Modelos de acceso de banda ancha ADSL

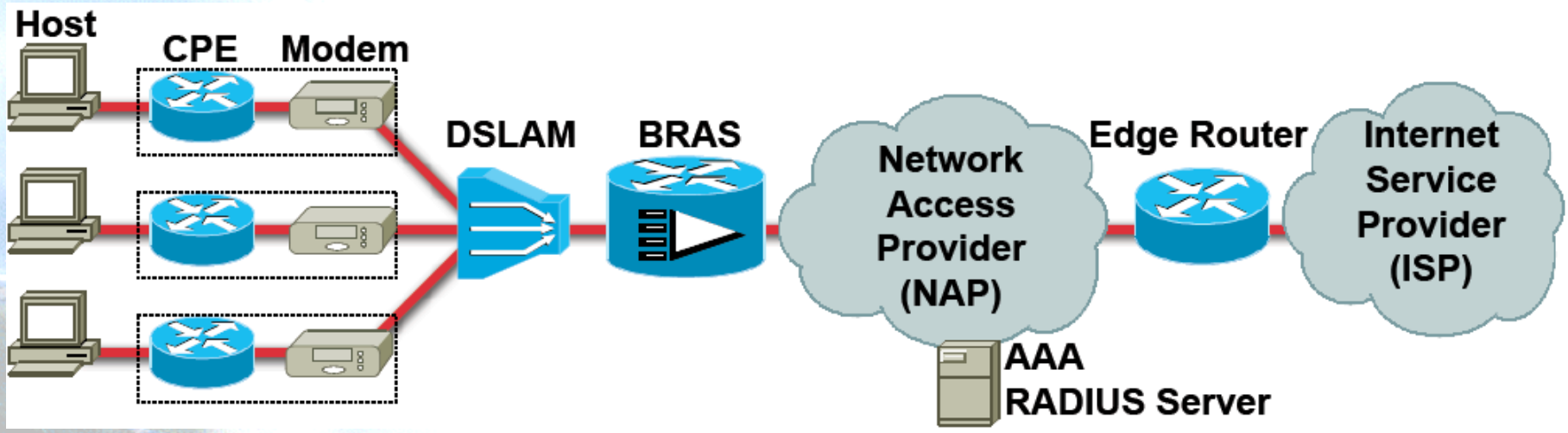
- NAP = NSP
  - Punto-a-punto
  - PPP Terminated Aggregation (PTA)
- NAP # NSP
  - Agregación L2TPv2 (LAA)



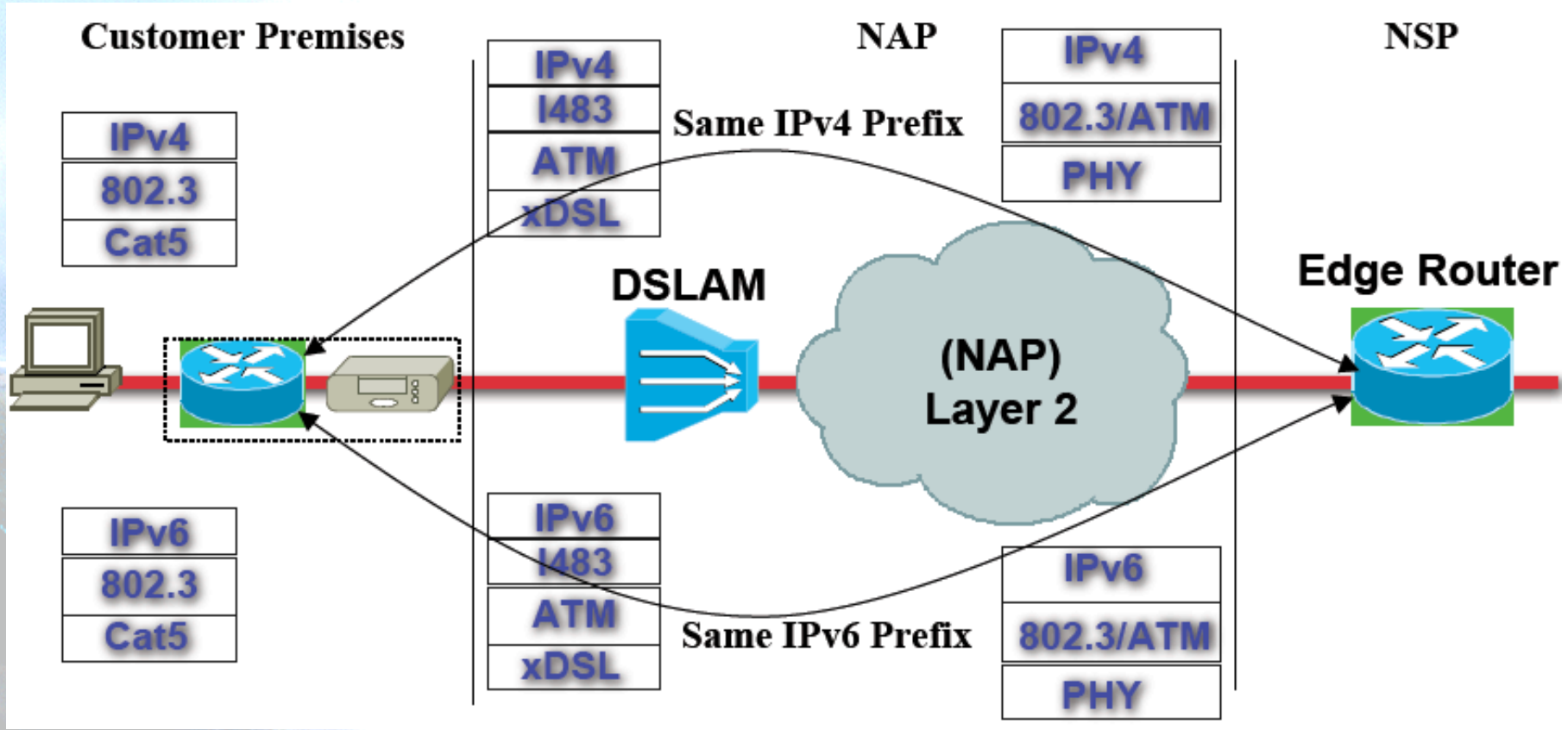
Componentes de red ADSL

- Broadband Remote Access Server (BRAS)
- Digital Subscriber Line Access Multiplexer (DSLAM)
- DSL Modem
- Customer Premises Equipment (CPE)
- Host
- Edge Router (ER)

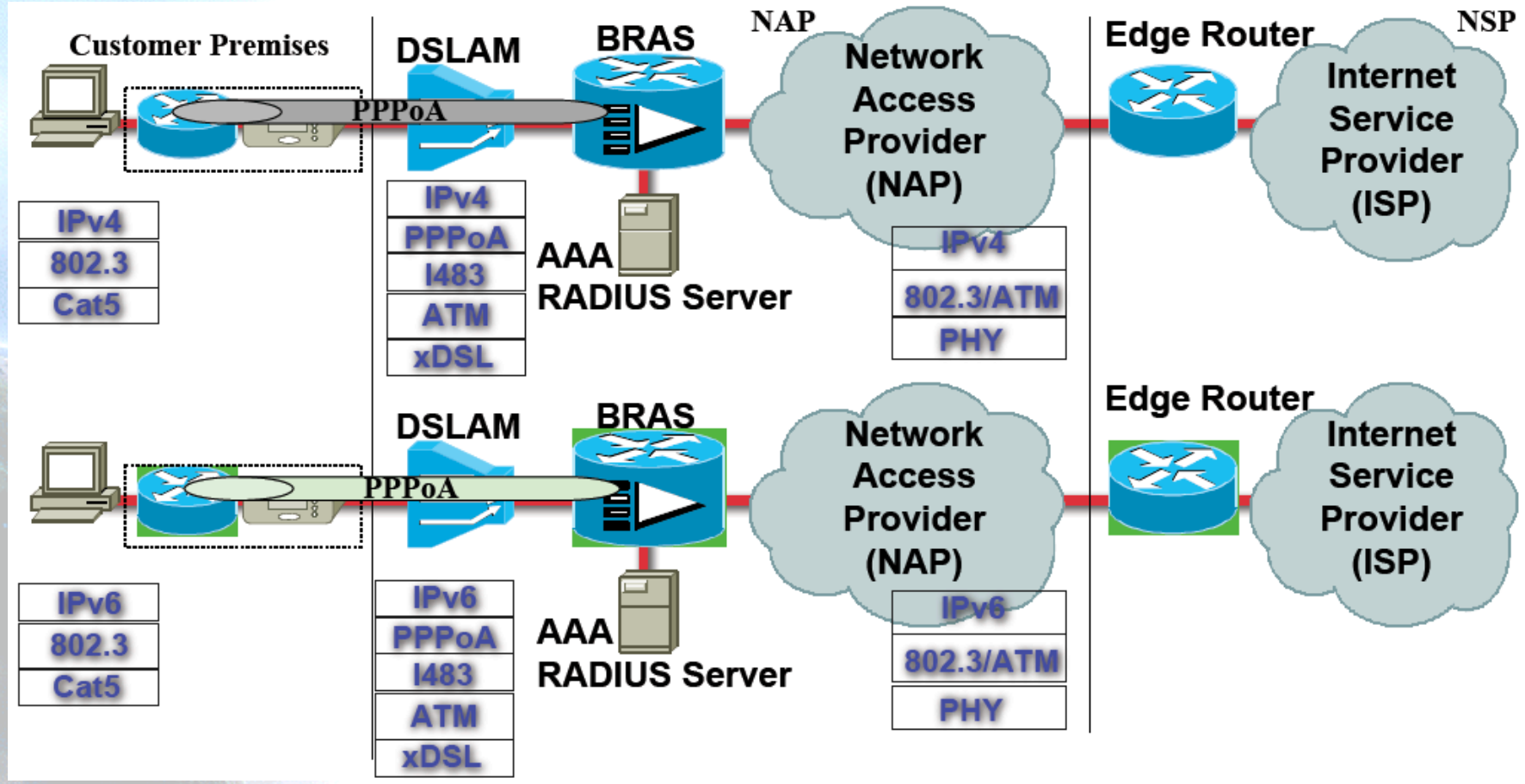
Topología básica de red ADSL



Modelo Punto-a-punto

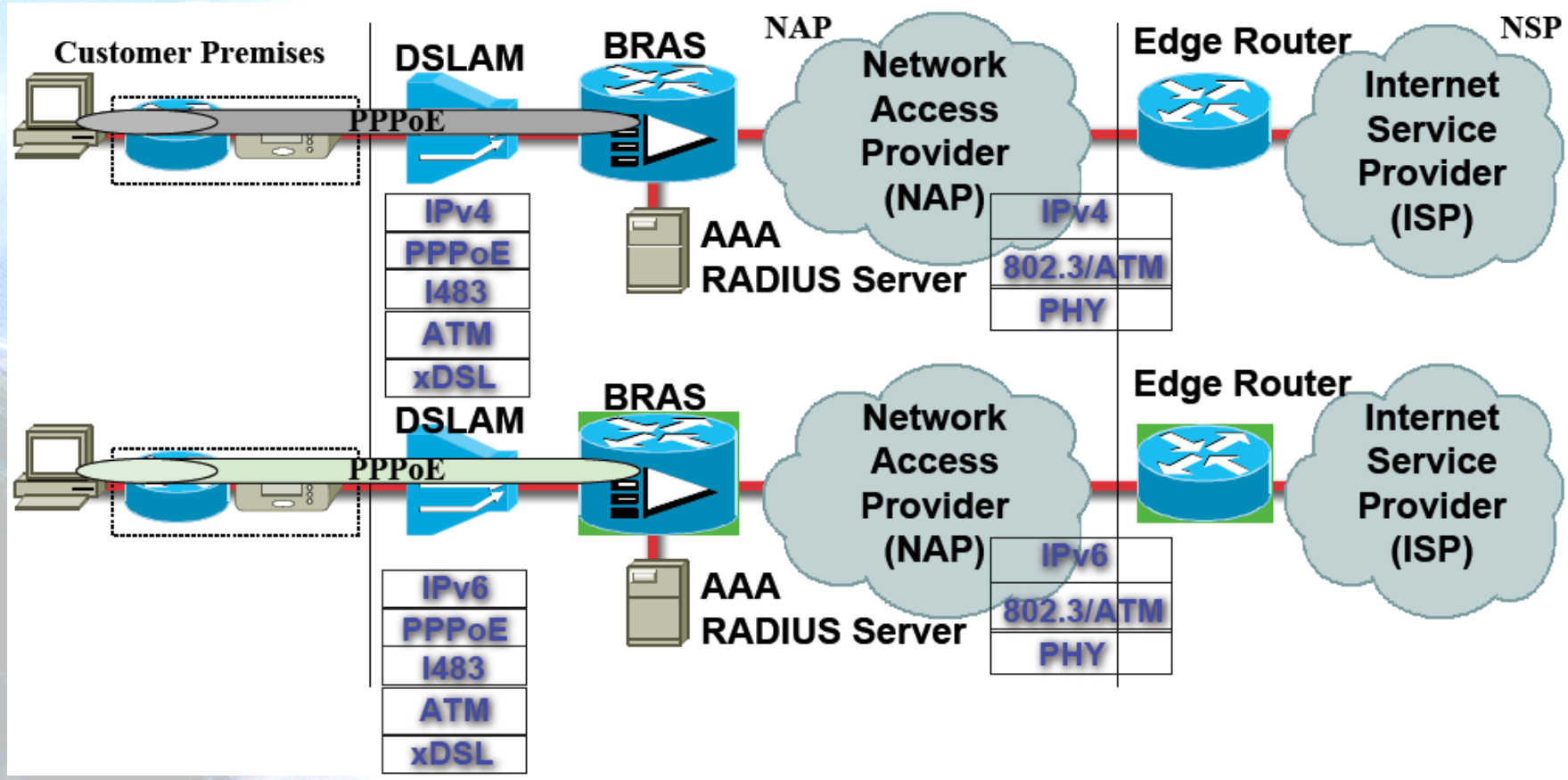


Modelo PPP Terminated Aggregation (PTA) - PPPoA



Nota: Solo una sesión PPPoA por PVC

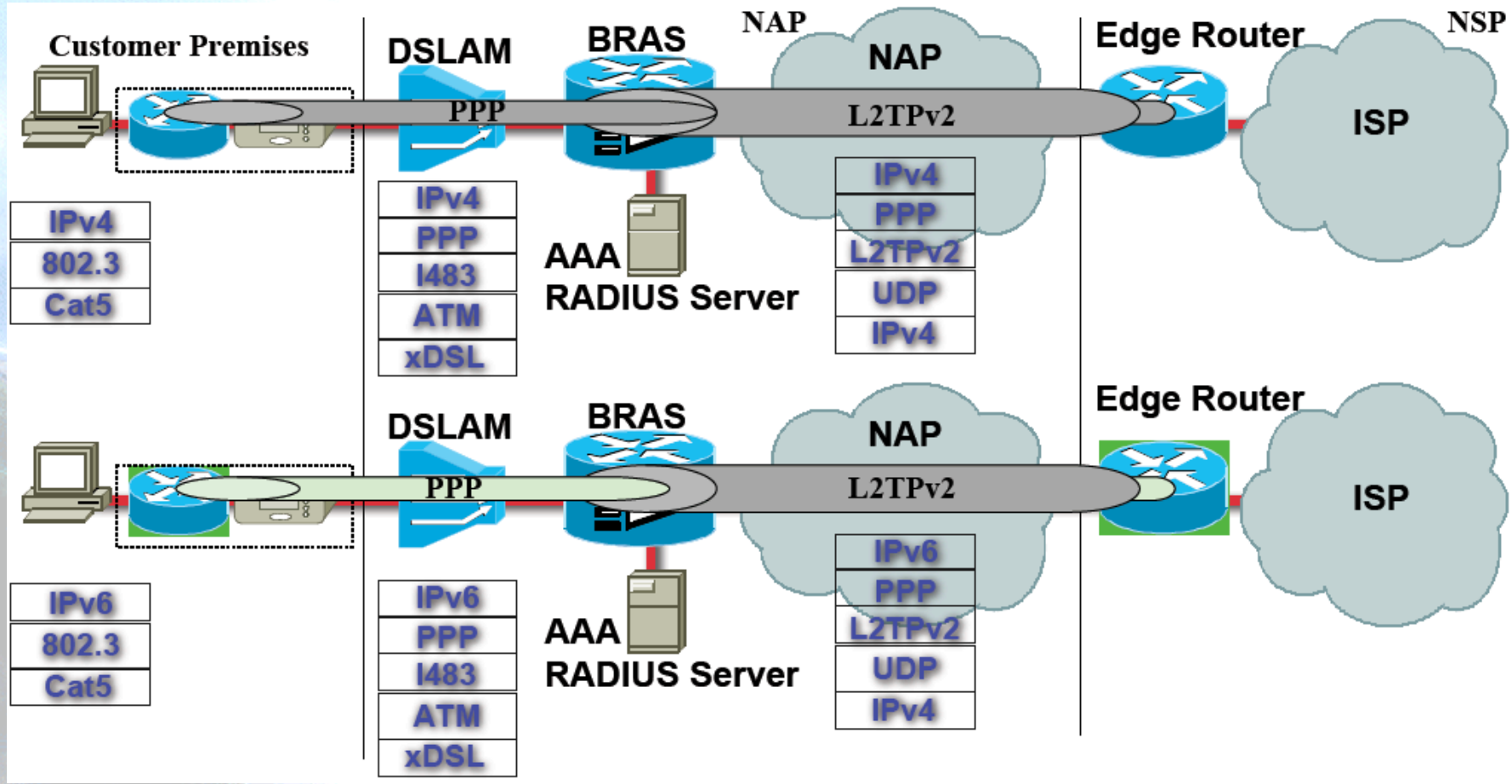
Modelo PPP Terminated Aggregation (PTA) - PPPoE



Notas: Múltiples sesiones PPPoE por PVC

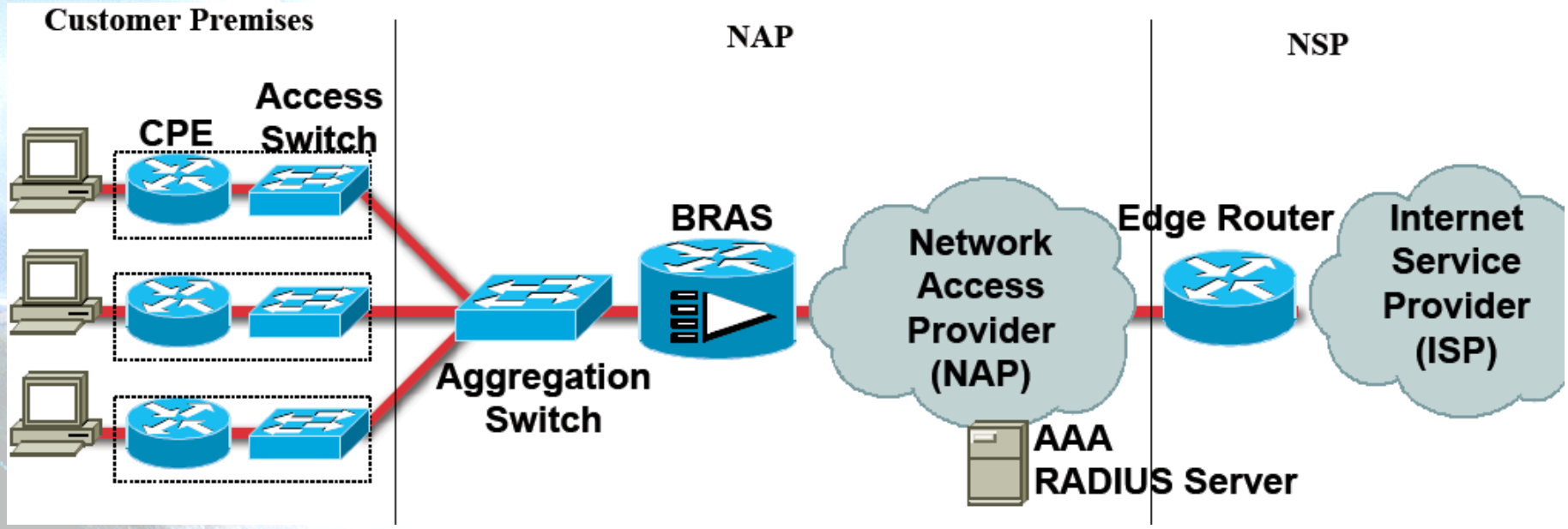
Las sesiones PPPoE pueden ser iniciadas por los hosts o los CPEs

Modelo Agregación de Acceso L2TPv2 (LAA)



4.2.3 IPv6 en redes Ethernet

Topología básica de red Ethernet de banda ancha

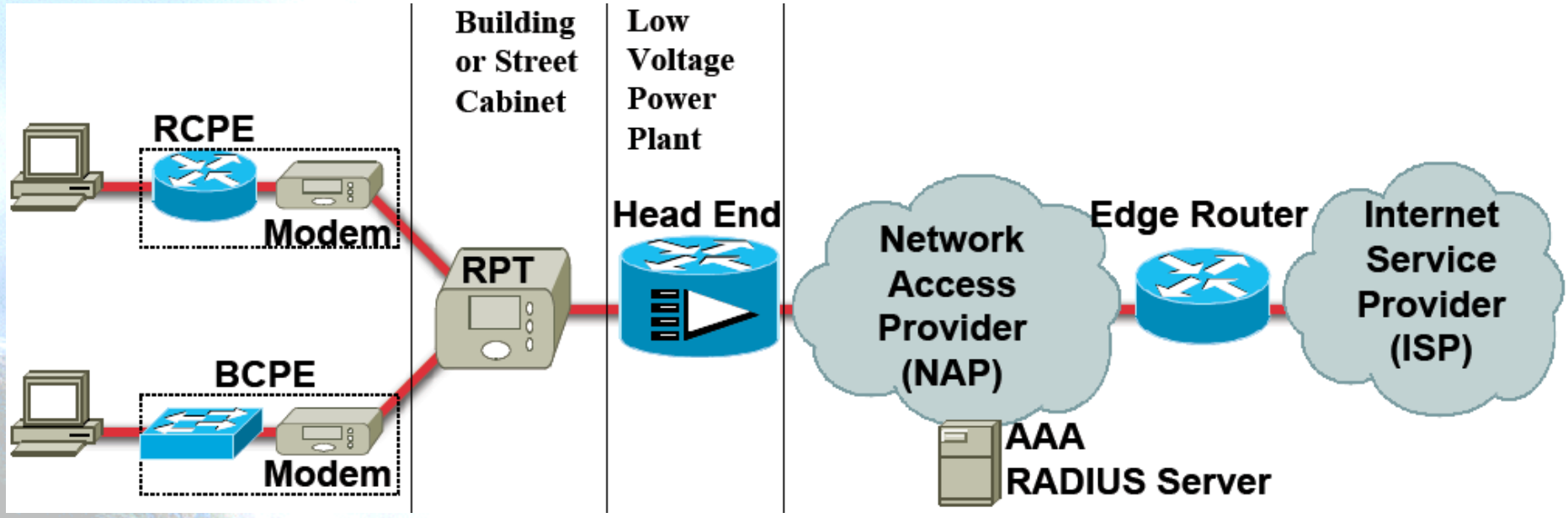


Modelos

- NAP = NSP
  - Punto-a-punto
  - PPP Terminated Aggregation (PTA)
- NAP # NSP
  - Agregación L2TPv2 (LAA)

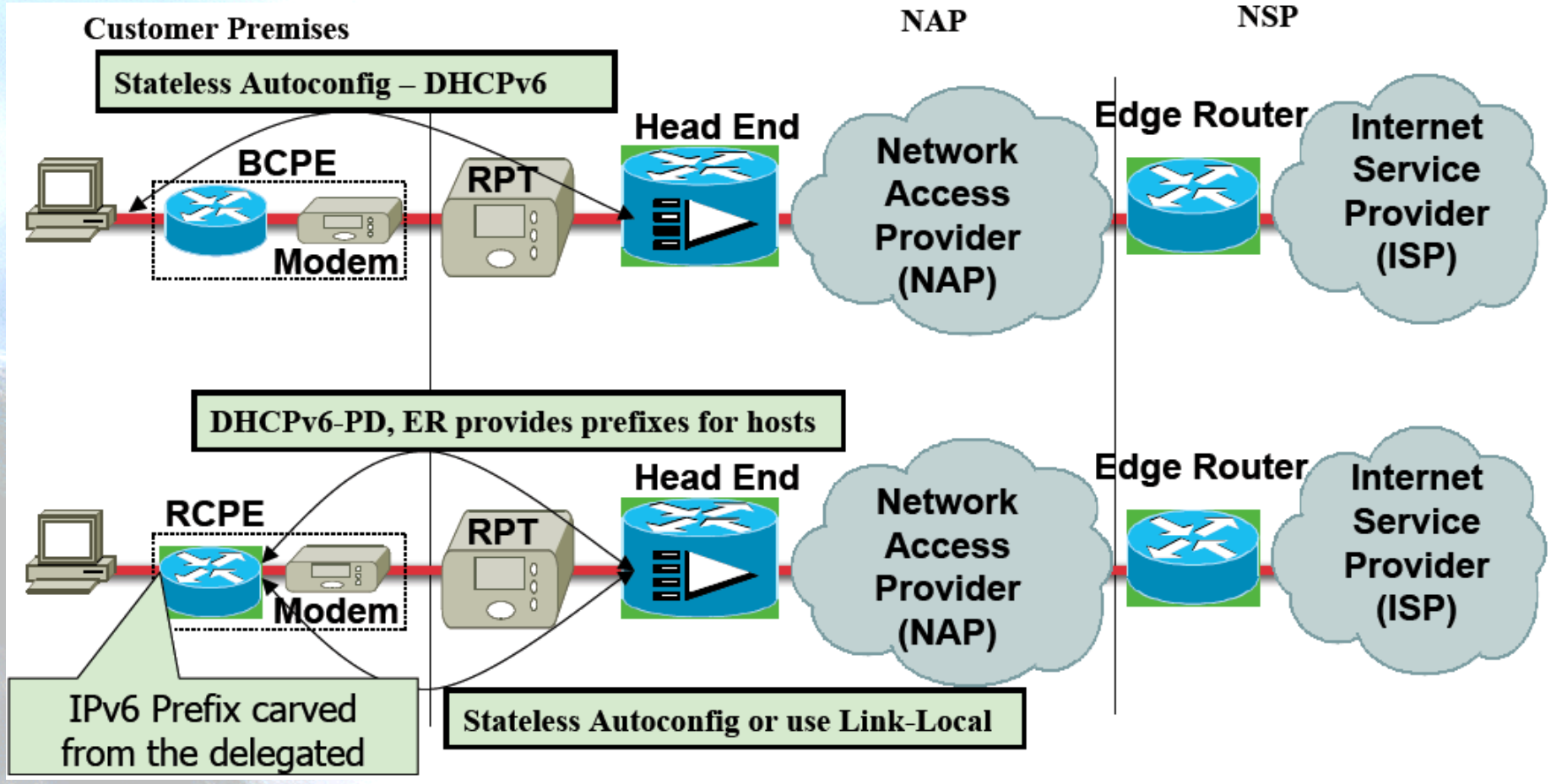
4.2.4 IPv6 en redes PLC

Topología básica de red PLC



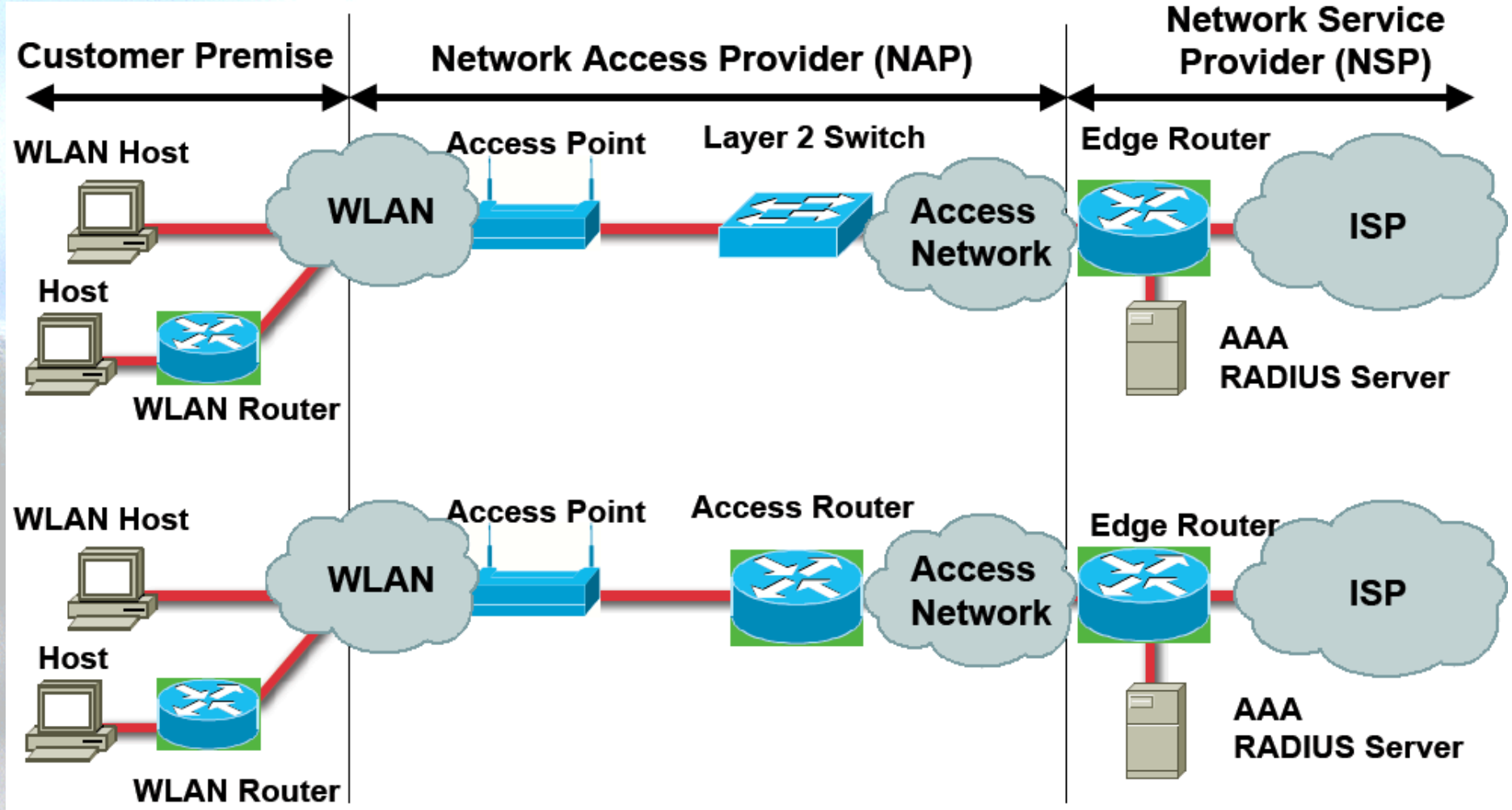
Nota: RTP es típicamente un dispositivos de nivel 2, pero puede ser un router en algunos casos

IPv6 en red PLC

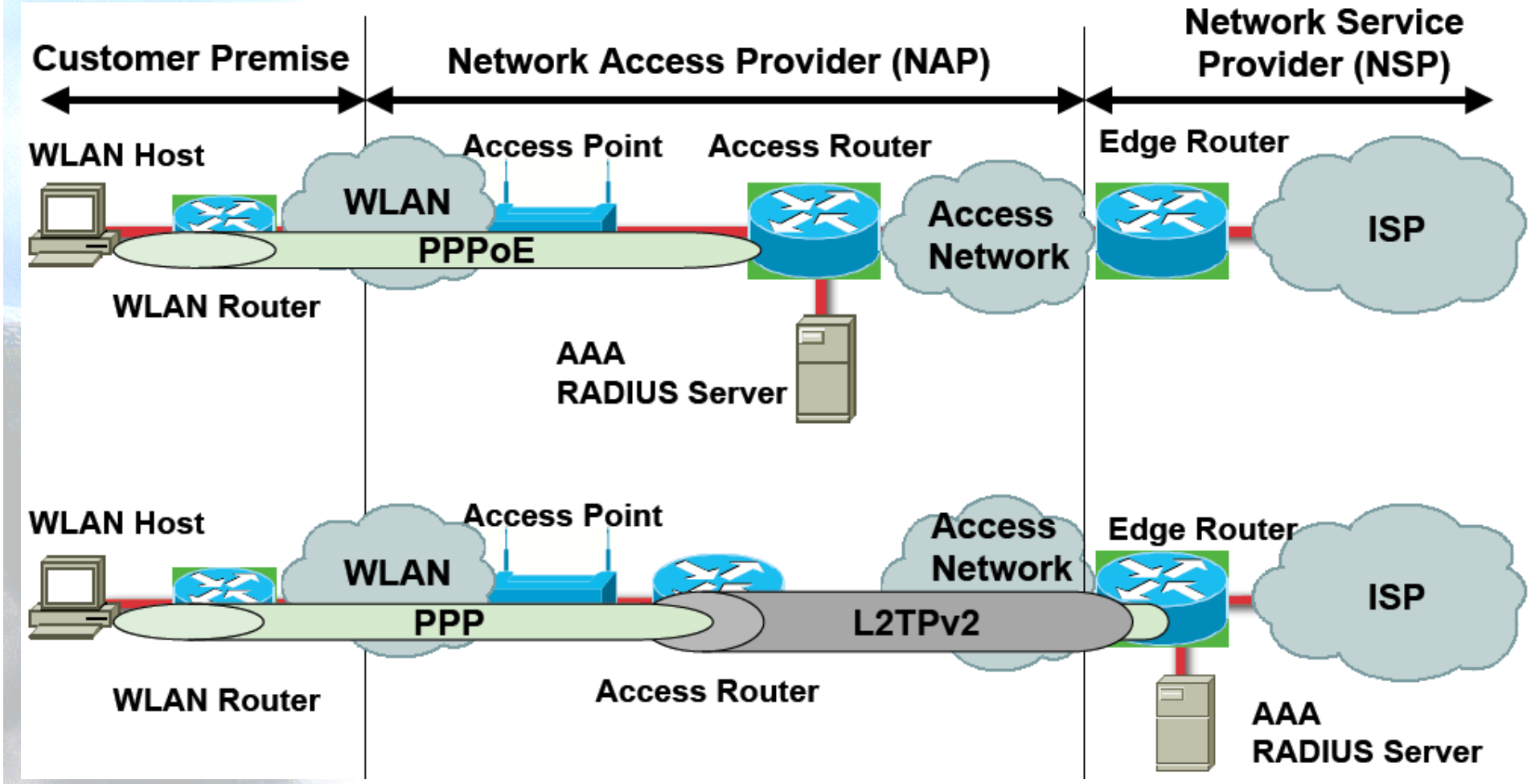


4.2.5 IPv6 en redes Inalámbricas

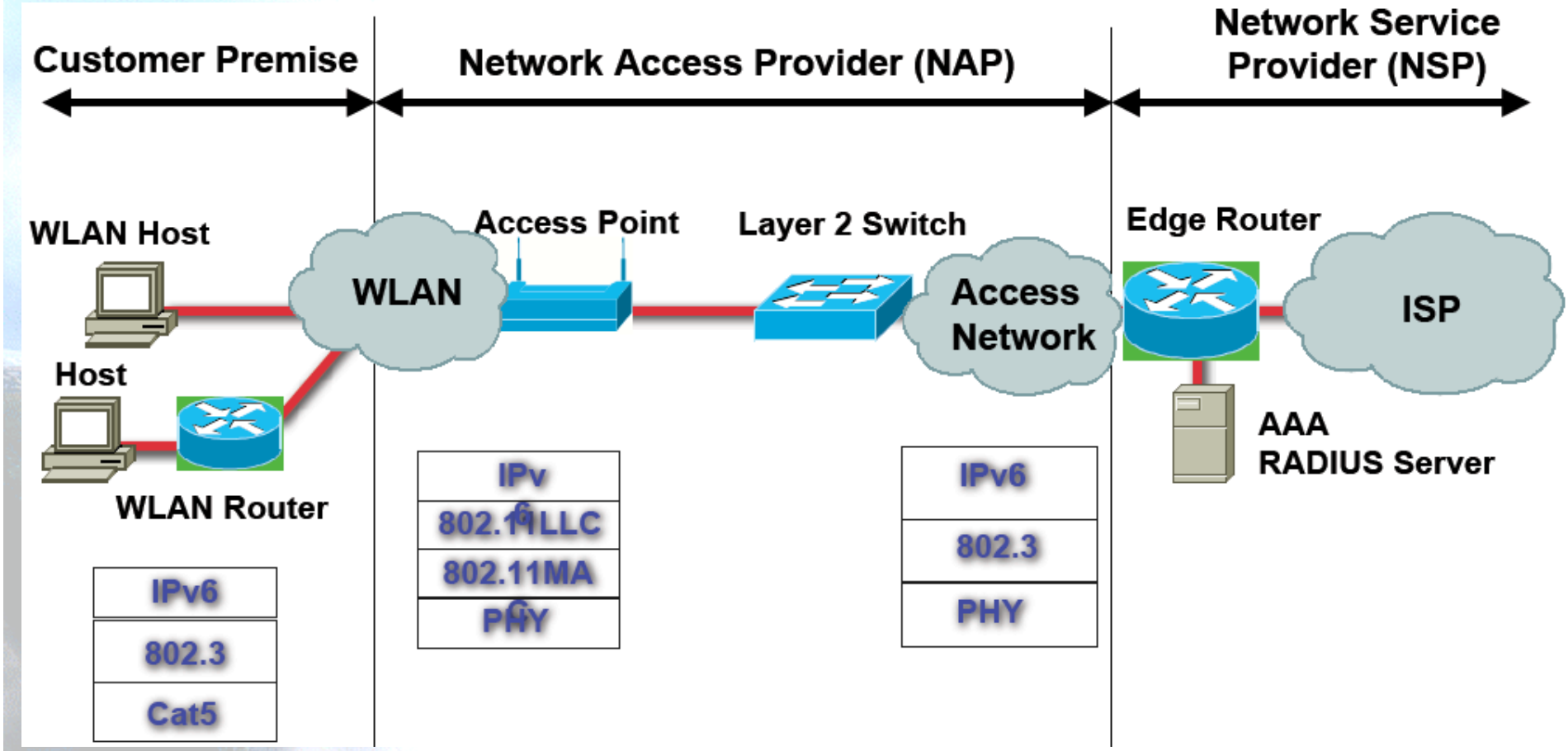
Modelos de IPv6 en redes Inalámbricas (1)



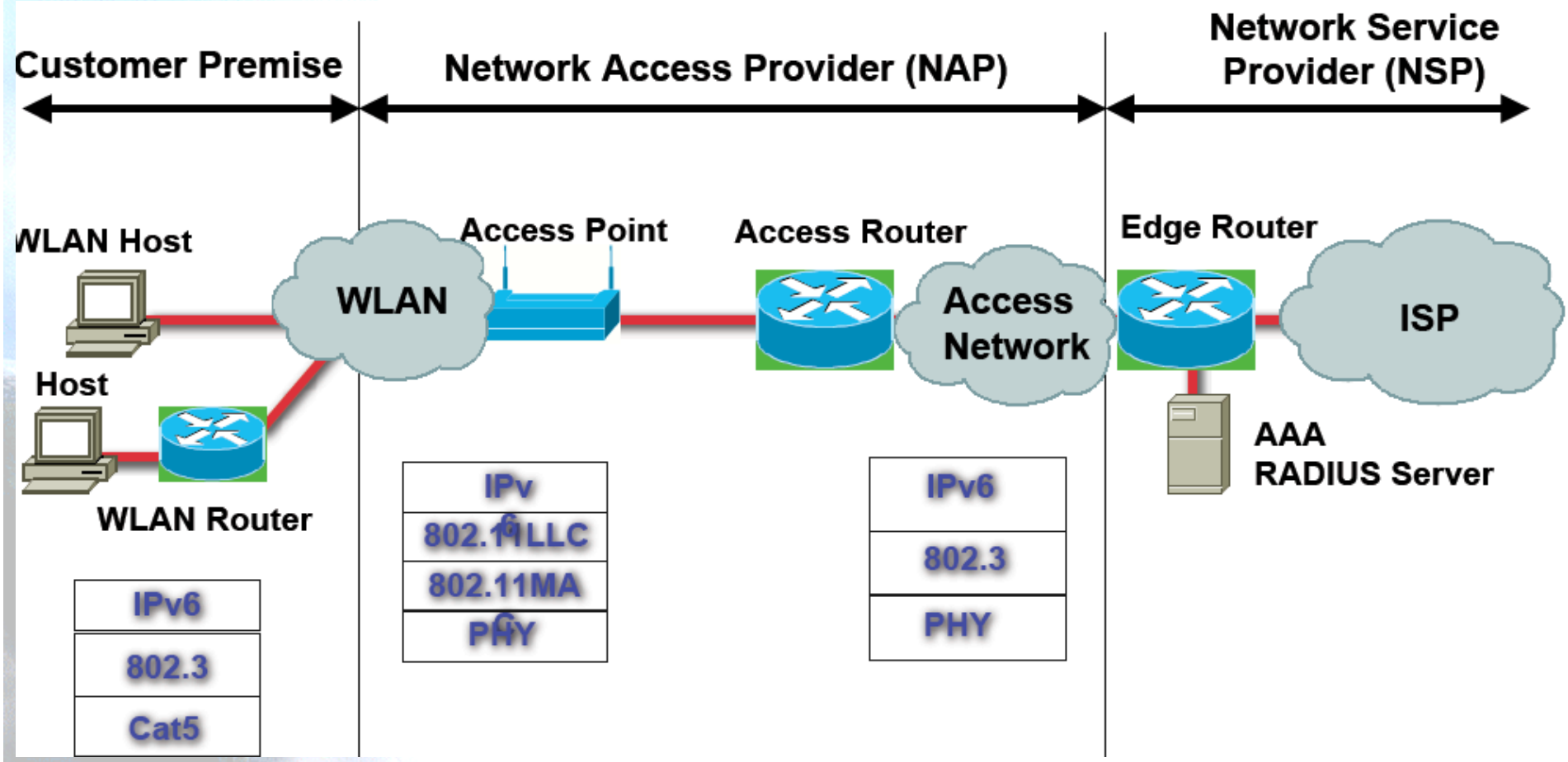
Modelos de IPv6 en redes Inalámbricas (2)



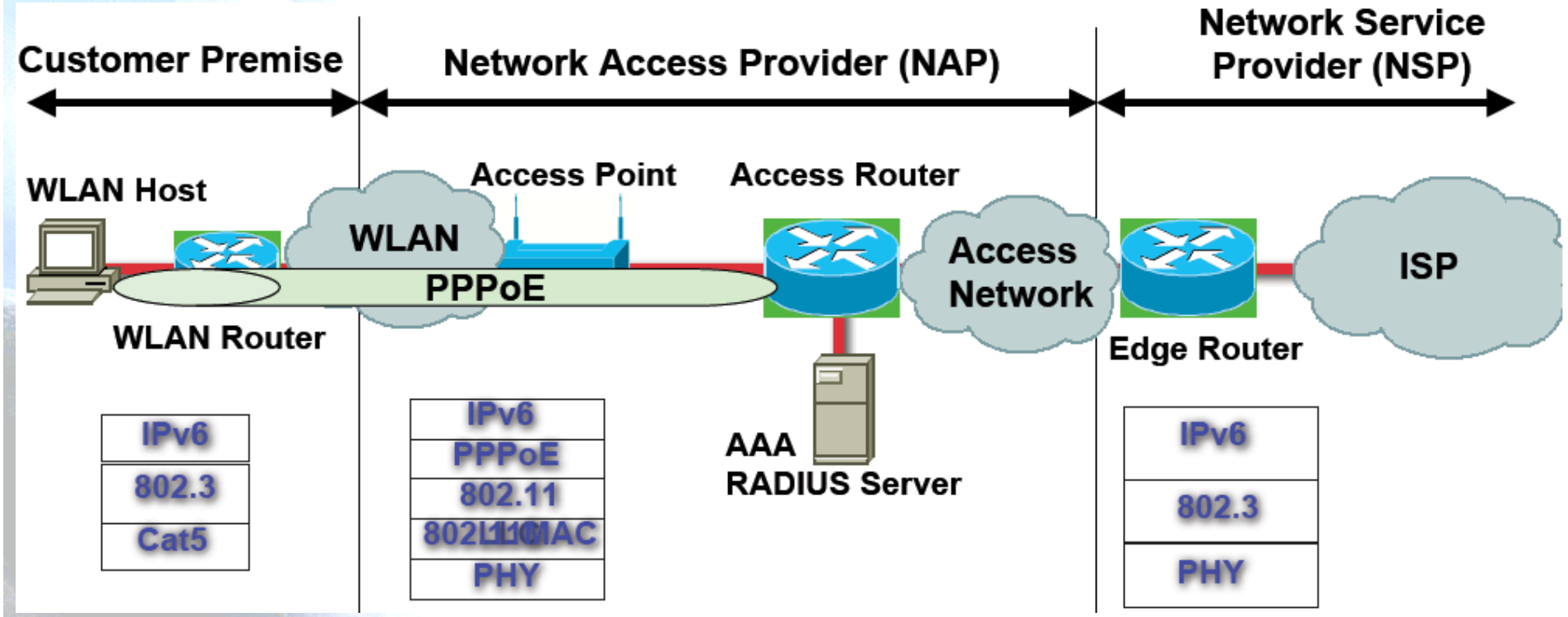
Switch nivel 2 entre AP y ER



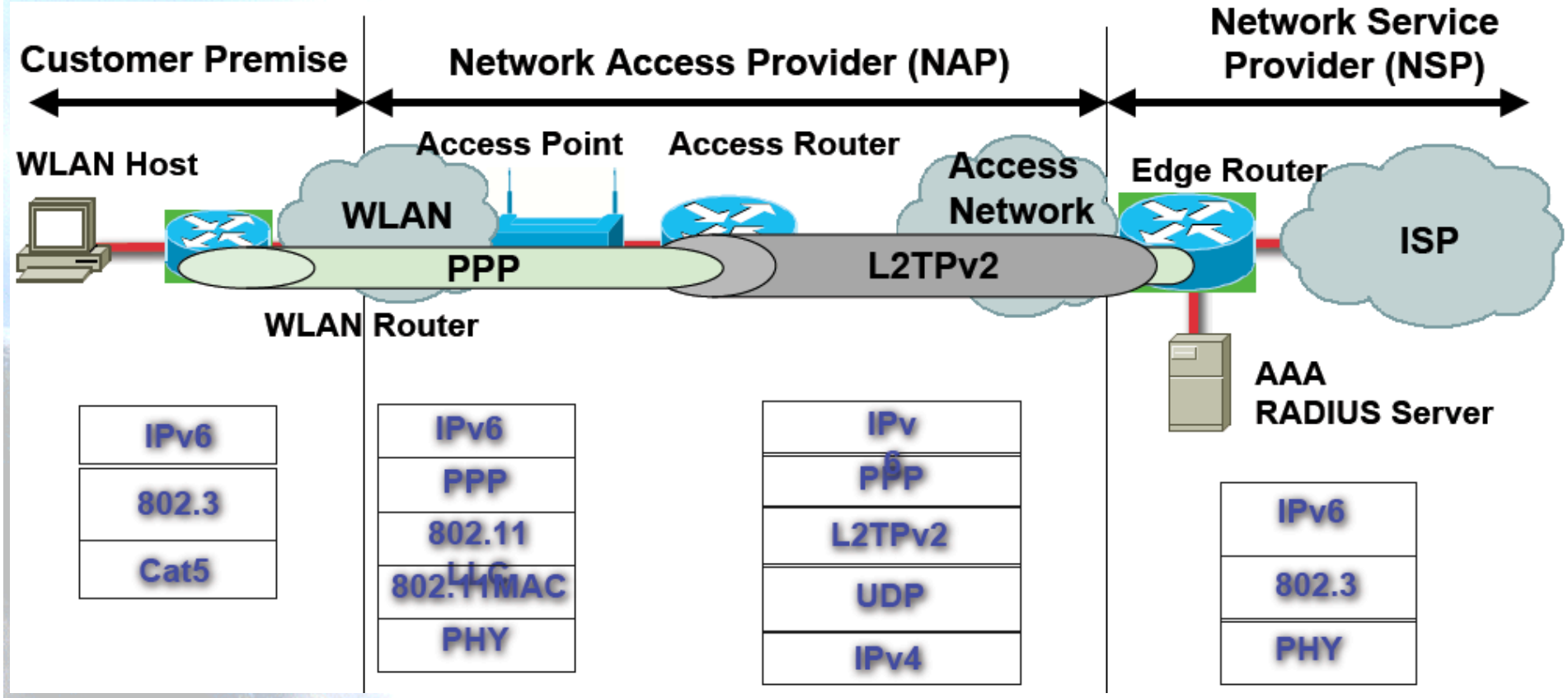
Router de acceso entre AP y ER



PPP Terminated Aggregation (PTA)



Agregación de Acceso L2TPv2 (LAA)



Referencias IPv6 y banda ancha

- EC IST 6LINK, “IPv6 and Broadband” http://www.ipv6tf.org/pdf/ISTClusterbooklet2005.pdf
- Ahmed, Popoviciu and Palet, “IPv6 Deployment Scenarios in Broadband Access Networks”, Barcelona Global IPv6 Summit, June 2005
- Atkinson, Correa and Hedlund, “Explaining International Broadband Leadership,” ITIF May 2008, http://www.itif.org/index.php?id=142
- Varios RFCs específicos detallados a continuación:

IPv6 en redes de Acceso de banda ancha

- RFC4779: ISP IPv6 Deployment Scenarios in Broadband Access Networks
  - Describe con detalle el despliegue de IPv6 en redes de proveedores de servicio de banda ancha
    - Escenarios
    - Métodos de integración
    - Coexistencia con servicios IPv4 ya instalados
    - Mecanismos de túneles e IPv6 nativo
  - Trata el despliegue en
    - Cable/HFC
    - Broadband Ethernet
    - xDSL
    - Broadband Power Line Communications (PLC/BPL)

IPv6 en IEEE 802.16 – WiMAX

- RFC4968: Analysis of IPv6 Link Models for IEEE 802.16 Based Networks
- RFC5120: Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks
- RFC5154: IP over IEEE 802.16 Problem Statement and Goals
- RFC5181:IPv6 Deployment Scenarios in 802.16 Networks
  - Describen el modelo, transmisión, escenarios de despliegue y objetivos de IPv6 en redes IEEE 802.16

IPv6 en 3G

- RFC3314: Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards
- RFC3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC3481: TCP over Second (2.5G) and Third (3G) Generation Wireless Networks
- RFC3574: Transition Scenarios for 3GPP Networks
- RFC4083: Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)
- RFC4215: Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks
- 3GPP Release 5
  - Describen la peculiaridades de IPv6 en redes de 3G

Gracias !!

Contacto:

- Jordi Palet (Consulintel): jordi.palet@consulintel.es

The IPv6 Portal:

http://www.ipv6tf.org